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

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1995, University of Toronto.

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

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. GateD is based on Kirton’s EGP, UC Berkeley’s routing daemon (routed), and DCM’s HELLO routing protocol.

Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

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

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

JUNOS Software Interfaces and Routing Configuration Guide
Release 10.2
Copyright © 2010, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Revision History
May 2010—Revision 01

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.

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions. Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details. For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.
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 reinstalling 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 II) 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 présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, 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

**About This Guide**  xxxvii

## Part 1  Configuring Router Interfaces

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Interfaces Overview</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Configuring Ethernet, DS1, DS3, and Serial Interfaces</td>
<td>81</td>
</tr>
<tr>
<td>3</td>
<td>Configuring Channelized T1/E1/ISDN PRI Interfaces</td>
<td>117</td>
</tr>
<tr>
<td>4</td>
<td>Configuring Digital Subscriber Line Interfaces</td>
<td>133</td>
</tr>
<tr>
<td>5</td>
<td>Configuring G.SHDSL Interfaces</td>
<td>165</td>
</tr>
<tr>
<td>6</td>
<td>Configuring DOCSIS Mini-PIM Interfaces</td>
<td>181</td>
</tr>
<tr>
<td>7</td>
<td>Configuring VDSL2 Interface</td>
<td>189</td>
</tr>
<tr>
<td>8</td>
<td>Configuring 2-Port 10 Gigabit Ethernet XPIM</td>
<td>227</td>
</tr>
<tr>
<td>9</td>
<td>Voice over Internet Protocol with Avaya</td>
<td>237</td>
</tr>
<tr>
<td>10</td>
<td>Configuring Point-to-Point Protocol over Ethernet</td>
<td>289</td>
</tr>
<tr>
<td>11</td>
<td>Configuring ISDN</td>
<td>309</td>
</tr>
<tr>
<td>12</td>
<td>Configuring 3G Wireless Modems for WAN Connections</td>
<td>355</td>
</tr>
<tr>
<td>13</td>
<td>Configuring USB Modems for Dial Backup</td>
<td>383</td>
</tr>
<tr>
<td>14</td>
<td>Configuring Link Services Interfaces</td>
<td>399</td>
</tr>
<tr>
<td>15</td>
<td>Aggregated Ethernet</td>
<td>449</td>
</tr>
</tbody>
</table>

## Part 2  Routing Protocols

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>Routing Overview</td>
<td>467</td>
</tr>
<tr>
<td>17</td>
<td>Static Routing</td>
<td>475</td>
</tr>
<tr>
<td>18</td>
<td>RIP</td>
<td>485</td>
</tr>
<tr>
<td>19</td>
<td>OSPF</td>
<td>503</td>
</tr>
<tr>
<td>20</td>
<td>IS-IS</td>
<td>525</td>
</tr>
<tr>
<td>21</td>
<td>BGP</td>
<td>535</td>
</tr>
<tr>
<td>22</td>
<td>Multicast</td>
<td>559</td>
</tr>
</tbody>
</table>

## Part 3  Routing Policies and Stateless Firewall Filters

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>Routing Policies</td>
<td>581</td>
</tr>
<tr>
<td>24</td>
<td>Stateless Firewall Filters</td>
<td>607</td>
</tr>
</tbody>
</table>

## Part 4  Layer 2 Bridging and Switching

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>Configuring Ethernet Ports for Switching</td>
<td>641</td>
</tr>
</tbody>
</table>
# Table of Contents

## About This Guide

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>J Series and SRX Series Documentation and Release Notes</td>
<td>xxxvii</td>
</tr>
<tr>
<td>Objectives</td>
<td>xxxviii</td>
</tr>
<tr>
<td>Audience</td>
<td>xxxviii</td>
</tr>
<tr>
<td>Supported Routing Platforms</td>
<td>xxxviii</td>
</tr>
<tr>
<td>Document Conventions</td>
<td>xxxviii</td>
</tr>
<tr>
<td>Documentation Feedback</td>
<td>xl</td>
</tr>
<tr>
<td>Requesting Technical Support</td>
<td>xl</td>
</tr>
<tr>
<td>Self-Help Online Tools and Resources</td>
<td>xli</td>
</tr>
<tr>
<td>Opening a Case with JTAC</td>
<td>xli</td>
</tr>
</tbody>
</table>

## Part 1

### Configuring Router Interfaces

## Chapter 1

### Interfaces Overview

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces Terms</td>
<td>4</td>
</tr>
<tr>
<td>Network Interfaces</td>
<td>8</td>
</tr>
<tr>
<td>Media Types</td>
<td>9</td>
</tr>
<tr>
<td>Network Interface Naming</td>
<td>9</td>
</tr>
<tr>
<td>Interface Naming Conventions</td>
<td>9</td>
</tr>
<tr>
<td>Understanding CLI Output for Interfaces</td>
<td>12</td>
</tr>
<tr>
<td>Data Link Layer Overview</td>
<td>14</td>
</tr>
<tr>
<td>Physical Addressing</td>
<td>14</td>
</tr>
<tr>
<td>Network Topology</td>
<td>14</td>
</tr>
<tr>
<td>Error Notification</td>
<td>14</td>
</tr>
<tr>
<td>Frame Sequencing</td>
<td>14</td>
</tr>
<tr>
<td>Flow Control</td>
<td>14</td>
</tr>
<tr>
<td>Data Link Sublayers</td>
<td>14</td>
</tr>
<tr>
<td>MAC Addressing</td>
<td>15</td>
</tr>
<tr>
<td>Ethernet Interface Overview</td>
<td>15</td>
</tr>
<tr>
<td>Ethernet Access Control and Transmission</td>
<td>16</td>
</tr>
<tr>
<td>Collisions and Detection</td>
<td>16</td>
</tr>
<tr>
<td>Collision Detection</td>
<td>16</td>
</tr>
<tr>
<td>Backoff Algorithm</td>
<td>17</td>
</tr>
<tr>
<td>Collision Domains and LAN Segments</td>
<td>17</td>
</tr>
<tr>
<td>Repeaters</td>
<td>17</td>
</tr>
<tr>
<td>Bridges and Switches</td>
<td>18</td>
</tr>
<tr>
<td>Broadcast Domains</td>
<td>18</td>
</tr>
<tr>
<td>Ethernet Frames</td>
<td>18</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>T1 and E1 Interfaces Overview</td>
<td>19</td>
</tr>
<tr>
<td>T1 Overview</td>
<td>19</td>
</tr>
<tr>
<td>E1 Overview</td>
<td>20</td>
</tr>
<tr>
<td>T1 and E1 Signals</td>
<td>20</td>
</tr>
<tr>
<td>Encoding</td>
<td>20</td>
</tr>
<tr>
<td>AMI Encoding</td>
<td>21</td>
</tr>
<tr>
<td>B8ZS and HDB3 Encoding</td>
<td>21</td>
</tr>
<tr>
<td>T1 and E1 Framing</td>
<td>21</td>
</tr>
<tr>
<td>Superframe (D4) Framing for T1</td>
<td>21</td>
</tr>
<tr>
<td>Extended Superframe (ESF) Framing for T1</td>
<td>22</td>
</tr>
<tr>
<td>T1 and E1 Loopback Signals</td>
<td>22</td>
</tr>
<tr>
<td>Channelized T1/E1/ISDN PRI Interfaces Overview</td>
<td>23</td>
</tr>
<tr>
<td>T3 and E3 Interfaces Overview</td>
<td>23</td>
</tr>
<tr>
<td>Multiplexing DS1 Signals</td>
<td>24</td>
</tr>
<tr>
<td>DS2 Bit Stuffing</td>
<td>24</td>
</tr>
<tr>
<td>DS3 Framing</td>
<td>25</td>
</tr>
<tr>
<td>M13 Asynchronous Framing</td>
<td>25</td>
</tr>
<tr>
<td>C-Bit Parity Framing</td>
<td>26</td>
</tr>
<tr>
<td>Serial Interface Overview</td>
<td>28</td>
</tr>
<tr>
<td>Serial Transmissions</td>
<td>29</td>
</tr>
<tr>
<td>Signal Polarity</td>
<td>30</td>
</tr>
<tr>
<td>Serial Clocking Modes</td>
<td>30</td>
</tr>
<tr>
<td>Serial Interface Transmit Clock Inversion</td>
<td>31</td>
</tr>
<tr>
<td>DTE Clock Rate Reduction</td>
<td>31</td>
</tr>
<tr>
<td>Serial Line Protocols</td>
<td>31</td>
</tr>
<tr>
<td>EIA-530</td>
<td>32</td>
</tr>
<tr>
<td>RS-232</td>
<td>32</td>
</tr>
<tr>
<td>RS-422/449</td>
<td>33</td>
</tr>
<tr>
<td>V.35</td>
<td>33</td>
</tr>
<tr>
<td>X.21</td>
<td>34</td>
</tr>
<tr>
<td>ADSL Interface Overview</td>
<td>34</td>
</tr>
<tr>
<td>ADSL Systems</td>
<td>35</td>
</tr>
<tr>
<td>ADSL2 and ADSL2+</td>
<td>37</td>
</tr>
<tr>
<td>ATM CoS Support</td>
<td>37</td>
</tr>
<tr>
<td>SHDSL Interface Overview</td>
<td>38</td>
</tr>
<tr>
<td>G.SHDSL Mini-PIM</td>
<td>39</td>
</tr>
<tr>
<td>G.SHDSL 8–Wire Mini-PIM Overview</td>
<td>39</td>
</tr>
<tr>
<td>Operating Modes and Line Rates of the G.SHDSL Mini-PIM</td>
<td>40</td>
</tr>
<tr>
<td>ATM CoS Support</td>
<td>40</td>
</tr>
<tr>
<td>VDSL2 Interface Overview</td>
<td>41</td>
</tr>
<tr>
<td>VDSL2 Systems</td>
<td>41</td>
</tr>
<tr>
<td>Packet Transfer Mode</td>
<td>41</td>
</tr>
<tr>
<td>Discrete Multitone Modulation</td>
<td>41</td>
</tr>
<tr>
<td>VDSL2 Terms</td>
<td>42</td>
</tr>
<tr>
<td>Implementation of a VDSL2 Network Using SRX Series Services</td>
<td>42</td>
</tr>
<tr>
<td>Gateways</td>
<td>42</td>
</tr>
<tr>
<td>VDSL2 Mini-PIM Support on SRX210 and SRX240 Services</td>
<td>44</td>
</tr>
<tr>
<td>Gateways</td>
<td>44</td>
</tr>
<tr>
<td>Supported Profiles</td>
<td>44</td>
</tr>
<tr>
<td>Supported Features</td>
<td>44</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>DOCSIS Mini-PIM Interface Overview</td>
<td>45</td>
</tr>
<tr>
<td>Introduction</td>
<td>45</td>
</tr>
<tr>
<td>Software Features Supported on DOCSIS Mini-PIMs</td>
<td>45</td>
</tr>
<tr>
<td>Configuring DOCSIS Mini-PIM</td>
<td>45</td>
</tr>
<tr>
<td>2-Port 10 Gigabit Ethernet XPIM Overview</td>
<td>47</td>
</tr>
<tr>
<td>10 Gigabit Ethernet Interface Overview</td>
<td>47</td>
</tr>
<tr>
<td>2-Port Gigabit Ethernet XPIM Overview</td>
<td>47</td>
</tr>
<tr>
<td>2-Port 10 Gigabit Ethernet XPIM Terminology</td>
<td>48</td>
</tr>
<tr>
<td>Supported Features</td>
<td>49</td>
</tr>
<tr>
<td>ISDN Interface Overview</td>
<td>49</td>
</tr>
<tr>
<td>ISDN Channels</td>
<td>49</td>
</tr>
<tr>
<td>ISDN Interfaces</td>
<td>50</td>
</tr>
<tr>
<td>Typical ISDN Network</td>
<td>50</td>
</tr>
<tr>
<td>NT Devices and S and T Interfaces</td>
<td>51</td>
</tr>
<tr>
<td>U Interface</td>
<td>51</td>
</tr>
<tr>
<td>ISDN Call Setup</td>
<td>51</td>
</tr>
<tr>
<td>Layer 2 ISDN Connection Initialization</td>
<td>51</td>
</tr>
<tr>
<td>Layer 3 ISDN Session Establishment</td>
<td>52</td>
</tr>
<tr>
<td>Interface Physical Properties</td>
<td>52</td>
</tr>
<tr>
<td>Bit Error Rate Testing</td>
<td>53</td>
</tr>
<tr>
<td>Interface Clocking</td>
<td>54</td>
</tr>
<tr>
<td>Data Stream Clocking</td>
<td>54</td>
</tr>
<tr>
<td>Explicit Clocking Signal Transmission</td>
<td>55</td>
</tr>
<tr>
<td>Frame Check Sequences</td>
<td>55</td>
</tr>
<tr>
<td>Cyclic Redundancy Checks and Checksums</td>
<td>55</td>
</tr>
<tr>
<td>Two-Dimensional Parity</td>
<td>55</td>
</tr>
<tr>
<td>MTU Default and Maximum Values</td>
<td>56</td>
</tr>
<tr>
<td>Physical Encapsulation on an Interface</td>
<td>57</td>
</tr>
<tr>
<td>Frame Relay</td>
<td>57</td>
</tr>
<tr>
<td>Virtual Circuits</td>
<td>58</td>
</tr>
<tr>
<td>Switched and Permanent Virtual Circuits</td>
<td>58</td>
</tr>
<tr>
<td>Data-Link Connection Identifiers</td>
<td>58</td>
</tr>
<tr>
<td>Congestion Control and Discard Eligibility</td>
<td>58</td>
</tr>
<tr>
<td>Point-to-Point Protocol</td>
<td>59</td>
</tr>
<tr>
<td>Link Control Protocol</td>
<td>59</td>
</tr>
<tr>
<td>PPP Authentication</td>
<td>60</td>
</tr>
<tr>
<td>Network Control Protocols</td>
<td>60</td>
</tr>
<tr>
<td>Magic Numbers</td>
<td>61</td>
</tr>
<tr>
<td>CSU/DSU Devices</td>
<td>61</td>
</tr>
<tr>
<td>Point-to-Point Protocol over Ethernet</td>
<td>61</td>
</tr>
<tr>
<td>PPPoE Discovery</td>
<td>62</td>
</tr>
<tr>
<td>PPPoE Sessions</td>
<td>62</td>
</tr>
<tr>
<td>High-Level Data Link Control</td>
<td>63</td>
</tr>
<tr>
<td>HDLC Stations</td>
<td>63</td>
</tr>
<tr>
<td>HDLC Operational Modes</td>
<td>63</td>
</tr>
</tbody>
</table>
### Interface Logical Properties

- Protocol Families .................................................................64
  - Common Protocol Suites ..................................................64
  - Other Protocol Suites ..........................................................65
- IPv4 Addressing ........................................................................65
  - IPv4 Classful Addressing ..................................................65
  - IPv4 Dotted Decimal Notation ............................................66
  - IPv4 Subnetting .....................................................................66
  - IPv4 Variable-Length Subnet Masks ........................................67
- IPv6 Addressing ........................................................................68
  - IPv6 Address Representation .............................................68
  - IPv6 Address Types .............................................................69
  - IPv6 Address Scope .............................................................69
  - IPv6 Address Structure ........................................................69
  - IPv6 Protocol Family: inet6 ...............................................70
  - Enabling Flow-Based Processing for IPv6 Traffic ....................71
- Virtual LANs ............................................................................72
- Special Interfaces .......................................................................74
  - Discard Interface ................................................................76
  - Loopback Interface .............................................................76
  - Management Interface ........................................................77
  - Services Interfaces .............................................................78
    - MLPPP and MLFR ..........................................................78
    - MLFR Frame Relay Forum ...............................................78
    - CRTP .............................................................................79

## Chapter 2 Configuring Ethernet, DS1, DS3, and Serial Interfaces 81

- Before You Begin ........................................................................81
- Configuring Interfaces—Quick Configuration .................................82
  - Configuring an E1 Interface with Quick Configuration ..................84
  - Configuring an E3 Interface with Quick Configuration ..................87
  - Configuring a Fast Ethernet Interface with Quick Configuration ....90
  - Configuring Gigabit Ethernet Interfaces—Quick Configuration ....94
  - Configuring T1 Interfaces with Quick Configuration ....................97
  - Configuring T3 Interfaces with Quick Configuration ...................101
  - Configuring Serial Interfaces with Quick Configuration ...............104
- Enabling and Disabling Promiscuous Mode on Ethernet Interfaces ....108
  - Understanding Promiscuous Mode .........................................108
  - Enabling and Disabling Promiscuous Mode ................................109
    - J-Web Point and Click CLI Configuration .............................109
    - CLI Configuration ...........................................................109
- Configuring Network Interfaces with a Configuration Editor .............109
  - Adding a Network Interface with a Configuration Editor .............110
  - Configuring Static ARP Entries on Ethernet Interfaces ...............111
  - Deleting a Network Interface with a Configuration Editor ...........112
- Verifying Interface Configuration .............................................113
  - Verifying the Link State of All Interfaces ..................................113
  - Verifying Interface Properties ..............................................114
Chapter 5  Configuring G.SHDSL Interfaces 165

Before You Begin .................................................................165
Configuring the G.SHDSL Interface with the CLI Configuration Editor ........165
Verifying G.SHDSL Interface Properties ........................................168
Configuring the G.SHDSL Interface on SRX Series Devices ..............176
  Topology Diagrams of the G.SHDSL Mini-PIM ..........................176
  Example: Configuring the G.SHDSL Interface on the SRX210 Services
           Gateway ....................................................................177

Chapter 6  Configuring DOCSIS Mini-PIM Interfaces 181

Before You Begin ......................................................................181
Configuring the DOCSIS Interfaces (CLI procedure) .........................181
Configuring the DOCSIS Logical Interfaces (J-Web procedure) ..........183
Configuring the DOCSIS Physical Interfaces (J-Web procedure) ..........184
Verifying DOCSIS Interfaces Properties ...................................184

Chapter 7  Configuring VDSL2 Interface 189

Before You Begin ......................................................................189
Configuring the VDSL2 Interface with the CLI Configuration Editor ..........189
Example: Configuring the VDSL2 Interface on SRX Series Services Gateways
  (CLI) .............................................................................191
  Requirements .................................................................191
  Overview .........................................................................191
Before You Begin ......................................................................192
VDSL2 Interface Configuration ......................................................193
  VDSL2 Mini-PIM Default Configuration and Verification ...............193
  Configuring the VDSL2 Interface for End-to-End Data Path ..........196
  Configuring PPPoE on the pt-x/x/x Interface with a Static IP
     Address ........................................................................199
  Configuring PPPoE on the pt-x/x/x Interface with a Static IP
     Address (CHAP Authentication) ....................................200
  Configuring PPPoE on the pt-x/x/x Interface with Unnumbered IP
     (PAP Authentication) ......................................................202
  Configuring PPPoE on the pt-x/x/x Interface with Unnumbered IP
     (CHAP Authentication) ......................................................203
  Configuring PPPoE on the pt-x/x/x Interface with Negotiated IP (PAP
     Authentication) .............................................................205
  Configuring PPPoE on the pt-x/x/x Interface with Negotiated IP
     (CHAP Authentication) ......................................................206
Example: Configuring the ADSL Interface on SRX Series Services Gateway
  (CLI) .............................................................................208
  Requirements .....................................................................208
  Overview .........................................................................208
Chapter 8 Configuring 2-Port 10 Gigabit Ethernet XPIM

Configuring 2-Port 10 Gigabit Ethernet XPIM Interface (CLI Procedure) ........................................... 227
Configuring 2-Port 10 Gigabit Ethernet XPIM Interface (J-Web Procedure) ........................................... 230
Verifying the 2-Port 10 Gigabit Ethernet XPIM Configuration ................................................................. 233

Chapter 9 Voice over Internet Protocol with Avaya

Console and Connector Port Pinouts ................................................. 238
TGM550 Console Port Pinouts ....................................................... 238
TGM550 RJ-11 Connector Pinout for Analog Ports ...................... 239
TIM508 Connector Pinout ............................................................. 239
TIM510 RJ-45 Connector Pinout ................................................... 240
TIM514 Connector Pinout .............................................................. 240
TIM516 Connector Pinout .............................................................. 241
TIM518 Connector Pinout .............................................................. 242
Avaya VoIP Modules ................................................................. 244
Avaya VoIP Module Summary ..................................................... 244
TGM550 Telephony Gateway Module ........................................ 247
TIM508 Analog Telephony Interface Module ......................... 250
TIM510 E1/T1 Telephony Interface Module .............................. 251
TIM514 Analog Telephony Interface Module ............................ 253
TIM516 Analog Telephony Interface Module ............................ 254
TIM518 Analog Telephony Interface Module ............................ 255
TIM521 BRI Telephony Interface Module ................................. 256
VoIP Terms ........................................................................... 257
VoIP Overview ............................................................................................259
  About the Avaya IG550 Integrated Gateway ........................................260
  VoIP Interfaces .....................................................................................261
  Avaya VoIP Modules Overview .............................................................262
  Media Gateway Controller .....................................................................263
  Avaya Communication Manager ...........................................................264
  Dynamic Call Admission Control Overview ...........................................264
    Supported Interfaces ........................................................................264
    Bearer Bandwidth Limit and Activation Priority ..............................265
    Rules for Determining Reported BBL ..............................................265
  TGM550 Firmware Compatibility with JUNOS Internet Software ...........266
  TGM550 IP Addressing Guidelines ........................................................266

Before You Begin .........................................................................................267
  Configuring VoIP Interfaces with EPW and Disk-on-Key .........................268
  Configuring VoIP Interfaces with Quick Configuration .............................269
  Configuring VoIP with a Configuration Editor .........................................272
    Configuring the VoIP Interface (Required) ...........................................272
    Configuring the Media Gateway Controller List (Required) ...............273
    Configuring an MGC List and Adding Addresses ................................274
    Clearing an MGC List .....................................................................275
    Configuring Dynamic Call Admission Control on WAN Interfaces
      (Optional) ...................................................................................275
  Modifying the IP Address of the TGM550 ..............................................277

Accessing and Administering the TGM550 CLI ............................................278
  TGM550 Access Requirements ..............................................................279
  Connecting Through the TGM550 Console Port ..................................279
  Connecting to the TGM550 with SSH .................................................280
  Accessing the TGM550 with Telnet ......................................................280
    Enabling Telnet Service on the TGM550 .......................................280
    Connecting to the TGM550 with Telnet .......................................281
    Disabling Telnet Service on the TGM550 .......................................281
  Accessing the Services Router from the TGM550 .................................282
  Resetting the TGM550 .....................................................................282
  Saving the TGM550 Configuration ......................................................283

Verifying the VoIP Configuration .................................................................283
  Verifying the VoIP Interface ................................................................283
  Verifying the Media Gateway Controller List .......................................285
  Verifying Bandwidth Available for VoIP Traffic .................................285

Frequently Asked Questions About the VoIP Interface .................................286
  TGM550 Is Installed But the VoIP Interface Is Unavailable .................286
Dialer Interface ...............................................................................313
Before You Begin .........................................................................................313
Configuring ISDN BRI Interfaces with Quick Configuration .........................314
Configuring ISDN BRI Physical Interfaces with Quick Configuration ...314
Configuring ISDN BRI Dialer Interfaces with Quick Configuration ........317
Configuring ISDN Interfaces and Features with a Configuration Editor ..........321
Adding an ISDN BRI Interface (Required) ..............................................321
Configuring Dialer Interfaces (Required) ...............................................324
Configuring Dial Backup .......................................................................327
Configuring Dialer Filters for Dial-on-Demand Routing Backup ........328
    Configuring the Dialer Filter ...........................................................328
    Applying the Dial-on-Demand Dialer Filter to the Dialer Interface ........329
Configuring Dialer Watch ......................................................................330
    Adding a Dialer Watch Interface on the Device .......................330
    Configuring the ISDN Interface for Dialer Watch ................330
Configuring Dial-on-Demand Routing Backup with OSPF Support (Optional) .................................................................331
    Configuring Bandwidth on Demand (Optional) ................332
    Configuring Dialer Interfaces for Bandwidth on Demand ..........332
    Configuring an ISDN Interface for Bandwidth on Demand .........336
Configuring Dial-In and Callback (Optional) ........................................337
    Configuring Dialer Interfaces for Dial-In and Callback ..........339
    Configuring an ISDN Interface to Screen Incoming Calls ..........340
    Configuring the Device to Reject Incoming ISDN Calls ..........341
Disabling Dialing Out Through Dialer Interfaces ...................................342
Disabling ISDN Signaling .......................................................................343
Verifying the ISDN Configuration ..........................................................343
Displaying the ISDN Status ...................................................................344
Verifying an ISDN BRI Interface ............................................................345
Verifying an ISDN PRI Interface and Checking B-Channel Interface Statistics .................................................................346
Checking D-Channel Interface Statistics ................................................347
Displaying the Status of ISDN Calls .......................................................349
Verifying Dialer Interface Configuration ................................................350

Chapter 12 Configuring 3G Wireless Modems for WAN Connections 355

3G Wireless Modem Support on Different Device Types .........................356
3G Wireless Overview ...........................................................................356
    Supported Devices and 3G Wireless Modem Cards ........357
3G Terms ..............................................................................................357
    Related Topics ..............................................................................359
Understanding the 3G Wireless Modem Interface ....................................359
    Related Topics ..............................................................................359
Understanding the Dialer Interface ......................................................360
    Authentication for GSM HSDPA 3G Wireless Modems ..........360
    Backup, Dialer Filter, and Dialer Watch ....................360
    Operating Parameters ..........................................................361
    Related Topics ..............................................................................361
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding the GSM Profile</td>
<td>361</td>
</tr>
<tr>
<td>Related Topics</td>
<td>362</td>
</tr>
<tr>
<td>3G Wireless Modem Configuration Overview</td>
<td>362</td>
</tr>
<tr>
<td>Related Topics</td>
<td>363</td>
</tr>
<tr>
<td>Configuring the 3G Wireless Modem Interface—Quick Configuration</td>
<td>363</td>
</tr>
<tr>
<td>Related Topics</td>
<td>365</td>
</tr>
<tr>
<td>Configuring the Dialer Interface</td>
<td>365</td>
</tr>
<tr>
<td>J-Web Configuration</td>
<td>365</td>
</tr>
<tr>
<td>CLI Configuration</td>
<td>366</td>
</tr>
<tr>
<td>Related Topics</td>
<td>366</td>
</tr>
<tr>
<td>Configuring the 3G Wireless Modem Interface</td>
<td>367</td>
</tr>
<tr>
<td>J-Web Configuration</td>
<td>367</td>
</tr>
<tr>
<td>CLI Configuration</td>
<td>367</td>
</tr>
<tr>
<td>Related Topics</td>
<td>368</td>
</tr>
<tr>
<td>Configuring the GSM Profile</td>
<td>368</td>
</tr>
<tr>
<td>J-Web Configuration</td>
<td>369</td>
</tr>
<tr>
<td>CLI Configuration</td>
<td>369</td>
</tr>
<tr>
<td>Related Topics</td>
<td>370</td>
</tr>
<tr>
<td>Configuring PAP on the Dialer Interface</td>
<td>370</td>
</tr>
<tr>
<td>J-Web Configuration</td>
<td>370</td>
</tr>
<tr>
<td>CLI Configuration</td>
<td>371</td>
</tr>
<tr>
<td>Related Topics</td>
<td>371</td>
</tr>
<tr>
<td>Configuring CHAP on the Dialer Interface</td>
<td>371</td>
</tr>
<tr>
<td>J-Web Configuration</td>
<td>372</td>
</tr>
<tr>
<td>CLI Configuration</td>
<td>372</td>
</tr>
<tr>
<td>Related Topics</td>
<td>373</td>
</tr>
<tr>
<td>Configuring the Dialer Interface as a Backup WAN Connection</td>
<td>373</td>
</tr>
<tr>
<td>J-Web Configuration</td>
<td>373</td>
</tr>
<tr>
<td>CLI Configuration</td>
<td>373</td>
</tr>
<tr>
<td>Related Topics</td>
<td>374</td>
</tr>
<tr>
<td>Configuring Dialer Watch for the 3G Wireless Modem Interface</td>
<td>374</td>
</tr>
<tr>
<td>J-Web Configuration</td>
<td>374</td>
</tr>
<tr>
<td>CLI Configuration</td>
<td>374</td>
</tr>
<tr>
<td>Related Topics</td>
<td>375</td>
</tr>
<tr>
<td>Configuring Dialer Filter for the 3G Wireless Modem Interface</td>
<td>375</td>
</tr>
<tr>
<td>J-Web Configuration</td>
<td>375</td>
</tr>
<tr>
<td>CLI Configuration</td>
<td>376</td>
</tr>
<tr>
<td>Related Topics</td>
<td>376</td>
</tr>
<tr>
<td>Understanding Account Activation for CDMA EV-DO Cards</td>
<td>376</td>
</tr>
<tr>
<td>Related Topics</td>
<td>378</td>
</tr>
<tr>
<td>Activating the CDMA EV-DO Modem Card with OTASP Provisioning</td>
<td>378</td>
</tr>
<tr>
<td>CLI Operational Mode Command</td>
<td>378</td>
</tr>
<tr>
<td>Activating the CDMA EV-DO Modem Card Manually</td>
<td>379</td>
</tr>
<tr>
<td>CLI Operational Mode Command</td>
<td>380</td>
</tr>
<tr>
<td>Related Topics</td>
<td>380</td>
</tr>
<tr>
<td>Activating the CDMA EV-DO Modem Card with IOTA Provisioning</td>
<td>380</td>
</tr>
<tr>
<td>CLI Operational Mode Command</td>
<td>381</td>
</tr>
<tr>
<td>Unlocking the GSM 3G Wireless Modem</td>
<td>381</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Verifying Link Services CoS</td>
<td>437</td>
</tr>
<tr>
<td>Frequently Asked Questions About the Link Services Interface</td>
<td>439</td>
</tr>
<tr>
<td>Which CoS Components Are Applied to the Constituent Links?</td>
<td>439</td>
</tr>
<tr>
<td>What Causes Jitter and Latency on the Multilink Bundle?</td>
<td>440</td>
</tr>
<tr>
<td>Are LFI and Load Balancing Working Correctly?</td>
<td>441</td>
</tr>
<tr>
<td>Why Are Packets Dropped on a PVC Between a J Series Device and Another Vendor?</td>
<td>447</td>
</tr>
</tbody>
</table>

Chapter 15

Aggregated Ethernet

Aggregated Ethernet Overview ................................................................. 449
Related Topics ..................................................................................... 450
Configuring Aggregated Ethernet Interfaces ......................................... 450
  Configuring the Number of Aggregated Ethernet Interfaces on the Device | 451
  Associating Physical Interfaces with Aggregated Ethernet Interfaces ... 452
  Configuring Aggregated Ethernet Link Speed .................................... 452
  Configuring Aggregated Ethernet Minimum Links ................................ 453
  Deleting Aggregated Ethernet Interfaces ....................................... 453
Related Topics ..................................................................................... 454
Understanding Chassis Cluster Redundant Ethernet Interface Link Aggregation Groups ............................................................. 454
Related Topics ..................................................................................... 454
Understanding the Link Aggregation Control Protocol ............................ 455
Related Topics ..................................................................................... 456
Understanding LACP in Chassis Cluster Mode ........................................ 456
Related Topics ..................................................................................... 457
Configuring LACP on Stand-Alone Devices .......................................... 457
  Configuring LACP ........................................................................... 457
  Configuring the Link Aggregation Control PDU Transmit Interval .......... 457
  Related Topics ............................................................................... 458
Configuring LACP on Chassis Clusters ................................................ 458
  Configuring LACP ........................................................................... 458
  Configuring the Link Aggregation Control PDU Transmit Interval .......... 458
  Related Topics ............................................................................... 459
Verifying Aggregated Ethernet Interfaces .......................................... 459
  Verifying Aggregated Ethernet Interfaces (terse) .............................. 459
  Verifying Aggregated Ethernet Interfaces (extensive) ....................... 460
  Verifying LACP Statistics ................................................................. 461
  Verifying LACP Aggregated Ethernet Interfaces ................................ 461
  Verifying LACP Redundant Ethernet Interfaces .................................. 462
### Table of Contents

#### Part 2 Routing Protocols

**Chapter 16 Routing Overview**

- Routing Overview .......................................................................................... 467
- Networks and Subnetworks ........................................................................... 468
- Autonomous Systems ................................................................................. 468
- Interior and Exterior Gateway Protocols .................................................. 468
- Routing Tables .............................................................................................. 468
- Forwarding Tables ......................................................................................... 469
- Dynamic and Static Routing ........................................................................ 470
- Route Advertisements ................................................................................. 470
- Route Aggregation ......................................................................................... 471

**Chapter 17 Static Routing**

- Static Routing Configuration Overview ...................................................... 475
- Basic Static Routes ......................................................................................... 476
- Understanding Basic Static Routing ............................................................ 476
- Example: Configuring a Basic Set of Static Routes (CLI) ......................... 476
- Static Route Selection ................................................................................... 477
- Understanding Static Route Preferences and Qualified Next Hops.......... 477
- Example: Controlling Static Route Selection (CLI) ..................................... 478
- Static Route Control in Routing and Forwarding Tables .......................... 480
- Understanding Static Route Control in Routing and Forwarding Tables...
  - Route Retention .......................................................................................... 480
  - Readvertisement Prevention ...................................................................... 481
  - Forced Rejection of Passive Route Traffic .............................................. 481
- Example: Controlling Static Routes in the Routing and Forwarding Tables
  (CLI) ........................................................................................................... 481
- Default Static Route Behavior ...................................................................... 482
- Understanding Static Routing Default Properties .................................... 482
- Example: Defining Default Behavior for All Static Routes (CLI) ............. 483
- Verifying the Static Route Configuration .................................................... 483

**Chapter 18 RIP**

- RIP Overview ............................................................................................... 485
- Distance-Vector Routing Protocols .............................................................. 485
- Maximizing Hop Count ................................................................................ 486
- RIP Packets ................................................................................................... 486
- Split Horizon and Poison Reverse Efficiency Techniques ....................... 487
- Limitations of Unidirectional Connectivity ............................................... 488
- RIPng Overview ........................................................................................... 489
- RIPng Protocol Overview ........................................................................... 489
- RIPng Standards .......................................................................................... 490
Chapter 19  OSPF  503

OSPF Overview ................................................................. 503
OSPF Configuration Overview .......................................... 504
OSPF Designated Routers .................................................. 506
   Understanding OSPF Designated Routers ......................... 506
   Example: Configuring the OSPF Router Identifier (CLI) .......... 506
   Example: Controlling OSPF Designated Router Election (CLI) .... 507
OSPF Areas, Area Border Routers, and Backbone Areas ........ 508
   Understanding OSPF Areas, Area Border Routers, and Backbones ... 508
   Example: Configuring a Single-Area OSPF Network (CLI) ...... 509
   Example: Configuring a Multiarea OSPF Network (CLI) .......... 511
      Creating the Backbone Area ........................................... 511
      Creating Additional OSPF Areas .................................... 511
      Configuring Area Border Routers .................................... 512
OSPF Stub Areas and Not-So-Stubby Areas ......................... 513
   Understanding OSPF Stub Areas and Not-So-Stubby Areas ....... 513
   Example: Configuring OSPF Stub and Not-So-Stubby Areas (CLI) 514
OSPF Authentication ......................................................... 515
   Understanding OSPF Authentication .................................... 515
   Example: Enabling Authentication for OSPF Exchanges (CLI) ... 516
OSPF Traffic Control ........................................................ 517
   Understanding OSPF Traffic Control ................................... 517
   Example: Controlling the Cost of Individual OSPF Network Segments (CLI) ........................................................ 518
   Example: Controlling OSPF Route Selection in the Forwarding Table (CLI) ......................................................... 519
Verifying an OSPF Configuration ....................................... 519
   Verifying OSPF-Enabled Interfaces ..................................... 519
   Verifying OSPF Neighbors ............................................... 520
   Verifying the Number of OSPF Routes ................................. 521
   Verifying Reachability of All Hosts in an OSPF Network ........ 522
<table>
<thead>
<tr>
<th>Chapter 20</th>
<th>IS-IS</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS-IS Overview</td>
<td>525</td>
</tr>
<tr>
<td>IS-IS Areas</td>
<td>525</td>
</tr>
<tr>
<td>System Identifier Mapping</td>
<td>526</td>
</tr>
<tr>
<td>ISO Network Addresses</td>
<td>526</td>
</tr>
<tr>
<td>IS-IS Path Selection</td>
<td>527</td>
</tr>
<tr>
<td>Protocol Data Units</td>
<td>527</td>
</tr>
<tr>
<td>IS-IS Hello PDU</td>
<td>527</td>
</tr>
<tr>
<td>Link-State PDU</td>
<td>528</td>
</tr>
<tr>
<td>Complete Sequence Number PDU</td>
<td>528</td>
</tr>
<tr>
<td>Partial Sequence Number PDU</td>
<td>528</td>
</tr>
<tr>
<td>IS-IS Configuration Overview</td>
<td>529</td>
</tr>
<tr>
<td>Example: Configuring IS-IS (CLI)</td>
<td>529</td>
</tr>
<tr>
<td>IS-IS Designated Routers</td>
<td>530</td>
</tr>
<tr>
<td>Understanding IS-IS Designated Routers</td>
<td>530</td>
</tr>
<tr>
<td>Configuring IS-IS Designated Routers (CLI Procedure)</td>
<td>531</td>
</tr>
<tr>
<td>Verifying the IS-IS Configuration</td>
<td>531</td>
</tr>
<tr>
<td>Verifying IS-IS Interface Configuration</td>
<td>531</td>
</tr>
<tr>
<td>Verifying IS-IS Interface Configuration Detail</td>
<td>532</td>
</tr>
<tr>
<td>Verifying IS-IS Adjacencies</td>
<td>533</td>
</tr>
<tr>
<td>Verifying IS-IS Adjacencies in Detail</td>
<td>533</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 21</th>
<th>BGP</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Overview</td>
<td>535</td>
</tr>
<tr>
<td>BGP Messages for Session Establishment</td>
<td>535</td>
</tr>
<tr>
<td>BGP Messages for Session Maintenance</td>
<td>536</td>
</tr>
<tr>
<td>IBGP and EBGP</td>
<td>536</td>
</tr>
<tr>
<td>Route Selection</td>
<td>537</td>
</tr>
<tr>
<td>Local Preference</td>
<td>538</td>
</tr>
<tr>
<td>AS Path</td>
<td>539</td>
</tr>
<tr>
<td>Origin</td>
<td>539</td>
</tr>
<tr>
<td>Multiple Exit Discriminator</td>
<td>540</td>
</tr>
<tr>
<td>Default MED Usage</td>
<td>540</td>
</tr>
<tr>
<td>Additional MED Options for Path Selection</td>
<td>541</td>
</tr>
<tr>
<td>Scaling BGP for Large Networks</td>
<td>542</td>
</tr>
<tr>
<td>BGP Configuration Overview</td>
<td>542</td>
</tr>
<tr>
<td>BGP Peering Sessions</td>
<td>543</td>
</tr>
<tr>
<td>Understanding BGP Peering Sessions</td>
<td>543</td>
</tr>
<tr>
<td>Example: Configuring BGP Point-to-Point Peering Sessions (CLI)</td>
<td>544</td>
</tr>
<tr>
<td>Example: Configuring Internal BGP Peering Sessions (CLI)</td>
<td>545</td>
</tr>
<tr>
<td>BGP Route Reflectors</td>
<td>547</td>
</tr>
<tr>
<td>Understanding BGP Route Reflectors</td>
<td>547</td>
</tr>
<tr>
<td>Example: Configuring a Route Reflector (CLI)</td>
<td>549</td>
</tr>
</tbody>
</table>
### Chapter 22 Multicast

**Multicast Overview** ............................................................ 559
**Multicast Architecture** .................................................. 560
- Upstream and Downstream Interfaces ................................ 560
- Subnetwork Leaves and Branches .................................... 560
- Multicast IP Address Ranges ........................................... 561
- Notation for Multicast Forwarding States ....................... 561
**Dense and Sparse Routing Modes** ............................... 561
**Strategies for Preventing Routing Loops** .................. 562
- Reverse-Path Forwarding for Loop Prevention .................. 562
- Shortest-Path Tree for Loop Prevention .......................... 562
- Administrative Scoping for Loop Prevention .................. 563
**Multicast Protocol Building Blocks** ............................. 563
**Multicast Configuration Overview** ................................. 565
**SAP and SDP Multicast Session Announcements** .......... 566
- Example: Configuring SAP and SDP to Listen for Session Announcements (CLI) ........................................ 567
**Multicast IGMP** ............................................................... 567
- Understanding IGMP and Multicast ............................... 567
- Example: Configuring IGMP for Multicast (CLI) ............... 568
**Multicast PIM and Static RPs** ......................................... 569
- Understanding PIM and Static RPs ............................... 569
- Example: Configuring PIM Sparse Mode and RP Static IP Addresses (CLI) ........................................ 569
**PIM Register Messages** ................................................ 570
- Understanding PIM Register Messages .......................... 571
- Example: Rejecting Incoming PIM Register Messages on an RP Router (CLI) ........................................ 571
- Example: Stopping Outgoing PIM Register Messages on a Designated Router (CLI) ........................................ 572
**PIM RPF Routing Tables** ................................................ 573
- Understanding PIM RPF Routing Tables ........................ 573
- Example: Configuring a PIM RPF Routing Table (CLI) .... 574
**Verifying a Multicast Configuration** .............................. 575
- Verifying SAP and SDP Addresses and Ports .................. 575
- Verifying the IGMP Version ........................................... 576
- Verifying the PIM Mode and Interface Configuration ....... 576
- Verifying the PIM RP Configuration .............................. 577
- Verifying the RPF Routing Table Configuration ............... 577
# Part 3

## Routing Policies and Stateless Firewall Filters

### Chapter 23  Routing Policies  581

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Policies Overview</td>
<td>581</td>
</tr>
<tr>
<td>Routing Policies Configuration Overview</td>
<td>582</td>
</tr>
<tr>
<td>Routing Policies</td>
<td>583</td>
</tr>
<tr>
<td>Understanding Routing Policies</td>
<td>583</td>
</tr>
<tr>
<td>Example: Creating a Routing Policy</td>
<td>583</td>
</tr>
<tr>
<td>Routing Policy Terms</td>
<td>584</td>
</tr>
<tr>
<td>Understanding Routing Policy Terms</td>
<td>585</td>
</tr>
<tr>
<td>Example: Creating a Routing Policy Term</td>
<td>585</td>
</tr>
<tr>
<td>Routing Policy Match Conditions and Actions</td>
<td>586</td>
</tr>
<tr>
<td>Understanding Routing Policy Match Conditions and Actions</td>
<td>587</td>
</tr>
<tr>
<td>Match Conditions</td>
<td>587</td>
</tr>
<tr>
<td>Actions</td>
<td>588</td>
</tr>
<tr>
<td>Route-Based Match Conditions</td>
<td>591</td>
</tr>
<tr>
<td>Understanding Route-Based Match Conditions</td>
<td>591</td>
</tr>
<tr>
<td>Example: Rejecting Known Invalid Routes</td>
<td>592</td>
</tr>
<tr>
<td>Example: Grouping Source and Destination Prefixes into a Forwarding Class</td>
<td>594</td>
</tr>
<tr>
<td>Protocol-Based Match Conditions</td>
<td>596</td>
</tr>
<tr>
<td>Understanding Protocol-Based Match Conditions</td>
<td>596</td>
</tr>
<tr>
<td>Example: Injecting OSPF Routes into the BGP Routing Table</td>
<td>597</td>
</tr>
<tr>
<td>Autonomous System Path-Based Actions</td>
<td>599</td>
</tr>
<tr>
<td>Understanding Autonomous System Path-Based Actions</td>
<td>599</td>
</tr>
<tr>
<td>Example: Configuring a Routing Policy to Prepend the AS Path</td>
<td>600</td>
</tr>
<tr>
<td>Routing Policy Damping Parameters</td>
<td>602</td>
</tr>
<tr>
<td>Understanding Damping Parameters</td>
<td>602</td>
</tr>
<tr>
<td>Example: Configuring Damping Parameters</td>
<td>603</td>
</tr>
</tbody>
</table>

### Chapter 24  Stateless Firewall Filters  607

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stateless Firewall Filter Overview</td>
<td>607</td>
</tr>
<tr>
<td>Stateless Firewall Filter Configuration Overview</td>
<td>608</td>
</tr>
<tr>
<td>Stateless Firewall Filter Terms</td>
<td>609</td>
</tr>
<tr>
<td>Understanding Stateless Firewall Filter Terms</td>
<td>609</td>
</tr>
<tr>
<td>Stateless Firewall Filter Match Conditions</td>
<td>610</td>
</tr>
<tr>
<td>Stateless Firewall Filter Actions and Action Modifiers</td>
<td>615</td>
</tr>
<tr>
<td>Trusted Source Stateless Firewall Filters</td>
<td>618</td>
</tr>
<tr>
<td>Understanding Trusted Source Stateless Firewall Filters</td>
<td>618</td>
</tr>
<tr>
<td>Example: Configuring a Stateless Firewall Filter to Accept Traffic from Trusted Sources</td>
<td>618</td>
</tr>
<tr>
<td>Flood Prevention Stateless Firewall Filters</td>
<td>623</td>
</tr>
<tr>
<td>Understanding Flood Prevention Stateless Firewall Filters</td>
<td>624</td>
</tr>
<tr>
<td>Example: Configuring a Stateless Firewall Filter to Protect Against TCP and ICMP Floods</td>
<td>624</td>
</tr>
</tbody>
</table>
Configuring Enhanced Switching Mode Features .........................................657
  Configuring VLANs—Quick Configuration .............................................657
  Configuring a Spanning Tree—Quick Configuration ..............................660
  Configuring LACP in J-Web .................................................................663
  Configuring 802.1X Features .................................................................666
    Configuring Authentication Features (J-Web) ..................................666
    Specifying RADIUS Server Connections on an SRX Series or J Series
      Device (CLI) ...................................................................................669
    Configuring 802.1X Interface Settings (CLI) ....................................670
    Example: Configuring a Guest VLAN (CLI) ....................................670
  Configuring IGMP Snooping—Quick Configuration ..............................671
  Configuring GVRP—Quick Configuration ............................................673

Chapter 26 Configuring Layer 2 Bridging and Transparent Mode 675

Layer 2 Bridging and Transparent Mode Overview ......................................676
  Related Topics ......................................................................................676
Understanding Bridge Domains ...............................................................677
  Layer 2 Bridging Exceptions on SRX Series Devices ................................678
  Layer 2 Bridging Terms ........................................................................678
  Related Topics ......................................................................................679
Understanding Transparent Mode Conditions ............................................679
  Related Topics ......................................................................................680
Understanding Layer 2 Interfaces .............................................................680
  Related Topics ......................................................................................680
Configuring Bridge Domains .................................................................680
  J-Web Configuration ............................................................................681
  CLI Configuration ..................................................................................682
  Related Topics ......................................................................................682
Configuring Layer 2 Logical Interfaces .....................................................682
  J-Web Configuration ............................................................................683
  CLI Configuration ..................................................................................683
  Related Topics ......................................................................................684
Understanding Layer 2 Security Zones .....................................................684
  Related Topics ......................................................................................685
Understanding Security Policies in Transparent Mode ...............................685
  Related Topics ......................................................................................686
Creating Layer 2 Security Zones .............................................................686
  J-Web Configuration ............................................................................686
  CLI Configuration ..................................................................................687
  Related Topics ......................................................................................687
Configuring Security Policies for Transparent Mode ....................................687
  J-Web Configuration ............................................................................688
  CLI Configuration ..................................................................................689
  Related Topics ......................................................................................689
Understanding VLAN Retagging ..............................................................689
  Related Topics ......................................................................................690
Configuring VLAN Retagging .................................................................690
  J-Web Configuration ............................................................................690
  CLI Configuration ..................................................................................691
Part 5  MPLS

Chapter 27  MPLS

MPLS Overview ................................................................. 709
  Label Switching ............................................................ 710
  Label-Switched Paths ..................................................... 710
  Label-Switching Routers .................................................. 711
  Labels .............................................................................. 712
  Label Operations ........................................................... 712
  Penultimate Hop Popping .................................................. 713
Part 6  Configuring Class of Service

Chapter 32 Class of Service Overview

CoS Terms ............................................................... 790
Benefits of CoS ....................................................... 791
CoS Across the Network .......................................... 792
JUNOS CoS Components ........................................ 793
  Code-Point Aliases .................................................. 793
  Classifiers .......................................................... 793
    Behavior Aggregate Classifiers ................................ 793
    Multifield Classifiers ........................................... 795
  Forwarding Classes ............................................... 796
  Loss Priorities ..................................................... 796
  Forwarding Policy Options ...................................... 797
  Transmission Queues ............................................. 797
  Schedulers .......................................................... 797
    Transmit Rate ..................................................... 798
    Delay Buffer Size ............................................... 798
    Scheduling Priority ............................................ 799
    Shaping Rate ..................................................... 799
    RED Drop Profiles ............................................ 799
    Default Drop Profiles ......................................... 800
  Virtual Channels ................................................ 800
  Policers for Traffic Classes .................................... 801
  Rewrite Rules ..................................................... 801
How CoS Components Work ..................................... 801
  CoS Process on Incoming Packets ......................... 802
  CoS Process on Outgoing Packets ......................... 803
Default CoS Settings ............................................. 803
  Default CoS Values and Aliases .............................. 804
  Forwarding Class Queue Assignments .................... 806
  Scheduler Settings .............................................. 807
Chapter 33 Configuring Class of Service 815

Before You Begin ................................................................. 816
Configuring CoS (J-Web Procedure) ............................................................. 816
Defining CoS Value Aliases ................................................................... 817
Defining Forwarding Classes ................................................................... 819
Defining Classifiers ............................................................................... 820
Defining Rewrite Rules .......................................................................... 822
Defining Schedulers .............................................................................. 824
Defining Scheduler Maps ...................................................................... 827
Defining Drop Profiles .......................................................................... 828
Defining Virtual Channel Groups .......................................................... 829
Assigning CoS Components to Interfaces ......................................... 831
Configuring CoS Components with a Configuration Editor .............. 833
Configuring a Policer for a Firewall Filter ........................................... 834
Configuring and Applying a Firewall Filter for a Multifield Classifier .... 835
Assigning Forwarding Classes to Output Queues ................................. 838
Configuring Forwarding Classes ......................................................... 840
Assigning a Forwarding Class to an Interface .................................... 840
Example: Configuring Up to Eight Forwarding Classes ............... 841
Configuring and Applying Rewrite Rules ............................................. 845
Configuring and Applying Behavior Aggregate Classifiers ............. 848
Example: Defining Aliases for Bits ................................................... 852
Configuring RED Drop Profiles for Congestion Control ............... 854
Example: Configuring RED Drop Profiles ........................................ 856
Configuring Schedulers ......................................................................... 857
Configuring and Applying Scheduler Maps ......................................... 860
Scheduler Maps: Sample Configuration ............................................. 863
Schedulers: Sample Configuration ...................................................... 863
Configuring and Applying Virtual Channels ..................................... 864
Configuring and Applying an Adaptive Shaper ................................. 868
Configuring Virtual Channels ............................................................. 869
Configuring CoS Virtual Channels ....................................................... 870
Creating a List of Virtual Channel Names ......................................... 871
Defining a Virtual Channel Group ....................................................... 871
Applying a Virtual Channel Group to a Logical Interface .................... 872
Selecting Traffic to Be Transmitted from a Particular Virtual Channel ... 873
Example: Configuring Virtual Channels ............................................ 873
Configuring Adaptive Shaping for Frame Relay ...........................................875
Configuring an Adaptive Shaper .................................................................876
Applying an Adaptive Shaper to a Logical Interface ..............................876
Classifying Frame Relay Traffic ...............................................................876
Assigning the Default Frame Relay Loss Priority Map to an Interface ....877
Defining a Custom Frame Relay Loss Priority Map .................................877
Applying the Map to a Logical Interface ..................................................877
Verifying Your Configuration ..................................................................878
Rewriting Frame Relay Headers ...............................................................878
Assigning the Default Frame Relay Rewrite Rule to an Interface ..........878
Defining a Custom Frame Relay Rewrite Rule ..........................................879
Applying the Rule to a Logical Interface .................................................879
Configuring Strict-High Priority ...............................................................879
Example: Configuring Strict High Priority Using the CLI .......................881
Example: Configuring Priority Scheduling ..............................................883
Configuring CoS for Tunnels ....................................................................884
Configuring CoS Queuing for Tunnels with a Configuration Editor ........885
Preserving the ToS Value of a Tunneled Packet .......................................887
Example: Configuring CoS for GRE/IPIP tunnels ...................................888
Restrictions on CoS Shapers ....................................................................893
Configuring Strict High Priority for Queuing with a Configuration Editor ..893
Configuring Large Delay Buffers with a Configuration Editor ...............900
Maximum Delay Buffer Sizes Available to Channelized T1/E1 Interfaces .................................................................900
Delay Buffer Size Allocation Methods ......................................................901
Specifying Delay Buffer Sizes for Queues ..............................................902
Configuring a Large Delay Buffer on a non-Channelized T1 Interface ....903
Configuring a Large Delay Buffer on a Channelized T1 Interface ..........904
Applying an Ingress Interface Policer .........................................................906
Configuring Simple Filters and Policers ...................................................907
Configuring a Simple Filter ....................................................................907
Applying a Simple Filter ........................................................................908
Configuring Policers ................................................................................909
Example: Applying a Two-Rate Tricolor Marking Policer to a Firewall Filter .................................................................909
Configuring CoS Hierarchical Schedulers ...............................................910
Hierarchical Scheduler Terminology .......................................................912
SRX3400 and SRX3600 Device Hardware Capabilities and Limitations ....913
Configuring an Interface Set ....................................................................915
Applying an Interface Set .......................................................................916
Interface Set Caveats ...............................................................................916
Introduction to Hierarchical Schedulers ..................................................917
Scheduler Hierarchy Example .................................................................918
Interfaces for the Hierarchical Example .................................................919
Traffic Control Profiles for the Hierarchical Example ..........................920
Schedulers for the Hierarchical Example ................................................921
Drop Profiles for the Hierarchical Example ..........................................922
Scheduler Maps for the Hierarchical Example .......................................922
Applying Traffic Control Profiles for the Hierarchical Example ..........922
Part 8

Index

Index ...........................................................................................................969
About This Guide

This preface provides the following guidelines for using the *JUNOS Software Interfaces and Routing Configuration Guide*:

- J Series and SRX Series Documentation and Release Notes on page xxxvii
- Objectives on page xxxviii
- Audience on page xxxviii
- Supported Routing Platforms on page xxxviii
- Document Conventions on page xxxviii
- Documentation Feedback on page xl
- Requesting Technical Support on page xl

### J Series and SRX Series Documentation and Release Notes

For a list of related J Series documentation, see [http://www.juniper.net/techpubs/software/junos-jseries/index-main.html](http://www.juniper.net/techpubs/software/junos-jseries/index-main.html).

For a list of related SRX Series documentation, see [http://www.juniper.net/techpubs/hardware/srx-series-main.html](http://www.juniper.net/techpubs/hardware/srx-series-main.html).

If the information in the latest release notes differs from the information in the documentation, follow the *JUNOS Software 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/](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 JUNOS Software 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 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](http://www.juniper.net/books).
Objectives

This guide contains instructions for configuring the J Series and SRX Series interfaces for basic IP routing with standard routing protocols. It also shows how to create backup ISDN interfaces, configure digital subscriber line (DSL) connections and link services, create stateless firewall filters—also known as access control lists (ACLs)—and configure class-of-service (CoS) traffic classification.

Audience

This manual is designed for anyone who installs, sets up, configures, monitors, or administers a J Series Services Router or an SRX Series Services Gateway running Junos OS. The manual is intended for the following audiences:

- Customers with technical knowledge of and experience with networks and network security, the Internet, and Internet routing protocols
- Network administrators who install, configure, and manage Internet routers

Supported Routing Platforms

This manual describes features supported on J Series Services Routers and SRX Series Services Gateways running Junos OS.

Document Conventions

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>❗️</td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td>🌟</td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
</tbody>
</table>
Table 2 on page xxxix defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold text like this</strong></td>
<td>Represents text that you type.</td>
<td>To enter configuration mode, type the <code>configure</code> command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>user@host&gt; <code>configure</code></td>
</tr>
<tr>
<td><strong>Fixed-width text like this</strong></td>
<td>Represents output that appears on the terminal screen.</td>
<td>user@host&gt; <code>show chassis alarms</code> No alarms currently active</td>
</tr>
<tr>
<td><strong>Italic text like this</strong></td>
<td>■ Introduces important new terms.</td>
<td>■ A policy <code>term</code> is a named structure that defines match conditions and actions.</td>
</tr>
<tr>
<td></td>
<td>■ Identifies book names.</td>
<td>■ <em>Junos System Basics Configuration Guide</em></td>
</tr>
<tr>
<td></td>
<td>■ Identifies RFC and Internet draft titles.</td>
<td>■ RFC 1997, <em>BGP Communities Attribute</em></td>
</tr>
<tr>
<td><strong>Italic text like this</strong></td>
<td>Represents variables (options for which you substitute a value) in commands or configuration statements.</td>
<td>Configure the machine’s domain name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[edit] root@# <code>set system domain-name domain-name</code></td>
</tr>
<tr>
<td><strong>Plain text like this</strong></td>
<td>Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.</td>
<td>■ To configure a stub area, include the stub statement at the <code>[edit protocols ospf area area-id]</code> hierarchy level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ The console port is labeled <code>CONSOLE</code>.</td>
</tr>
<tr>
<td><code>&lt; &gt;</code> (angle brackets)</td>
<td>Enclose optional keywords or variables.</td>
<td><code>stub &lt;default-metric metric&gt;;</code></td>
</tr>
<tr>
<td>`</td>
<td>` (pipe symbol)</td>
<td>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.</td>
</tr>
<tr>
<td><code>#</code> (pound sign)</td>
<td>Indicates a comment specified on the same line as the configuration statement to which it applies.</td>
<td><code>rsvp { # Required for dynamic MPLS only</code></td>
</tr>
<tr>
<td><code>[ ]</code> (square brackets)</td>
<td>Enclose a variable for which you can substitute one or more values.</td>
<td><code>community name members [ community-ids ]</code></td>
</tr>
</tbody>
</table>
Table 2: Text and Syntax Conventions (continued)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indention and braces ( { } )</td>
<td>Identify a level in the configuration hierarchy</td>
<td>[edit] routing-options {</td>
</tr>
<tr>
<td></td>
<td></td>
<td>static {</td>
</tr>
<tr>
<td>; (semicolon)</td>
<td>Identifies a leaf statement at a configuration</td>
<td>route default {</td>
</tr>
<tr>
<td></td>
<td>hierarchy level</td>
<td>nexthop address;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>retain;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>

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.

■ 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/](http://www.juniper.net/customers/support/)
- Search for known bugs: [http://www2.juniper.net/kb/](http://www2.juniper.net/kb/)
- Find product documentation: [http://www.juniper.net/techpubs/](http://www.juniper.net/techpubs/)
- Find solutions and answer questions using our Knowledge Base: [http://kb.juniper.net/](http://kb.juniper.net/)
- Download the latest versions of software and review release notes: [http://www.juniper.net/customers/csc/software/](http://www.juniper.net/customers/csc/software/)
- Search technical bulletins for relevant hardware and software notifications: [https://www.juniper.net/alerts/](https://www.juniper.net/alerts/)
- Join and participate in the Juniper Networks Community Forum: [http://www.juniper.net/company/communities/](http://www.juniper.net/company/communities/)
- Open a case online in the CSC Case Management tool: [http://www.juniper.net/cm/](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/](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/](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](http://www.juniper.net/support/requesting-support.html)
Part 1
Configuring Router Interfaces

- Interfaces Overview on page 3
- Configuring Ethernet, DS1, DS3, and Serial Interfaces on page 81
- Configuring Channelized T1/E1/ISDN PRI Interfaces on page 117
- Configuring Digital Subscriber Line Interfaces on page 133
- Configuring G.SHDSL Interfaces on page 165
- Configuring DOCSIS Mini-PIM Interfaces on page 181
- Configuring VDSL2 Interface on page 189
- Configuring 2-Port 10 Gigabit Ethernet XPIM on page 227
- Voice over Internet Protocol with Avaya on page 237
- Configuring Point-to-Point Protocol over Ethernet on page 289
- Configuring ISDN on page 309
- Configuring 3G Wireless Modems for WAN Connections on page 355
- Configuring USB Modems for Dial Backup on page 383
- Configuring Link Services Interfaces on page 399
- Aggregated Ethernet on page 449
Chapter 1

Interfaces Overview

J Series Services Routers and SRX Series Service Gateways support a variety of interface types.

To configure and monitor J Series or SRX Series device interfaces, you need to understand their media characteristics, as well as physical and logical properties such as IP addressing, link-layer protocols, and link encapsulation.

For more information about interfaces, see the Junos Network Interfaces Configuration Guide, the Junos Services Interfaces Configuration Guide, and the Junos Interfaces Command Reference.

For information about which devices support the features documented in this chapter, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.

This chapter contains the following topics:

- Interfaces Terms on page 4
- Network Interfaces on page 8
- Data Link Layer Overview on page 14
- Ethernet Interface Overview on page 15
- T1 and E1 Interfaces Overview on page 19
- Channelized T1/E1/ISDN PRI Interfaces Overview on page 23
- T3 and E3 Interfaces Overview on page 23
- Serial Interface Overview on page 28
- ADSL Interface Overview on page 34
- SHDSL Interface Overview on page 38
- G.SHDSL Mini-PIM on page 39
- VDSL2 Interface Overview on page 41
- DOCSIS Mini-PIM Interface Overview on page 45
- 2-Port 10 Gigabit Ethernet XPIM Overview on page 47
- ISDN Interface Overview on page 49
- Interface Physical Properties on page 52
- Physical Encapsulation on an Interface on page 57
To understand interfaces, become familiar with the terms defined in Table 3 on page 4.

**Table 3: Network Interfaces Terms**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>10GBASE-T or IEEE 802.3an</td>
<td>Standard Ethernet specification that provides 10 Gbps connections over unshielded or shielded twisted pair cables.</td>
</tr>
<tr>
<td>1000BASE-T IEEE 802.3ab</td>
<td>Standard Ethernet specification that provides 1 Gbps connections over twisted pair.</td>
</tr>
<tr>
<td>100BASE-T IEEE 802.3u</td>
<td>Standard Ethernet specification that provides 100 Mbps connections over twisted pair.</td>
</tr>
<tr>
<td>alternate mark inversion (AMI)</td>
<td>Original method of formatting T1 and E1 data streams.</td>
</tr>
<tr>
<td>asymmetric digital subscriber line (ADSL) interface</td>
<td>Physical WAN interface for connecting a J Series device to a digital subscriber line access multiplexer (DSLAM). An ADSL interface allocates line bandwidth asymmetrically with downstream (provider-to-customer) data rates of up to 8 Mbps for ADSL, 12 Mbps for ADSL2, and 25 Mbps for ADSL2+, and upstream (customer-to-provider) rates of up to 800 Kbps for ADSL and 1 Mbps for ADSL2 and ADSL2+, depending on the implementation.</td>
</tr>
<tr>
<td>ADSL2 interface</td>
<td>An ADSL interface that supports ITU-T Standards G.992.3 and G.992.4 and allocates downstream (provider-to-customer) data rates of up to 12 Mbps and upstream (customer-to-provider) rates of up to 1 Mbps.</td>
</tr>
<tr>
<td>ADSL2+ interface</td>
<td>An ADSL interface that supports ITU-T Standard G.992.5 and allocates downstream (provider-to-customer) data rates of up to 25 Mbps and upstream (customer-to-provider) rates of up to 1 Mbps.</td>
</tr>
<tr>
<td>Annex A</td>
<td>ITU-T Standard G.992.1 that defines how ADSL works over plain old telephone service (POTS) lines.</td>
</tr>
<tr>
<td>Annex B</td>
<td>ITU-T Standard G.992.1 that defines how ADSL works over Integrated Services Digital Network (ISDN) lines.</td>
</tr>
<tr>
<td>binary 8-zero substitution (B8ZS)</td>
<td>Improved method of formatting T1 and E1 data streams, in which a special code is substituted whenever 8 consecutive zeros are sent over the link.</td>
</tr>
<tr>
<td>Challenge Handshake Authentication Protocol (CHAP)</td>
<td>Protocol that authenticates remote users. CHAP is a server-driven, three-step authentication method that depends on a shared secret password residing on both the server and the client.</td>
</tr>
<tr>
<td>checksum</td>
<td>See frame checksum sequence.</td>
</tr>
<tr>
<td>channel group</td>
<td>Combination of DS0 interfaces partitioned from a channelized interface into a single logical bundle.</td>
</tr>
<tr>
<td>channel service unit (CSU)</td>
<td>Unit that connects a digital telephone line to a multiplexer or other signal service.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>channelized E1</td>
<td>2.048-Mbps interface that can be configured as a single clear-channel E1 interface or channelized into as many as 31 discrete DS0 interfaces, or up to 30 ISDN PRI B-channels and 1 D-channel. On J Series channelized T1/E1/ISDN PRI interfaces, time slots are numbered from 1 through 31, and time slot 1 is reserved for framing. When the interface is configured for ISDN PRI service, time slot 16 is reserved for the D-channel.</td>
</tr>
<tr>
<td>channelized interface</td>
<td>Interface that is a subdivision of a larger interface, minimizing the number of Physical Interface Modules (PIMs) that an installation requires. On a channelized PIM, each port can be configured as a single clear channel or partitioned into multiple discrete T1, E1, and DS0 interfaces.</td>
</tr>
<tr>
<td>channelized T1</td>
<td>1.544-Mbps interface that can be configured as a single clear-channel T1 interface or channelized into as many as 24 discrete DS0 interfaces, or up to 23 ISDN PRI B-channels and 1 D-channel. When the interface is configured for ISDN PRI service, time slot 24 is reserved for the D-channel.</td>
</tr>
<tr>
<td>Cisco HDLC</td>
<td>Cisco High-level Data Link Control protocol. Proprietary Cisco encapsulation for transmitting LAN protocols over a WAN. HDLC specifies a data encapsulation method on synchronous serial links by means of frame characters and checksums. Cisco HDLC enables the transmission of multiple protocols.</td>
</tr>
<tr>
<td>clock source</td>
<td>Source of the consistent, periodic signal used by a device to synchronize data communication and processing tasks.</td>
</tr>
<tr>
<td>CSU compatibility mode</td>
<td>Subrate on an E3 or T3 interface that allows a J Series device to connect to a channel service unit (CSU) with proprietary multiplexing at the remote end of the line. Subrating an E3 or T3 interface reduces the maximum allowable peak rate by limiting the payload encapsulated by the High-level Data Link Control protocol (HDLC).</td>
</tr>
<tr>
<td>data-link connection identifier (DLCI)</td>
<td>Identifier for a Frame Relay virtual connection, also called a logical interface.</td>
</tr>
<tr>
<td>data service unit (DSU)</td>
<td>Unit that connects a data terminal equipment (DTE) device—in this case, a J Series Services Router or an SRX Series Services Gateway—to a digital telephone line.</td>
</tr>
<tr>
<td>data terminal equipment (DTE)</td>
<td>RS-232 interface that a Juniper Networks device uses to exchange information with a serial device.</td>
</tr>
<tr>
<td>DS1</td>
<td>Digital signal 1, another name for a T1 interface.</td>
</tr>
<tr>
<td>DS3 interface</td>
<td>Digital signal 3, another name for a T3 interface.</td>
</tr>
<tr>
<td>data inversion</td>
<td>Transmission of all data bits in the data stream so that zeros are transmitted as ones and ones are transmitted as zeros. Data inversion is normally used only in alternate mark inversion (AMI) mode to guarantee ones density in the transmitted stream.</td>
</tr>
<tr>
<td>E1 interface</td>
<td>Physical WAN interface for transmitting signals in European digital transmission (E1) format. The E1 signal format carries information at a rate of 2.048 Mbps and can carry 32 channels of 64 Kbps each.</td>
</tr>
<tr>
<td>E3 interface</td>
<td>Physical WAN interface for transmitting 16 E1 circuits over copper wires using time-division multiplexing. E3 is widely used outside of North America and transfers traffic at the rate of 34.368 Mbps.</td>
</tr>
<tr>
<td>encapsulation type</td>
<td>Type of protocol header in which data is wrapped for transmission.</td>
</tr>
</tbody>
</table>
Table 3: Network Interfaces Terms (continued)

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast Ethernet interface</td>
<td>Physical LAN interface for transmitting data at 100 Mbps. Fast Ethernet, also called 100Base-T, additionally supports standard 10Base-T Ethernet transmission. Fast Ethernet is available on both dual-port and 4-port PIMs for the J4350 and J6350 devices.</td>
</tr>
<tr>
<td>FPC</td>
<td>Logical identifier for a Physical Interface Module (PIM) installed on a J Series device. The FPC number used in the JUNOS command-line interface (CLI) and displayed in command output represents the chassis slot in which a PIM is installed.</td>
</tr>
<tr>
<td>fractional E1</td>
<td>Interface that contains one or more of the 32 DS0 time slots that can be reserved from an E1 interface. (Time slot 0 is reserved.)</td>
</tr>
<tr>
<td>fractional T1</td>
<td>Interface that contains one or more of the 24 DS0 time slots that can be reserved from a T1 interface. (Time slot 0 is reserved.)</td>
</tr>
<tr>
<td>frame check sequence (FCS)</td>
<td>Calculation that is added to a frame to control errors in High-level Data Link Control (HDLC), Frame Relay, and other data link layer protocols.</td>
</tr>
<tr>
<td>Frame Relay</td>
<td>An efficient WAN protocol that does not require explicit acknowledgement of each frame of data. Frame Relay allows private networks to reduce costs by sharing facilities between the endpoint switches of a network managed by a Frame Relay service provider. Individual data link connection identifiers (DLCIs) are assigned to ensure that customers receive only their own traffic.</td>
</tr>
<tr>
<td>Gigabit Ethernet interface</td>
<td>Physical LAN or WAN interface for transmitting data at 1000 Mbps. The four built-in ports on J4350 and J6350 devices are Gigabit Ethernet interfaces. Gigabit Ethernet is also available in a single-port copper or optical PIM for these devices. Gigabit Ethernet is also supported in SRX Series devices.</td>
</tr>
<tr>
<td>High-Level Data Link Control</td>
<td>International Telecommunication Union (ITU) standard for a bit-oriented data link layer protocol on which most other bit-oriented protocols are based.</td>
</tr>
<tr>
<td>(HDLC)</td>
<td></td>
</tr>
<tr>
<td>hostname</td>
<td>Name assigned to the device during initial configuration.</td>
</tr>
<tr>
<td>ITU-T G.991.2</td>
<td>International Telecommunication Union standard describing a data transmission method for symmetric high-speed digital subscriber line (SHDSL) as a means for data transport in telecommunications access networks. The standard also describes the functionality required for interoperability of equipment from various manufacturers.</td>
</tr>
<tr>
<td>ITU-T G.992.1</td>
<td>International Telecommunication Union standard that requires the downstream (provider-to-customer) data transmission to consist of full-duplex low-speed bearer channels and simplex high-speed bearer channels. In the upstream (customer-to-provider) transmissions, only low-speed bearer channels are provided.</td>
</tr>
<tr>
<td>ITU-T G.993.2</td>
<td>International Telecommunication Union standard describing a data transmission method for VDSL2 transceivers.</td>
</tr>
<tr>
<td>ITU-T G.994.1</td>
<td>International Telecommunication Union standard describing the types of signals, messages, and procedures exchanged between digital subscriber line (DSL) equipment when the operational modes of equipment need to be automatically established and selected.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td>ITU-T G.997.1</td>
<td>International Telecommunication Union standard describing the physical layer management for asymmetric digital subscriber line (ADSL) transmission systems. The standard specifies the means of communication on a transport transmission channel defined in the physical layer recommendations. In addition, the standard describes the content and syntax of network elements for configuration, fault management, and performance management.</td>
</tr>
<tr>
<td>logical interface</td>
<td>Virtual interface that you create on a physical interface to identify its connection. Creating multiple logical interfaces allows you to associate multiple virtual circuits, data line connections, or virtual LANs (VLANs) with a single interface device.</td>
</tr>
<tr>
<td>maximum transmission unit (MTU)</td>
<td>Maximum or largest segment size that a network can transmit.</td>
</tr>
<tr>
<td>Multilink Frame Relay (MLFR)</td>
<td>Protocol that allows multiple Frame Relay links to be aggregated by inverse multiplexing.</td>
</tr>
<tr>
<td>Multilink Point-to-Point Protocol (MLPPP)</td>
<td>Protocol that allows you to bundle multiple Point-to-Point Protocol (PPP) links into a single logical unit. MLPPP improves bandwidth efficiency and fault tolerance and reduces latency.</td>
</tr>
<tr>
<td>Password Authentication Protocol (PAP)</td>
<td>Authentication protocol that uses a simple 2-way handshake to establish identity.</td>
</tr>
</tbody>
</table>
| Physical Interface Module (PIM) | Network interface card that is fixed or can be interchangeably installed on a J Series device to provide the physical connections to a LAN or WAN, receiving incoming packets and transmitting outgoing packets. A PIM contains one of the following interfaces or sets of interfaces:  
  ■ Single Gigabit Ethernet LAN or WAN interface  
  ■ Two or four Fast Ethernet LAN interfaces  
  ■ Two T1 or two E1 WAN interfaces  
  ■ Single E3 or T3 (DS3) WAN interface (J4350 and J6350 models only)  
  ■ Single asynchronous digital subscriber line (ADSL) WAN interface—Annex A to support ADSL over plain old telephone service (POTS) lines or Annex B to support ADSL over ISDN  
  ■ Four ISDN BRI S/T or U interfaces  
  ■ Two channelized T1/E1/ISDN PRI interfaces  
  ■ Two serial interfaces  
  ■ Symmetric high-speed digital subscriber line (SHDSL) WAN interface—Annex A or Annex B to support ATM-over-SHDSL connections |
| Point-to-Point Protocol (PPP) | Link-layer protocol that provides multiprotocol encapsulation. PPP is used for link-layer and network-layer configuration. |
| Packet Transfer Mode (PTM) | Transport of packet-based services method based on the EFM IEEE802.3AH standard. |
### Table 3: Network Interfaces Terms (continued)

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>serial interface</td>
<td>Physical LAN interface for transmitting data between computing devices. A J Series device has two types of serial interfaces:</td>
</tr>
<tr>
<td>■ Asynchronous serial interface—Console port, with speeds up to 110.5 Kbps. The console port supports an RS-232 (EIA-232) standard serial cable with a 25-pin (DB-25) connector.</td>
<td></td>
</tr>
<tr>
<td>■ Synchronous serial interface—Port that transmits packets to and from, for example, a T1 device or microwave link, at speeds up to 8 Mbps. You cannot use this serial interface to connect a console. J Series device synchronous serial interfaces support RS-232 (EIA-232), RS-422/449 (EIA-449), RS-530 (EIA-530), V.35, and X.21 cable types. For details, see “Serial Line Protocols” on page 31. For cable details, see the J Series Services Routers Hardware Guide.</td>
<td></td>
</tr>
<tr>
<td>SFP +</td>
<td>Fiber optic transceiver module designed for 10-Gigabit Ethernet and 8.5 Gbps fiber channel systems.</td>
</tr>
<tr>
<td>symmetric high-speed digital subscriber line (G.SHDSL)</td>
<td>Physical WAN symmetric DSL interface capable of sending and receiving high-speed symmetrical data streams over a single pair of copper wires at rates between 192 Kbps and 2.31 Mbps. G.SHDSL incorporates features of other DSL technologies such as asymmetric DSL and transports T1, E1, ISDN, Asynchronous Transfer Mode (ATM), and IP signals.</td>
</tr>
<tr>
<td>symmetric high-speed digital subscriber line (SHDSL) transceiver unit—remote (STU–R)</td>
<td>Equipment that provides symmetric high-speed digital subscriber line (SHDSL) connections to remote user terminals such as data terminals or telecommunications equipment.</td>
</tr>
<tr>
<td>T1 interface</td>
<td>Physical WAN interface for transmitting digital signals in the T-carrier system used in the United States, Japan, and Canada. The T1 signal format carries 24 pulse code modulation (PCM) signals using time-division multiplexing (TDM) at an overall rate of 1.544 Mbps.</td>
</tr>
<tr>
<td>T3 interface</td>
<td>Physical WAN interface for transmitting digital signals in the T-carrier system used in the United States, Japan, and Canada. T3 signals are formatted like T1 signals, but carry information at the higher rate of 44.736 Mbps. T3 is also called DS3.</td>
</tr>
<tr>
<td>VDSL2</td>
<td>VDSL2 is an enhancement to G.993.1 (VDSL) that permits the transmission of asymmetric and symmetric (full duplex) aggregate data at faster rate. VDSL2 is based on ITU-T G.993.2 (VDSL2) standard.</td>
</tr>
<tr>
<td>XPIM</td>
<td>Physical Interface Modules (PIMs) that provides 10-Gigabit Ethernet front end interface connection.</td>
</tr>
</tbody>
</table>

### Network Interfaces

All Juniper Networks devices use network interfaces to make physical connections to other devices. A connection takes place along media-specific physical wires through a port on a Physical Interface Module (PIM) installed in the J Series Services Router or an Input/Output Card (IOC) in the SRX Series Services Gateway. Each device interface has a unique name that follows a naming convention.
This section contains the following topics:
- Media Types on page 9
- Network Interface Naming on page 9

Media Types

Each type of interface on a J Series or SRX Series device uses a particular medium to transmit data. The physical wires and data link layer protocols used by a medium determine how traffic is sent. See the Junos OS Feature Support Reference for SRX Series and J Series Devices for a list of media supported on each type of device.

You must configure each network interface before it can operate on the device. Configuring an interface can define both the physical properties of the link and the logical properties of a logical interface on the link.

Network Interface Naming

The interfaces on the J Series and SRX Series devices are used for networking and services. Most interfaces are configurable, but some internally generated interfaces are not configurable. If you are familiar with Juniper Networks M Series and T Series routing platforms, be aware that device interface names are similar to but not identical with the interface names on those routing platforms.

This section contains the following topics:
- Interface Naming Conventions on page 9
- Understanding CLI Output for Interfaces on page 12

Interface Naming Conventions

The unique name of each network interface identifies its type and location and indicates whether it is a physical interface or an optional logical unit created on a physical interface:

- The name of each network interface has the following format to identify the physical device that corresponds to a single physical network connector:

  \texttt{type-slot/pim-or-ioc/port}

- Network interfaces that are fractionalized into time slots include a channel number in the name, preceded by a colon (\texttt{:})

  \texttt{type-slot/pim-or-ioc/port:channel}

- Each logical interface has an additional logical unit identifier, preceded by a period (\texttt{.})

  \texttt{type-slot/pim-or-ioc/port:<channel>.unit}

The parts of an interface name are summarized in Table 4 on page 10.
Table 4: Network Interface Names

<table>
<thead>
<tr>
<th>Name Part</th>
<th>Meaning</th>
<th>Possible Values</th>
</tr>
</thead>
</table>
| type      | Type of network medium that can connect to this interface. | ae—Aggregated Ethernet interface  
at—ATM-over-ADSL or ATM-over-SHDSL WAN interface  
bc—Bearer channel on an ISDN interface  
br—Basic Rate Interface for establishing ISDN connections  
ce1—Channelized E1 interface  
ct1—Channelized T1 interface  
dc—Delta channel on an ISDN interface  
dl—Dialer interface for initiating ISDN and USB modem connections  
e1—E1 WAN interface  
e3—E3 WAN interface  
ze—Fast Ethernet interface  
ge—Gigabit Ethernet interface  
pt—VDSL2 interface  
reth—For chassis cluster configurations only, redundant Ethernet interface  
se—Serial interface (either RS-232, RS-422/499, RS-530, V.35, or X.21)  
t1—T1 (also called DS1) WAN interface  
t3—T3 (also called DS3) WAN interface  
wx—WXC Integrated Services Module (ISM 200) interface for WAN acceleration  
x0—10-Gigabit Ethernet interface |

In addition to these network interfaces, devices can have the following special interfaces: `dsc`, `gr`, `gre`, `ip`, `ipip`, `lo`, `ls`, `lsi`, `lt`, `pd`, `pimd`, `pc`, `pe`, and `pime`, `pp0`, `st`, `tap`, and `umd0`. For more information, see “Special Interfaces” on page 74.
<table>
<thead>
<tr>
<th>Name Part</th>
<th>Meaning</th>
<th>Possible Values</th>
</tr>
</thead>
</table>
| **slot**  | Number of the chassis slot in which a PIM or IOC is installed. | J Series Services Router: The slot number begins at 1 and increases as follows from top to bottom, left to right:  
- J2320 router—Slots 1 to 3  
- J2350 router—Slots 1 to 5  
- J4350 or J6350 router—PIM slots 1 to 6  

The slot number 0 is reserved for the out-of-band management ports. (See “Management Interface” on page 77.)  

SRX5600 and SRX5800 devices: The slot number begins at 0 and increases as follows from left to right, bottom to top:  
- SRX5600 device—Slots 0 to 5  
- SRX5800 device—Slots 0 to 5, 7 to 11  

SRX3400 and SRX3600 devices: The Switch Fabric Board (SFB) is always 0. Slot numbers increase as follows from top to bottom, left to right:  
- SRX3400 device—Slots 0 to 4  
- SRX3600 device—Slots 0 to 6  |
| **pim-or-ioc** | Number of the PIM or IOC on which the physical interface is located. | J Series devices: This number is always 0. Only one PIM can be installed in a slot.  

SRX5600 and SRX5800 devices: For 40-port Gigabit Ethernet IOCs or 4-port 10-Gigabit Ethernet IOCs, this number can be 0, 1, 2, or 3.  

SRX3400 and SRX3600 devices: This number is always 0. Only one IOC can be installed in a slot. |
| **port** | Number of the port on a PIM or IOC on which the physical interface is located. | J Series Services Routers:  
- On a single-port PIM, always 0.  
- On a multiple-port PIM, this number begins at 0 and increases from left to right, bottom to top, to a maximum of 3.  

On SRX5600 and SRX5800 devices:  
- For 40-port Gigabit Ethernet IOCs, this number begins at 0 and increases from left to right to a maximum of 9.  
- For 4-port 10-Gigabit Ethernet IOCs, this number is always 0.  

On SRX3400 and SRX3600 devices:  
- For the SFB built-in copper Gigabit Ethernet ports, this number begins at 0 and increases from top to bottom, left to right, to a maximum of 7. For the SFB built-in fiber Gigabit Ethernet ports, this number begins at 8 and increases from left to right to a maximum of 11.  
- For 16-port Gigabit Ethernet IOCs, this number begins at 0 to a maximum of 15.  
- For 2-port 10-Gigabit Ethernet IOCs, this number is 0 or 1.  

Port numbers appear on the PIM or IOC faceplate. |
Table 4: Network Interface Names (continued)

<table>
<thead>
<tr>
<th>Name Part</th>
<th>Meaning</th>
<th>Possible Values</th>
</tr>
</thead>
</table>
| channel   | Number of the channel (time slot) on a fractional or channelized T1 or E1 interface. | - On an E1 interface, a value from 1 through 31. The 1 time slot is reserved.  
- On a T1 interface, a value from 1 through 24. |
| unit      | Number of the logical interface created on a physical interface. | A value from 0 through 16384.  
If no logical interface number is specified, unit 0 is the default, but must be explicitly configured. For more information about logical interfaces, see “Interface Logical Properties” on page 64. |

For example, the interface name `e1-5/0/0:15.0` on a J Series Services Router represents the following information:
- E1 WAN interface
- PIM slot 5
- PIM number 0 (always 0)
- Port 0
- Channel 15
- Logical interface, or unit, 0

Understanding CLI Output for Interfaces

The JUNOS Software that operates on J Series Services Routers and SRX Series Services Gateways was originally developed for Juniper Networks routing platforms that support many ports, on interface cards called Physical Interface Cards (PICs). On these larger platforms, PICs are installed into slots on Flexible PIC Concentrators (FPCs), and FPCs are installed into slots in the router chassis.

For J Series and SRX Series devices, PIM and IOC slots are detected internally by the JUNOS Software as FPC slots, and the PIM or IOC in each slot is identified as a “PIC.” For example, in the following output, the three PIMs located in slots 0, 2, and 5 are reported as FPC 0, FPC 2, and FPC 5, and PIM 0 is reported as PIC 0:

```
user@host> show chassis hardware
Hardware inventory:

<table>
<thead>
<tr>
<th>Item</th>
<th>Version</th>
<th>Part number</th>
<th>Serial number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis</td>
<td></td>
<td></td>
<td></td>
<td>JN0000192AB</td>
</tr>
<tr>
<td>Midplane</td>
<td>REV 02.04 710-010001</td>
<td>CORE99563</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System I0</td>
<td>REV 02.03 710-010003</td>
<td>CORE100885</td>
<td></td>
<td>System I0 board</td>
</tr>
<tr>
<td>Routing Engine</td>
<td>RevX2.6 750-010005</td>
<td>IWGS40735451</td>
<td></td>
<td>RE-J.2</td>
</tr>
<tr>
<td>FPC 0</td>
<td></td>
<td></td>
<td></td>
<td>FPC</td>
</tr>
<tr>
<td>PIC 0</td>
<td></td>
<td></td>
<td></td>
<td>2x FE</td>
</tr>
<tr>
<td>FPC 2</td>
<td>RevX2.1 750-010355</td>
<td>CORE100458</td>
<td></td>
<td>FPC</td>
</tr>
<tr>
<td>PIC 0</td>
<td></td>
<td></td>
<td></td>
<td>2x T1</td>
</tr>
<tr>
<td>FPC 5</td>
<td>REV 04 750-010353</td>
<td>AF044451744</td>
<td></td>
<td>FPC</td>
</tr>
<tr>
<td>PIC 0</td>
<td></td>
<td></td>
<td></td>
<td>2x FE</td>
</tr>
</tbody>
</table>
```
To understand the abbreviations for PICs that appear in JUNOS CLI output, see Table 5 on page 13. For details, see the J Series Services Routers Hardware Guide.

### Table 5: PIC Abbreviations and Full Names

<table>
<thead>
<tr>
<th>PIC Abbreviation in JUNOS CLI</th>
<th>PIC or IOC Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2x FE</td>
<td>Dual-Port Fast Ethernet PIM</td>
</tr>
<tr>
<td>4x FE</td>
<td>4-Port Fast Ethernet ePIM</td>
</tr>
<tr>
<td>1x GE Copper</td>
<td>Copper Gigabit Ethernet ePIM (1 10-Mbps, 100-Mbps, or 1000-Mbps port)</td>
</tr>
<tr>
<td>1x GE SFP</td>
<td>SFP Gigabit Ethernet ePIM (1 fiber port)</td>
</tr>
<tr>
<td>1x SFP uPIM</td>
<td>1-Port Gigabit Ethernet uPIM</td>
</tr>
<tr>
<td>6x GE SFP uPIM</td>
<td>6-Port SFP Gigabit Ethernet uPIM</td>
</tr>
<tr>
<td>8x GE uPIM</td>
<td>8-Port Gigabit Ethernet uPIM</td>
</tr>
<tr>
<td>16x GE uPIM</td>
<td>16-Port Gigabit Ethernet uPIM</td>
</tr>
<tr>
<td>4x GE Base PIC</td>
<td>4 built-in Gigabit Ethernet ports on a chassis (fixed PIM)</td>
</tr>
<tr>
<td>1x 10GE</td>
<td>1-Port 10-Gigabit Ethernet IOC</td>
</tr>
<tr>
<td>10x 1GE</td>
<td>10-Port Gigabit Ethernet IOC</td>
</tr>
<tr>
<td>2x Serial</td>
<td>Dual-Port Serial PIM</td>
</tr>
<tr>
<td>2x T1</td>
<td>Dual-Port T1 PIM</td>
</tr>
<tr>
<td>2x E1</td>
<td>Dual-Port E1 PIM</td>
</tr>
<tr>
<td>1x T3</td>
<td>T3 PIM (1 port)</td>
</tr>
<tr>
<td>1x E3</td>
<td>E3 PIM (1 port)</td>
</tr>
<tr>
<td>4x BRI S/T</td>
<td>4-Port ISDN BRI S/T PIM</td>
</tr>
<tr>
<td>4x BRI U</td>
<td>4-Port ISDN BRI U PIM</td>
</tr>
<tr>
<td>1x ADSL Annex A</td>
<td>ADSL 2/2 + Annex A PIM (1 port, for POTS)</td>
</tr>
<tr>
<td>1x ADSL Annex B</td>
<td>ADSL 2/2 + Annex B PIM (1 port, for ISDN)</td>
</tr>
<tr>
<td>2x SHDSL (ATM)</td>
<td>G.SHDSL PIM (2-port two-wire mode or 1-port four-wire mode)</td>
</tr>
<tr>
<td>1x VDSL2 Annex A</td>
<td>VDSL2 Annex A Mini-PIM</td>
</tr>
<tr>
<td>Integrated Services Module</td>
<td>WXC Integrated Services Module (ISM 200)</td>
</tr>
<tr>
<td>2x 10G gPIM</td>
<td>2-Port 10-Gigabit Ethernet XPIM</td>
</tr>
</tbody>
</table>
Data Link Layer Overview

The data link layer is Layer 2 in the Open Systems Interconnection (OSI) model. The data link layer is responsible for transmitting data across a physical network link. Each physical medium has link-layer specifications for network and link-layer protocol characteristics such as physical addressing, network topology, error notification, frame sequencing, and flow control.

Physical Addressing

Physical addressing is different from network addressing. Network addresses differentiate between nodes or devices in a network, allowing traffic to be routed or switched through the network. In contrast, physical addressing identifies devices at the link-layer level, differentiating between individual devices on the same physical medium. The primary form of physical addressing is the media access control (MAC) address.

Network Topology

Network topology specifications identify how devices are linked in a network. Some media allow devices to be connected by a bus topology, while others require a ring topology. The bus topology is used by Ethernet technologies, which are supported on Juniper Networks devices.

Error Notification

The data link layer provides error notifications that alert higher-layer protocols that an error has occurred on the physical link. Examples of link-level errors include the loss of a signal, the loss of a clocking signal across serial connections, or the loss of the remote endpoint on a T1 or T3 link.

Frame Sequencing

The frame sequencing capabilities of the data link layer allow frames that are transmitted out of sequence to be reordered on the receiving end of a transmission. The integrity of the packet can then be verified by means of the bits in the Layer 2 header, which is transmitted along with the data payload.

Flow Control

Flow control within the data link layer allows receiving devices on a link to detect congestion and notify their upstream and downstream neighbors. The neighbor devices relay the congestion information to their higher-layer protocols so that the flow of traffic can be altered or rerouted.

Data Link Sublayers

The data link layer is divided into two sublayers: Logical Link Control (LLC) and Media Access Control (MAC). The LLC sublayer manages communications between devices.
over a single link of a network. This sublayer supports fields in link-layer frames that enable multiple higher-layer protocols to share a single physical link.

The MAC sublayer governs protocol access to the physical network medium. Through the MAC addresses that are typically assigned to all ports on a device, multiple devices on the same physical link can uniquely identify one another at the data link layer. MAC addresses are used in addition to the network addresses that are typically configured manually on ports within a network.

**MAC Addressing**

A MAC address is the serial number permanently stored in a device adapter to uniquely identify the device. MAC addresses operate at the data link layer, while IP addresses operate at the network layer. The IP address of a device can change as the device is moved around a network to different IP subnets, but the MAC address remains the same, because it is physically tied to the device.

Within an IP network, devices match each MAC address to its corresponding configured IP address by means of the Address Resolution Protocol (ARP). ARP maintains a table with a mapping for each MAC address in the network.

Most Layer 2 networks use one of three primary numbering spaces—MAC-48, EUI-48 (Extended Unique Identifier), and EUI-64—which are all globally unique. MAC-48 and EUI-48 spaces each use 48-bit addresses, and EUI-64 spaces use a 64-bit addresses, but all three use the same numbering format. MAC-48 addresses identify network hardware, and EUI-48 addresses identify other devices and software.

The Ethernet and ATM technologies supported on devices use the MAC-48 address space. IPv6 uses the EUI-64 address space.

MAC-48 addresses are the most commonly used MAC addresses in most networks. These addresses are 12-digit hexadecimal numbers (48 bits in length) that typically appear in one of the following formats:

- **MM:MM:MM:SS:SS:SS**
- **MM-MM-MM-SS-SS-SS**

The first three octets (**MM:MM:MM** or **MM-MM-MM**) are the ID number of the hardware manufacturer. Manufacturer ID numbers are assigned by the Institute of Electrical and Electronics Engineers (IEEE). The last three octets (**SS:SS:SS** or **SS-SS-SS**) make up the serial number for the device, which is assigned by the manufacturer. For example, an Ethernet interface card might have a MAC address of 00:05:85:c1:a6:a0.

**Ethernet Interface Overview**

Ethernet is a Layer 2 technology that operates in a shared bus topology. Ethernet supports broadcast transmission, uses best-effort delivery, and has distributed access control. Ethernet is a point-to-multipoint technology.

In a shared bus topology, all devices connect to a single, shared physical link through which all data transmissions are sent. All traffic is broadcast, so that all devices within
the topology receive every transmission. The devices within a single Ethernet topology make up a broadcast domain.

Ethernet uses best-effort delivery to broadcast traffic. The physical hardware provides no information to the sender about whether the traffic was received. If the receiving host is offline, traffic to the host is lost. Although the Ethernet data link protocol does not inform the sender about lost packets, higher-layer protocols like TCP/IP might provide this type of notification.

This section contains the following topics:
- Ethernet Access Control and Transmission on page 16
- Collisions and Detection on page 16
- Collision Domains and LAN Segments on page 17
- Broadcast Domains on page 18
- Ethernet Frames on page 18

**Ethernet Access Control and Transmission**

Ethernet’s access control is distributed, because Ethernet has no central mechanism that grants access to the physical medium within the network. Instead, Ethernet uses carrier sense multiple access with collision detection (CSMA/CD). Because multiple devices on an Ethernet network can access the physical medium, or wire, simultaneously, each device must determine whether the physical medium is in use. Each host listens on the wire to determine if a message is being transmitted. If it detects no transmission, the host begins transmitting its own data.

The length of each transmission is determined by fixed Ethernet packet sizes. By fixing the length of each transmission and enforcing a minimum idle time between transmissions, Ethernet ensures that no pair of communicating devices on the network can monopolize the wire and block others from sending and receiving traffic.

**Collisions and Detection**

When a device on an Ethernet network begins transmitting data, the data takes a finite amount of time to reach all hosts on the network. Because of this delay, or latency, in transmitting traffic, a device might detect an idle state on the wire just as another device initially begins its transmission. As a result, two devices might send traffic across a single wire at the same time. When the two electrical signals collide, they become scrambled so that both transmissions are effectively lost.

**Collision Detection**

To handle collisions, Ethernet devices monitor the link while they are transmitting data. The monitoring process is known as collision detection. If a device detects a foreign signal while it is transmitting, it terminates the transmission and attempts to transmit again only after detecting an idle state on the wire. Collisions continue to occur if two colliding devices both wait the same amount of time before retransmitting. To avoid this condition, Ethernet devices use a binary exponential backoff algorithm.
**Backoff Algorithm**

To use the binary exponential backoff algorithm, each device that sent a colliding transmission randomly selects a value within a range. The value represents the number of transmission times that the device must wait before retransmitting its data. If another collision occurs, the range of values is doubled and retransmission takes place again. Each time a collision occurs, the range of values doubles, to reduce the likelihood that two hosts on the same network can select the same retransmission time. Table 6 on page 17 shows collision rounds up to round 10.

<table>
<thead>
<tr>
<th>Round</th>
<th>Size of Set</th>
<th>Elements in the Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>(0,1)</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>(0,1,2,3)</td>
</tr>
<tr>
<td>3</td>
<td>8</td>
<td>(0,1,2,3,...,7)</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>(0,1,2,3,4,...,15)</td>
</tr>
<tr>
<td>5</td>
<td>32</td>
<td>(0,1,2,3,4,5,...,31)</td>
</tr>
<tr>
<td>6</td>
<td>64</td>
<td>(0,1,2,3,4,5,6,...,63)</td>
</tr>
<tr>
<td>7</td>
<td>128</td>
<td>(0,1,2,3,4,5,6,7,...,127)</td>
</tr>
<tr>
<td>8</td>
<td>256</td>
<td>(0,1,2,3,4,5,6,7,8,...,255)</td>
</tr>
<tr>
<td>9</td>
<td>512</td>
<td>(0,1,2,3,4,5,6,7,8,9,...,511)</td>
</tr>
<tr>
<td>10</td>
<td>1024</td>
<td>(0,1,2,3,4,5,6,7,8,9,10,...,1023)</td>
</tr>
</tbody>
</table>

**Collision Domains and LAN Segments**

Collisions are confined to a physical wire over which data is broadcast. Because the physical wires are subject to signal collisions, individual LAN segments are known as collision domains. Although the physical limitations on the length of an Ethernet cable restrict the length of a LAN segment, multiple collision domains can be interconnected by repeaters, bridges, and switches.

**Repeaters**

Repeaters are electronic devices that act on analog signals. Repeaters relay all electronic signals from one wire to another. A single repeater can double the distance between two devices on an Ethernet network. However, the Ethernet specification restricts the number of repeaters between any two devices on an Ethernet network to two, because collision detection with latencies increases in complexity as the wire length and number of repeaters increase.
Bridges and Switches

Bridges and switches combine LAN segments into a single Ethernet network by using multiple ports to connect the physical wires in each segment. Although bridges and switches are fundamentally the same, bridges generally provide more management and more interface ports. As Ethernet packets flow through a bridge, the bridge tracks the source MAC address of the packets and stores the addresses and their associated input ports in an interface table. As it receives subsequent packets, the bridge examines its interface table and takes one of the following actions:

- If the destination address does not match an address in the interface table, the bridge transmits the packet to all hosts on the network using the Ethernet broadcast address.
- If the destination address maps to the port through which the packet was received, the bridge or switch discards the packet. Because the other devices on the LAN segment also received the packet, the bridge does not need to retransmit it.
- If the destination address maps to a port other than the one through which the packet was received, the bridge transmits the packet through the appropriate port to the corresponding LAN segment.

Broadcast Domains

The combination of all the LAN segments within an Ethernet network is called a broadcast domain. In the absence of any signaling devices such as a repeater, bridge, or switch, the broadcast domain is simply the physical wire that makes up the connections in the network. If a bridge or switch is used, the broadcast domain consists of the entire LAN.

Ethernet Frames

Data is transmitted through an Ethernet network in frames. The frames are of variable length, ranging from 64 octets to 1518 octets, including the header, payload, and cyclic redundancy check (CRC) value. Figure 1 on page 18 shows the Ethernet frame format.

Figure 1: Ethernet Frame Format

Ethernet frames have the following fields:
The preamble (PRE) in the frame is 7 octets of alternating 0s and 1s. The predictable format in the preamble allows receiving interfaces to synchronize themselves to the data being sent. The preamble is followed by a 1-octet start-of-frame delimiter (SFD).

The destination address (DA) and source address (SA) fields contain the 6-octet (48-bit) MAC addresses for the destination and source ports on the network. These Layer 2 addresses uniquely identify the devices on the LAN.

The length/type field is a 2-octet field that either indicates the length of the frame's data field or identifies the protocol stack associated with the frame. Following are some common frame types:

- AppleTalk—0x809B
- AppleTalk ARP—0x80F3
- DECnet—0x6003
- IP—0x0800
- IPX—0x8137
- Loopback—0x9000
- XNS—0x0600

The frame data is the packet payload.

The frame check sequence (FCS) field is a 4-octet field that contains the calculated CRC value. This value is calculated by the originating host and appended to the frame. When it receives the frames, the receiving host calculates the CRC and checks it against this appended value to verify the integrity of the received frame.

**T1 and E1 Interfaces Overview**

T1 and E1 are equivalent digital data transmission formats that carry DS1 signals. T1 and E1 lines can be interconnected for international use. This section contains the following topics:

- T1 Overview on page 19
- E1 Overview on page 20
- T1 and E1 Signals on page 20
- Encoding on page 20
- T1 and E1 Framing on page 21
- T1 and E1 Loopback Signals on page 22

**T1 Overview**

T1 is a digital data transmission medium capable of handling 24 simultaneous connections running at a combined 1.544 Mbps. T1 combines these 24 separate connections, called channels or time slots, onto a single link. T1 is also called DS1.
The T1 data stream is broken into frames. Each frame consists of a single framing bit and 24 8-bit channels, totalling 193 bits per T1 frame. Frames are transmitted 8,000 times per second, at a data transmission rate of 1.544 Mbps (8,000 x 193 = 1.544 Mbps).

As each frame is received and processed, the data in each 8-bit channel is maintained with the channel data from previous frames, enabling T1 traffic to be separated into 24 separate flows across a single medium. For example, in the following set of 4-channel frames (without a framing bit), the data in channel 1 consists of the first octet of each frame, the data in channel 2 consists of the second octet of each frame, and so on:

<table>
<thead>
<tr>
<th>Chan. 1</th>
<th>Chan. 2</th>
<th>Chan. 3</th>
<th>Chan. 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame 1</td>
<td>[10001100]</td>
<td>[00110001]</td>
<td>[11111000]</td>
</tr>
<tr>
<td>Frame 2</td>
<td>[11100101]</td>
<td>[01110110]</td>
<td>[10001000]</td>
</tr>
<tr>
<td>Frame 3</td>
<td>[00010100]</td>
<td>[00101111]</td>
<td>[11000001]</td>
</tr>
</tbody>
</table>

**E1 Overview**

E1 is the European format for DS1 digital transmission. E1 links are similar to T1 links except that they carry signals at 2.048 Mbps. Each signal has 32 channels, and each channel transmits at 64 Kbps. E1 links have higher bandwidth than T1 links because they use all 8 bits of a channel. T1 links use 1 bit in each channel for overhead.

**T1 and E1 Signals**

T1 and E1 interfaces consist of two pairs of wires—a transmit data pair and a receive data pair. Clock signals, which determine when the transmitted data is sampled, are embedded in T1 and E1 transmissions.

Typical digital signals operate by sending either zeros (0s) or ones (1s), which are usually represented by the absence or presence of a voltage on the line. The receiving device need only detect the presence of the voltage on the line at the particular sampling edge to determine if the signal is 0 or 1. T1 and E1, however, use bipolar electrical pulses. Signals are represented by no voltage (0), positive voltage (1), or negative voltage (-1). The bipolar signal allows T1 and E1 receivers to detect error conditions in the line, depending on the type of encoding that is being used. For more information, see “Encoding” on page 20.

**Encoding**

Following are common T1 and E1 encoding techniques:

- Alternate mark inversion (AMI)—T1 and E1
- Bipolar with 8-zero substitution (B8ZS)—T1 only
- High-density bipolar 3 code (HDB3)—E1 only
AMI Encoding

AMI encoding forces the 1s signals on a T1 or E1 line to alternate between positive and negative voltages for each successive 1 transmission, as in this sample data transmission:

```
1 1 0 1 0 1 0 1
+ - 0 + 0 - 0 +
```

When AMI encoding is used, a data transmission with a long sequence of 0s has no voltage transitions on the line. In this situation, devices have difficulty maintaining clock synchronization, because they rely on the voltage fluctuations to constantly synchronize with the transmitting clock. To counter this effect, the number of consecutive 0s in a data stream is restricted to 15. This restriction is called the 1s density requirement, because it requires a certain number of 1s for every 15 0s that are transmitted.

On an AMI-encoded line, two consecutive pulses of the same polarity—either positive or negative—are called a bipolar violation (BPV), which is generally flagged as an error.

B8ZS and HDB3 Encoding

Both B8ZS and HDB3 encoding do not restrict the number of 0s that can be transmitted on a line. Instead, these encoding methods detect sequences of 0s and substitute bit patterns in their place to provide the signal oscillations required to maintain timing on the link.

The B8ZS encoding method for T1 lines detects sequences of eight consecutive 0 transmissions and substitutes a pattern of two consecutive BPVs (11110000). Because the receiving end uses the same encoding, it detects the BPVs as 0s substitutions, and no BPV error is flagged. A single BPV, which does not match the 11110000 substitution bit sequence, is likely to generate an error, depending on the configuration of the device.

The HDB3 encoding method for E1 lines detects sequences of four consecutive 0 transmissions and substitutes a single BPV (1100). Similar to B8ZS encoding, the receiving device detects the 0s substitutions and does not generate a BPV error.

T1 and E1 Framing

J Series Services Router T1 interfaces use two types of framing: superframe (D4) and extended superframe (ESF). E1 interfaces use G.704 framing or G.704 with no CRC4 framing, or can be in unframed mode.

Superframe (D4) Framing for T1

A D4 frame consists of 192 data bits: 24 8-bit channels and a single framing bit. The single framing bit is part of a 12-bit framing sequence. The 193rd bit in each T1 frame is set to a value, and every 12 consecutive frames are examined to determine the framing bit pattern for the 12-bit superframe.
The following sample 12-frame sequence shows the framing pattern for D4 framing:

```
[data bits][framing bit]
[xxxxxxxxxx][1]
[xxxxxxxxxx][0]
[xxxxxxxxxx][0]
[xxxxxxxxxx][0]
[xxxxxxxxxx][1]
[xxxxxxxxxx][1]
[xxxxxxxxxx][0]
[xxxxxxxxxx][1]
[xxxxxxxxxx][1]
[xxxxxxxxxx][1]
[xxxxxxxxxx][0]
[xxxxxxxxxx][0]
```

The 100011011100 12-bit pattern is repeated in each successive superframe. The receiving device detects these bits to synchronize with the incoming data stream and determine when the framing pattern begins and ends.

D4 framing requires the 8th bit of every byte (of every channel) within the frame to be set to 1, a process known as bit robbing. The bit-robbing requirement ensures that the 1s density requirements are met, regardless of the data contents of the frames, but it reduces the bandwidth on the T1 link by an eighth.

**Extended Superframe (ESF) Framing for T1**

ESF extends the D4 superframe from 12 frames to 24 frames. By expanding the size of the superframe, ESF increases the number of bits in the superframe framing pattern from 12 to 24. The extra bits are used for frame synchronization, error detection, and maintenance communications through the facilities data link (FDL).

The ESF pattern for synchronization bits is 001011. Only the framing bits from frames 4, 8, 12, 16, 20, and 24 in the superframe sequence are used to create the synchronization pattern.

The framing bits from frames 2, 6, 10, 14, 18, and 22 are used to pass a CRC code for each superframe block. The CRC code verifies the integrity of the received superframe and detects bit errors with a CRC6 algorithm.

The framing bits for frames 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, and 23 are used for the data link channel. These 12 bits enable the operators at the network control center to query the remote equipment for information about the performance of the link.

**T1 and E1 Loopback Signals**

The control signal on a T1 or E1 link is the loopback signal. Using the loopback signal, the operators at the network control center can force the device at the remote end of a link to retransmit its received signals back onto the transmit path. The transmitting device can then verify that the received signals match the transmitted signals, to perform end-to-end checking on the link.

Two loopback signals are used to perform the end-to-end testing:
The loop-up command signal sets the link into loopback mode, with the following command pattern:

...1000100001000100... 

The loop-down signal returns the link to its normal mode, with the following command pattern:

...100100100100100... 

While the link is in loopback mode, the operator can insert test equipment onto the line to test its operation.

Channelized T1/E1/ISDN PRI Interfaces Overview

Channelization enables devices to provide IP services to users with different access speeds and bandwidth requirements. Users share an interface that has been divided into discrete time slots, by transmitting in only their own time slot. On J Series devices, a single channelized T1/E1/ISDN PRI interface can be partitioned into the following numbers of DS0 or ISDN PRI time slots, by means of software configuration:

- T1 interface—Up to 24 DS0 time slots (channels 1 through 24).
- E1 interface—Up to 31 DS0 time slots (channels 1 through 31).
- ISDN PRI—Up to 23 ISDN PRI B-channels and 1 D-channel when the parent interface is channelized T1, and up to 30 ISDN PRI B-channels and 1 D-channel when the parent interface is channelized E1. Time slots on the interface unused by ISDN PRI can operate normally as DS0 interfaces.

For more information about ISDN, see “ISDN Interface Overview” on page 49.

NOTE: You cannot configure the channelized T1/E1/ISDN PRI PIM through a J-Web Quick Configuration page.

You can aggregate the channels on a channelized interface into bundles called channel groups to aggregate customer traffic.

A single channelized T1/E1/ISDN PRI interface also supports drop-and-insert multiplexing, to integrate voice and data channels on a single T1 or E1 link. The drop-and-insert feature allows you to remove the DS0 time slots of one T1 or E1 port and replace them by inserting the time slots of another T1 or E1 interface.

T3 and E3 Interfaces Overview

T3 is a high-speed data-transmission medium formed by multiplexing 28 DS1 signals into seven separate DS2 signals, and combining the DS2 signals into a single DS3 signal. T3 links operate at 43.736 Mbps. T3 is also called DS3.

E3 is the equivalent European transmission format. E3 links are similar to T3 (DS3) links, but carry signals at 34.368 Mbps. Each signal has 16 E1 channels, and each
channel transmits at 2.048 Mbps. E3 links use all 8 bits of a channel, whereas T3 links use 1 bit in each channel for overhead.

**Multiplexing DS1 Signals**

Four DS1 signals combine to form a single DS2 signal. The four DS1 signals form a single DS2 M-frame, which includes subframes M1 through M4. Each subframe has six 49-bit blocks, for a total of 294 bits per subframe. The first bit in each block is a DS2 overhead (OH) bit. The remaining 48 bits are DS1 information bits.

Figure 2 on page 24 shows the DS2 M-frame format.

**Figure 2: DS2 M-Frame Format**

The four DS2 subframes are not four DS1 channels. Instead, the DS1 data bits within the subframes are formed by data interleaved from the DS1 channels. The 0 values designate time slots devoted to DS1 inputs as part of the bit-by-bit interleaving process. After every 48 DS1 information bits (12 bits from each signal), a DS2 OH bit is inserted to indicate the start of a subframe.

**DS2 Bit Stuffing**

Because the four DS1 signals are asynchronous signals, they might operate at different line rates. To synchronize the asynchronous streams, the multiplexers on the line use bit stuffing.

A DS2 connection requires a nominal transmit rate of 6.304 Mbps. However, because multiplexers increase the overall output rate to the intermediate rate of 6.312 Mbps, the output rate is higher than individual input rates on DS1 signals. The extra bandwidth is used to stuff the incoming DS1 signals with extra bits until the output rate of each signal equals the increased intermediate rate. These stuffed bits are inserted at fixed locations in the DS2 M-frame. When DS2 frames are received and the signal is demultiplexed, the stuffing bits are identified and removed.
DS3 Framing

A set of four DS1 signals is multiplexed into seven DS2 signals, which are multiplexed into a single DS3 signal. The multiplexing occurs just as with DS1-to-DS2 multiplexing. The resulting DS3 signal uses either the standard M13 asynchronous framing format or the C-bit parity framing format. Although the two framing formats differ in their use of control and message bits, the basic frame structures are identical. The DS3 frame structures are shown in Figure 3 on page 25 and Figure 4 on page 27.

M13 Asynchronous Framing

A DS3 M-frame includes seven subframes, formed by DS2 data bits interleaved from the seven multiplexed DS2 signals. Each subframe has eight 85-bit blocks—a DS3 OH bit plus 84 data bits. The meaning of an OH bit depends on the block it precedes. Standard DS3 M13 asynchronous framing format is shown in Figure 3 on page 25.

### Figure 3: DS3 M13 Frame Format

<table>
<thead>
<tr>
<th>Block 1</th>
<th>Block 2</th>
<th>Block 3</th>
<th>Block 4</th>
<th>Block 5</th>
<th>Block 6</th>
<th>Block 7</th>
<th>Block 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st M-subframe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd M-subframe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3rd M-subframe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4th M-subframe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5th M-subframe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6th M-subframe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7th M-subframe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A DS3 M13 M-frame contains the following types of OH bits:

- **Framing bits (F-bits)**—Make up a frame alignment signal that synchronizes DS3 subframes. Each DS3 frame contains 28 F-bits (4 bits per subframe). F-bits are located at the beginning of blocks 2, 4, 6, and 8 of each subframe. When combined, the frame alignment pattern for each subframe is 1001. The pattern can be examined to detect bit errors in the transmission.

- **Multiframing bits (M-bits)**—Make up a multiframe alignment signal that synchronizes the M-frames in a DS3 signal. Each DS3 frame contains 3 M-bits,
which are located at the beginning of subframes 5, 6, and 7. When combined, the multiframe alignment pattern for each M-frame is 010.

- Bit stuffing control bits (C-bits)—Serve as bit stuffing indicators for each DS2 input. For example, \( C_{11} \), \( C_{12} \), and \( C_{13} \) are indicators for DS2 input 1. Their values indicate whether DS3 bit stuffing has occurred at the multiplexer. If the three C-bits in a subframe are all 0s, no stuffing was performed for the DS2 input. If the three C-bits are all 1s, stuffing was performed.

- Message bits (X-bits)—Used by DS3 transmitters to embed asynchronous in-service messages in the data transmission. Each DS3 frame contains 2 X-bits, which are located at the beginning of subframes 1 and 2. Within an DS3 M-frame, both X-bits must be identical.

- Parity bits (P-bits)—Compute parity over all but 1 bit of the M-frame. (The first X-bit is not included.) Each DS3 frame contains 2 P-bits, which are located at the beginning of subframes 3 and 4. Both P-bits must be identical.

  If the previous DS3 frame contained an odd number of 1s, both P-bits are set to 1. If the previous DS3 contained an even number of 1s, both P-bits are set to 0. If, on the receiving side, the number of 1s for a given frame does not match the P-bits in the following frame, it indicates one or more bit errors in the transmission.

### C-Bit Parity Framing

In M13 framing, every C-bit in a DS3 frame is used for bit stuffing. However, because multiplexers first use bit stuffing when multiplexing DS1 signals into DS2 signals, the incoming DS2 signals are already synchronized. Therefore, the bit stuffing that occurs when DS2 signals are multiplexed is redundant.

C-bit parity framing format redefines the function of C-bits and X-bits, using them to monitor end-to-end path performance and provide in-band data links. The C-bit parity framing structure is shown in Figure 4 on page 27.
In C-bit parity framing, the X-bits transmit error conditions from the far end of the link to the near end. If no error conditions exist, both X-bits are set to 1. If an out-of-frame (OOF) or alarm indication signal (AIS) error is detected, both X-bits are set to 0 in the upstream direction for 1 second to notify the other end of the link about the condition.

The C-bits that control bit stuffing in M13 frames are typically used in the following ways by C-bit parity framing:

- Application identification channel (AIC)—The first C-bit in the first subframe identifies the type of DS3 framing used. A value of 1 indicates that C-bit parity framing is in use.
- N—a reserved network application bit.
- Far-end alarm and control (FEAC) channel—The third C-bit in the first subframe is used for the FEAC channel. In normal transmissions, the FEAC C-bit transmits all 1s. When an alarm condition is present, the FEAC C-bit transmits a code word in the format 0xxxxxxx 1111111, in which x can be either 1 or 0. Bits are transmitted from right to left.

Table 7 on page 27 lists some C-bit code words and the alarm or status condition indicated.

### Table 7: FEAC C-Bit Condition Indicators

<table>
<thead>
<tr>
<th>Alarm or Status Condition</th>
<th>C-Bit Code Word</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS3 equipment failure requires immediate attention.</td>
<td>00110010 11111111</td>
</tr>
</tbody>
</table>
Table 7: FEAC C-Bit Condition Indicators (continued)

<table>
<thead>
<tr>
<th>Alarm or Status Condition</th>
<th>C-Bit Code Word</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS3 equipment failure occurred—such as suspended, not activated, or unavailable service—that is non-service-affecting</td>
<td>00011110 11111111</td>
</tr>
<tr>
<td>DS3 loss of signal.</td>
<td>00011100 11111111</td>
</tr>
<tr>
<td>DS3 out of frame.</td>
<td>00000000 11111111</td>
</tr>
<tr>
<td>DS3 alarm indication signal (AIS) received.</td>
<td>00101100 11111111</td>
</tr>
<tr>
<td>DS3 idle received.</td>
<td>00110100 11111111</td>
</tr>
<tr>
<td>Common equipment failure occurred that is non-service-affecting</td>
<td>00011101 11111111</td>
</tr>
<tr>
<td>Multiple DS1 loss of signal.</td>
<td>00101010 11111111</td>
</tr>
<tr>
<td>DS1 equipment failure occurred that requires immediate attention.</td>
<td>00001010 11111111</td>
</tr>
<tr>
<td>DS1 equipment failure occurred that is non-service-affecting.</td>
<td>00000110 11111111</td>
</tr>
<tr>
<td>Single DS1 loss of signal.</td>
<td>00111100 11111111</td>
</tr>
</tbody>
</table>

- Data links—The 12 C-bits in subframes 2, 5, 6, and 7 are data link (DL) bits for applications and terminal-to-terminal path maintenance.
- DS3 parity—The 3 C-bits in the third subframe are DS3 parity C-bits (also called CP-bits). When a DS3 frame is transmitted, the sending device sets the CP-bits to the same value as the P-bits. When the receiving device processes the frame, it calculates the parity of the M-frame and compares this value to the parity in the CP-bits of the following M-frame. If no bit errors have occurred, the two values are typically the same.
- Far-end block errors (FEBEs)—The 3 C-bits in the fourth subframe make up the far-end block error (FEBE) bits. If a framing or parity error is detected in an incoming M-frame (via the CP-bits), the receiving device generates a C-bit parity error and sends an error notification to the transmitting (far-end) device. If an error is generated, the FEBE bits are set to 000. If no error occurred, the bits are set to 111.

Serial Interface Overview

Serial links are simple, bidirectional links that require very few control signals. In a basic serial setup, data communications equipment (DCE) installed in a user’s premises is responsible for establishing, maintaining, and terminating a connection. A modem is a typical DCE device.

A serial cable connects the DCE to a telephony network where, ultimately, a link is established with data terminal equipment (DTE). DTE is typically where a serial link terminates.
The distinction between DCE and DTE is important because it affects the cable pinouts on a serial cable. A DTE cable uses a male 9-pin or 25-pin connector, and a DCE cable uses a female 9-pin or 25-pin connector.

To form a serial link, the cables are connected to each other. However, if the pins are identical, each side’s transmit and receive lines are connected, which makes data transport impossible. To address this problem, each cable is connected to a null modem cable, which crosses the transmit and receive lines in the cable.

**Serial Transmissions**

In basic serial communications, nine signals are critical to the transmission. Each signal is associated with a pin in either the 9-pin or 25-pin connector. Table 8 on page 29 lists and defines serial signals and their sources.

### Table 8: Serial Transmission Signals

<table>
<thead>
<tr>
<th>Signal Name</th>
<th>Definition</th>
<th>Signal Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>TD</td>
<td>Transmitted data</td>
<td>DTE</td>
</tr>
<tr>
<td>RD</td>
<td>Received data</td>
<td>DCE</td>
</tr>
<tr>
<td>RTS</td>
<td>Request to send</td>
<td>DTE</td>
</tr>
<tr>
<td>CTS</td>
<td>Clear to send</td>
<td>DCE</td>
</tr>
<tr>
<td>DSR</td>
<td>Data set ready</td>
<td>DCE</td>
</tr>
<tr>
<td>Signal Ground</td>
<td>Grounding signal</td>
<td>–</td>
</tr>
<tr>
<td>CD</td>
<td>Carrier detect</td>
<td>–</td>
</tr>
<tr>
<td>DTR</td>
<td>Data terminal ready</td>
<td>DTE</td>
</tr>
<tr>
<td>RI</td>
<td>Ring indicator</td>
<td>–</td>
</tr>
</tbody>
</table>

When a serial connection is made, a serial line protocol—such as EIA-530, X.21, RS-422/449, RS-232, or V.35—begins controlling the transmission of signals across the line as follows:

1. The DCE transmits a DSR signal to the DTE, which responds with a DTR signal. After this handshake, the link is established and traffic can pass.

2. When the DTE device is ready to receive data, it sets its RTS signal to a marked state (all 1s) to indicate to the DCE that it can transmit data. (If the DTE is not able to receive data—because of buffer conditions, for example—it sets the RTS signal to all 0s.)
3. When the DCE device is ready to receive data, it sets its CTS signal to a marked state to indicate to the DTE that it can transmit data. (If the DCE is not able to receive data, it sets the CTS signal to all 0s.)

4. When the negotiation to send information has taken place, data is transmitted across the transmitted data (TD) and received data (RD) lines:
   - TD line—Line through which data from a DTE device is transmitted to a DCE device
   - RD line—Line through which data from a DCE device is transmitted to a DTE device

   The name of the wire does not indicate the direction of data flow.

The DTR and DSR signals were originally designed to operate as a handshake mechanism. When a serial port is opened, the DTE device sets its DTR signal to a marked state. Similarly, the DCE sets its DSR signal to a marked state. However, because of the negotiation that takes place with the RTS and CTS signals, the DTR and DSR signals are not commonly used.

The carrier detect and ring indicator signals are used to detect connections with remote modems. These signals are not commonly used.

**Signal Polarity**

Serial interfaces use a balanced (also called differential) protocol signaling technique. Two serial signals are associated with a circuit: the A signal and the B signal. The A signal is denoted with a plus sign (for example, DTR+), and the B signal is denoted with a minus sign (for example, DTR–). If DTR is low, then DTR+ is negative with respect to DTR–. If DTR is high, then DTR+ is positive with respect to DTR–.

By default, all signal polarities are positive, but sometimes they might be reversed. For example, signals might be miswired as a result of reversed polarities.

**Serial Clocking Modes**

By default, a serial interface uses loop clocking to determine its timing source. For EIA-530 and V.35 interfaces, you can set each port independently to use one of the following clocking modes. X.21 interfaces can use only loop clocking mode.

- Loop clocking mode—Uses the DCE’s receive (RX) clock to clock data from the DCE to the DTE.
- DCE clocking mode—Uses the transmit (TXC) clock, generated by the DCE specifically to be used by the DTE as the DTE’s transmit clock.
- Internal clocking mode—Uses an internally generated clock. The speed of this clock is configured locally. Internal clocking mode is also known as line timing.

Both loop clocking mode and DCE clocking mode use external clocks generated by the DCE.
Figure 5 on page 31 shows the clock sources for loop, DCE, and internal clocking modes.

**Figure 5: Serial Interface Clocking Modes**

Serial Interface Transmit Clock Inversion

When an externally timed clocking mode (DCE or loop) is used, long cables might introduce a phase shift of the DTE-transmitted clock and data. At high speeds, this phase shift might cause errors. Inverting the transmit clock corrects the phase shift, thereby reducing error rates.

DTE Clock Rate Reduction

Although the serial interface is intended for use at the default clock rate of 16.384 MHz, you might need to use a slower rate under any of the following conditions:

- The interconnecting cable is too long for effective operation.
- The interconnecting cable is exposed to an extraneous noise source that might cause an unwanted voltage in excess of +1 volt.

  The voltage must be measured differentially between the signal conductor and the point in the circuit from which all voltages are measured (“circuit common”) at the load end of the cable, with a 50-ohm resistor substituted for the generator.
- Interference with other signals must be minimized.
- Signals must be inverted.

**Serial Line Protocols**

Serial interfaces support the following line protocols:

- EIA-530 on page 32
- RS-232 on page 32
- RS-422/449 on page 33
EIA-530

EIA-530 is an Electronic Industries Association (EIA) standard for the interconnection of DTE and DCE using serial binary data interchange with control information exchanged on separate control circuits. EIA-530 is also known as RS-530.

The EIA-530 line protocol is a specification for a serial interface that uses a DB-25 connector and balanced equivalents of the RS-232 signals—also called V.24. The EIA-530 line protocol is equivalent to the RS-422 and RS-423 interfaces implemented on a 25-pin connector.

The EIA-530 line protocol supports both balanced and unbalanced modes. In unbalanced transmissions, voltages are transmitted over a single wire. Because only a single signal is transmitted, differences in ground potential can cause fluctuations in the measured voltage across the link. For example, if a 3V signal is sent from one endpoint to another, and the receiving endpoint has a ground potential 1V higher than the transmitter, the signal on the receiving end is measured as a 2V signal.

Balanced transmissions use two wires instead of one. Rather than sending a single signal across the wire and having the receiving end measure the voltage, the transmitting device sends two separate signals across two separate wires. The receiving device measures the difference in voltage of the two signals (balanced sampling) and uses that calculation to evaluate the signal. Any differences in ground potential affect both wires equally, and the difference in the signals is still the same.

The EIA-530 interface supports asynchronous and synchronous transmissions at rates ranging from 20 Kbps to 2 Mbps.

RS-232

RS-232 is a Recommended Standard (RS) describing the most widely used type of serial communication. The RS-232 protocol is used for asynchronous data transfer as well as synchronous transfers using HDLC, Frame Relay, and X.25. RS-232 is also known as EIA-232.

The RS-232 line protocol is very popular for low-speed data signals. RS-232 signals are carried as single voltages referred to a common ground signal. The voltage output level of these signals varies between −12V and +12V. Within this range, voltages between −3V and +3V are considered inoperative and are used to absorb line noise. Control signals are considered operative when the voltage ranges from +3 to +25V.

The RS-232 line protocol is an unbalanced protocol, because it uses only one wire, and is susceptible to signal degradation. Degradation can be extremely disruptive, particularly when a difference in ground potential exists between the transmitting and receiving ends of a link.

The RS-232 interface is implemented in a 25-pin D-shell connector and supports line rates up to 200 Kbps over lines shorter than 98 feet (30 meters).
NOTE: RS-232 serial interfaces cannot function error-free with a clock rate greater than 200 KHz.

RS-422/449

RS-422 is a Recommended Standard (RS) describing the electrical characteristics of balanced voltage digital interface circuits that support higher bandwidths than traditional serial protocols like RS-232. RS-422 is also known as EIA-422.

The RS-449 standard (also known as EIA-449) is compatible with RS-422 signal levels. The EIA created RS-449 to detail the DB-37 connector pinout and define a set of modem control signals for regulating flow control and line status.

The RS-422/499 line protocol runs in balanced mode, allowing serial communications to extend over distances of up to 4,000 feet (1.2 km) and at very fast speeds of up to 10 Mbps.

In an RS-422/499-based system, a single master device can communicate with up to 10 slave devices in the system. To accommodate this configuration, RS-422/499 supports the following kinds of transmission:

- **Half-duplex transmission**—In half-duplex transmission mode, transmissions occur in only one direction at a time. Each transmission requires a proper handshake before it is sent. This operation is typical of a balanced system in which two devices are connected by a single connection.

- **Full-duplex transmission**—In full-duplex transmission mode, multiple transmissions can occur simultaneously so that devices can transmit and receive at the same time. This operation is essential when a single master in a point-to-multipoint system must communicate with multiple receivers.

- **Multipoint transmission**—RS-422/449 allows only a single master in a multipoint system. The master can communicate to all points in a multipoint system, and the other points must communicate with each other through the master.

V.35

V.35 is an ITU-T standard describing a synchronous, physical-layer protocol used for communications between a network access device and a packet network. V.35 is most commonly used in the United States and Europe.

The V.35 line protocol is a mixture of balanced (RS-422) and common ground (RS-232) signal interfaces. The V.35 control signals DTR, DSR, DCD, RTS, and CTS are single-wire common ground signals that are essentially identical to their RS-232 equivalents. Unbalanced signaling for these control signals is sufficient, because the control signals are mostly constant, varying at very low frequency, which makes single-wire transmission suitable. Higher-frequency data and clock signals are sent over balanced wires.

V.35 interfaces operate at line rates of 20 Kbps and above.
X.21

X.21 is an ITU-T standard for serial communications over synchronous digital lines. The X.21 protocol is used primarily in Europe and Japan.

The X.21 line protocol is a state-driven protocol that sets up a circuit-switched network using call setup. X.21 interfaces use a 15-pin connector with the following eight signals:

- **Signal ground (G)**—Reference signal used to evaluate the logic states of the other signals. This signal can be connected to the protective earth (ground).
- **DTE common return (Ga)**—Reference ground signal for the DCE interface. This signal is used only in unbalanced mode.
- **Transmit (T)**—Binary signal that carries the data from the DTE to the DCE. This signal can be used for data transfer or in call-control phases such as Call Connect or Call Disconnect.
- **Receive (R)**—Binary signal that carries the data from the DCE to the DTE. This signal can be used for data transfer or in call-control phases such as Call Connect or Call Disconnect.
- **Control (C)**—DTE-controlled signal that controls the transmission on an X.21 link. This signal must be on during data transfer, and can be on or off during call-control phases.
- **Indication (I)**—DCE-controlled signal that controls the transmission on an X.21 link. This signal must be on during data transfer, and can be on or off during call-control phases.
- **Signal Element Timing (S)**—Clocking signal that is generated by the DCE. This signal specifies when sampling on the line must occur.
- **Byte Timing (B)**—Binary signal that is on when data or call-control information is being sampled. When an 8-byte transmission is over, this signal switches to off.

Transmissions across an X.21 link require both the DCE and DTE devices to be in a ready state, indicated by an all 1s transmission on the T and R signals.

ADSL Interface Overview

Asymmetric digital subscriber line (ADSL) technology is part of the xDSL family of modem technologies that use existing twisted-pair telephone lines to transport high-bandwidth data. ADSL lines connect service provider networks and customer sites over the "last mile" of the network—the loop between the service provider and the customer site.

ADSL transmission is asymmetric because the downstream bandwidth is typically greater than the upstream bandwidth. The typical bandwidths of ADSL, ADSL2, and ADSL2+ circuits are defined in Table 9 on page 35.
Table 9: Standard Bandwidths of DSL Operating Modes

<table>
<thead>
<tr>
<th>Operating Modes</th>
<th>Upstream</th>
<th>Downstream</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADSL</td>
<td>800 Kbps — 1 Mbps</td>
<td>8 Mbps</td>
</tr>
<tr>
<td>ADSL2</td>
<td>1 — 1.5 Mbps</td>
<td>12 — 14 Mbps</td>
</tr>
<tr>
<td>ADSL2 +</td>
<td>1 — 1.15 Mbps</td>
<td>24 — 25 Mbps</td>
</tr>
<tr>
<td>ADSL2 + Annex M</td>
<td>4 Mbps</td>
<td>25 Mbps</td>
</tr>
</tbody>
</table>

SRX210 devices support ADSL, ADSL2, and ADSL2 +, which comply with the following standards:

- For Annex A:
  - ITU G.992.1 (ADSL)
- For Annex A only:
  - ANSI T1.413 Issue II
  - ITU G.992.3 (ADSL2)
  - ITU G.992.5 (ADSL2 +)
- For Annex M:
  - ITU G.992.3 (ADSL2)
  - ITU G.992.5 (ADSL2 +)
- For Annex B:
  - ITU G.992.1 (ADSL)
  - ITU G.992.3 (ADSL2)
  - ITU G.992.5 (ADSL2 +)
- For Annex B only
  - ETSI TS 101 388 V1.3

The ADSL Mini-PIM is supported on SRX210 devices. The ADSL Mini-PIM facilitates a maximum of ten virtual circuits on SRX210 devices.

SRX210 devices with Mini-PIMs can use PPP over Ethernet over ATM (PPPoEoA) and PPP over ATM (PPPoA) to connect through ADSL lines only.

**ADSL Systems**

ADSL links run across twisted-pair telephone wires. When ADSL modems are connected to each end of a telephone wire, a dual-purpose ADSL circuit can be created. Once established, the circuit can transmit lower-frequency voice traffic and higher-frequency data traffic.
To accommodate both types of traffic, ADSL modems are connected to plain old telephone service (POTS) splitters that filter out the lower-bandwidth voice traffic and the higher-bandwidth data traffic. The voice traffic can be directed as normal telephone voice traffic. The data traffic is directed to the ADSL modem, which is typically connected to the data network.

Because twisted-pair wiring has a length limit, ADSL modems are typically connected to multiplexing devices. DSL access multiplexers (DSLAMs) can process and route traffic from multiple splitters. This typical ADSL configuration is shown in Figure 6 on page 36 and Figure 7 on page 37.
The ADSL2 and ADSL2+ standards were adopted by the ITU in July 2002. ADSL2 improves the data rate and reach performance, diagnostics, standby mode, and interoperability of ADSL modems.

ADSL2+ doubles the possible downstream data bandwidth, enabling rates of 20 Mbps on telephone lines shorter than 5,000 feet (1.5 km).

ADSL2 uses seamless rate adaptation (SRA) to change the data rate of a connection during operation with no interruptions or bit errors. The ADSL2 transceiver detects changes in channel conditions—for example, the failure of another transceiver in a multcarrier link—and sends a message to the transmitter to initiate a data rate change. The message includes data transmission parameters such as the number of bits modulated and the power on each channel. When the transmitter receives the information, it transitions to the new transmission rate.

**ATM CoS Support**

Certain class-of-service (CoS) components for Asynchronous Transmission Mode (ATM) are provided to control data transfer, especially for time-sensitive voice packets. The ADSL Mini-PIM on the SRX210 device provides extended ATM CoS functionality to provide cells across the network. You can define bandwidth utilization, which consists of either a constant rate or a peak cell rate, with sustained cell rate and burst
tolerance. By default, unspecified bit rate (UBR) is used because the bandwidth utilization is unlimited.

The following ATM traffic shaping is supported for the SRX210 device:

<table>
<thead>
<tr>
<th>Traffic Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Constant bit rate, (CBR)</strong></td>
<td>CBR is the service category for traffic with rigorous timing requirements like voice, and certain types of video. CBR traffic needs a constant cell transmission rate throughout the duration of the connection.</td>
</tr>
<tr>
<td><strong>Variable bit rate non-real-time (VBR-NRT)</strong></td>
<td>VBR-NRT is intended for sources such as data transfer, which do not have strict time or delay requirements. VBR-NRT is suitable for packet data transfers.</td>
</tr>
<tr>
<td><strong>Unspecified bit rate (UBR)</strong></td>
<td>UBR is ATM’s best-effort service, which does not provide any CoS guarantees. This is suitable for noncritical applications that can tolerate or quickly adjust to loss of cells.</td>
</tr>
</tbody>
</table>

The ability of a network to guarantee class of service is related in the way in which the source generates cells and also on the availability of network resources. The connection contract between the user and the network will thus contain information about the way in which traffic will be generated by the source.

A set of traffic descriptors is specified for this purpose. The network provides the class of service for the cells that do not violate these specifications. The following are the traffic descriptors specified for an ATM network:

- Peak cell rate (PCR) - Top rate at which traffic can burst.
- Sustained cell rate (SCR) - Normal traffic rate averaged over time.
- Maximum burst size (MBS) - The maximum burst size that can be sent at the peak rate.
- Cell delay variation tolerance (CDVT) – Allows the user to delay the traffic for a particular time duration in microseconds to follow a rhythmic pattern.

**NOTE:** CDVT is not supported on J Series devices.

For traffic that does not require the ability to periodically burst to a higher rate, you can specify a CBR. You can configure VBR-NRT for ATM interfaces, which supports VBR data traffic with average and peak traffic parameters. VBR-NRT is scheduled with a lower priority and with a larger sustained cell rate (SCR) limit, allowing it to recover bandwidth if it falls behind.

**SHDSL Interface Overview**

SHDSL interfaces on J Series device support a symmetric, high-speed digital subscriber line (SHDSL) multirate technology for data transfer between a single customer premises equipment (CPE) subscriber and a central office (CO). ITU-T G.991.2 is the officially designated standard describing SHDSL, also known as G.SHDSL.
Unlike ADSL, which delivers more bandwidth downstream than available upstream, SHDSL is symmetrical and delivers a bandwidth of up to 2.3 Mbps in both directions. Because business applications require higher-speed digital transportation methods, SHDSL is becoming very popular and gaining wide acceptance in the industry. Additionally, SHDSL is compatible with ADSL and therefore causes very little, if any, interference between cables.

SHDSL is deployed on a network in much the same manner as ADSL.

**G.SHDSL Mini-PIM**

This topic includes the following sections:

- G.SHDSL 8–Wire Mini-PIM Overview on page 39
- Operating Modes and Line Rates of the G.SHDSL Mini-PIM on page 40
- ATM CoS Support on page 40

**G.SHDSL 8–Wire Mini-PIM Overview**

The G.SHDSL Mini-Physical Interface Module (Mini-PIM) is supported on SRX210 and SRX240 devices. The G.SHDSL supported on the SRX Series Services Gateways provides the physical connection to DSL network media types.

The G.SHDSL Mini-Physical Interface Module (Mini-PIM) provides the following key features:

- 2-wire (4 port 2-wire) mode, 4-wire (2 port 4–wire) mode, and 8-wire (1 port 8–wire) mode support
- Virtual circuits per Mini-PIM (8 maximum)
- ATM-over-G.SHDSL framing
- ATM OAM support
- Maximum MTU size of 9180 bytes
- Noise margin support
- Point-to-Point Protocol over ATM and PPPoE over ATM encapsulation support
- Local loop back mode support

The following four annexes are supported on the G.SHDSL Mini-PIM:

- Annex A
- Annex B
- Annex F
- Annex G
Operating Modes and Line Rates of the G.SHDSL Mini-PIM

The G.SHDSL Mini-PIM supports 2-wire, 4-wire and 8-wire modes; the Mini-PIM can be used in 1x 8-wire, 2x 4-wire and 4x 2-wire modes. The default operating mode is 2x 4-wire for this G.SHDSL Mini-PIM. G.SHDSL is supported on all SRX210 and SRX240 devices using the following Symmetrical WAN speeds as shown in Table 10 on page 40.

### Table 10: Symmetrical WAN speeds

<table>
<thead>
<tr>
<th>Modes</th>
<th>Symmetrical WAN Speed Using Annex A and B</th>
<th>Symmetrical WAN Speed Using Annex F and G</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-wire</td>
<td>2.3 Mbps</td>
<td>From 768 Kbps to 5.696 Mbps</td>
</tr>
<tr>
<td>4-wire</td>
<td>4.6 Mbps</td>
<td>From 1.536 Mbps to 11.392 Mbps</td>
</tr>
<tr>
<td>8-wire</td>
<td>9.2 Mbps</td>
<td>From 3.072 Mbps to 22.784 Mbps</td>
</tr>
</tbody>
</table>

**NOTE:** A maximum of 16 Mbps is supported on SRX210 and SRX240 devices.

ATM CoS Support

The G.SHDSL Mini-PIM on the SRX210 and SRX240 devices provide extended ATM CoS functionality to provide cells across the network. You can define bandwidth utilization, which consists of either a constant rate or a peak cell rate, with sustained cell rate and burst tolerance. By default, unspecified bit rate (UBR) is used because the bandwidth utilization is unlimited.

The following ATM traffic shaping is supported for the SRX210 and SRX240 devices:

- **Constant bit rate (CBR)**—CBR is the service category for traffic with rigorous timing requirements like voice and certain types of video. CBR traffic needs a constant cell transmission rate throughout the duration of the connection.

- **Variable bit rate, non-real-time (VBR-NRT)**—VBR-NRT is intended for sources such as data transfer, which do not have strict time or delay requirements. VBR-NRT is suitable for packet data transfers.

- **Variable bit rate, real-time (VBR-RT)**—VBR-RT is intended for sources such as data transfer, which takes place in real time. VBR-RT requires access to time slots at a rate that can vary significantly from time to time.

Table 11 on page 40 displays the traffic descriptors specified for an ATM network.

### Table 11: Traffic Descriptors

<table>
<thead>
<tr>
<th>Traffic Descriptors</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak cell rate (PCR)</td>
<td>Maximum rate at which traffic can burst.</td>
</tr>
</tbody>
</table>
Table 11: Traffic Descriptors (continued)

<table>
<thead>
<tr>
<th>Traffic Descriptors</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sustained cell rate (SCR)</td>
<td>Normal traffic rate averaged over time.</td>
</tr>
<tr>
<td>Maximum burst size (MBS)</td>
<td>Maximum burst size that can be sent at the peak rate.</td>
</tr>
</tbody>
</table>

VDSDL2 Interface Overview

This section includes the following topics:
- VDSL2 Systems on page 41
- VDSL2 Terms on page 42
- Implementation of a VDSL2 Network Using SRX Series Services Gateways on page 42
- VDSL2 Mini-PIM Support on SRX210 and SRX240 Services Gateways on page 44
- Supported Profiles on page 44
- Supported Features on page 44

VDSDL2 Systems

Very-high-bit-rate digital subscriber line (VDSL) technology is part of the xDSL family of modem technologies that provide faster data transmission over a single flat untwisted or twisted pair of copper wires. The VDSL lines connect service provider networks and customer sites to provide high bandwidth applications (Triple Play services) such as high-speed Internet access, telephone services like voice over IP (VoIP), high-definition TV (HDTV), and interactive gaming services over a single connection. VDSL2 is an enhancement to VDSL and permits the transmission of asymmetric and symmetric (full-duplex) aggregate data rates up to 100 Mbps on short copper loops using a bandwidth up to 30 MHz.

The VDSL2 technology is based on the ITU-T G.993.2 standard. The VDSL2 uses Discrete Multitone (DMT) modulation. VDSL2 provides backward compatibility with ADSL, ADSL2, and ADSL2+ because this technology is based on both the VDSL1-DMT and ADSL2/ADSL2+ recommendations.

Packet Transfer Mode

VDSDL2 interface supports Packet Transfer Mode (PTM). The PTM mode transports packets (IP, PPP, Ethernet, MPLS, and so on) over DSL links as an alternative to using Asynchronous Transfer Mode (ATM). PTM is based on the Ethernet in the First Mile (EFM) IEEE802.3ah standard.

Discrete Multitone Modulation

VDSDL2 interface uses DMT modulation. Discrete multitone (DMT) is a method of separating a digital subscriber line signal so that the usable frequency range is separated into 256 frequency bands (or channels) of 4.3125 KHz each. The DMT
uses the Fast Fourier Transform (FFT) algorithm for demodulation or modulation for increased speed.

**VDSL2 Terms**

Table 12 on page 42 lists the terms related to VDSL2 technology.

### Table 12: VDSL Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITU-T G.993.2</td>
<td>International Telecommunication Union standard describing a data transmission method for VDSL2 transceivers.</td>
</tr>
<tr>
<td>Packet Transfer Mode (PTM)</td>
<td>Transport of packet-based services method based on the EFM IEEE802.3ah standard.</td>
</tr>
<tr>
<td>VDSL</td>
<td>VDSL is a DSL technology that provides data transmission over a single, flat, untwisted or twisted pair of copper wires at faster rate.</td>
</tr>
<tr>
<td>VDSL2</td>
<td>VDSL2 is an enhancement to G.993.1 (VDSL) that permits the transmission of asymmetric and symmetric (full duplex) aggregate data at faster rate. VDSL2 is based on ITU-T G.993.2 (VDSL2) standard.</td>
</tr>
<tr>
<td>DMT</td>
<td>Discrete multitone (DMT) modulation is used by VDSL2. The DMT modulation is a method of separating a digital subscriber line signal so that the usable frequency range is separated into 256 frequency bands (or channels) of 4.3125 KHz each.</td>
</tr>
</tbody>
</table>

**Implementation of a VDSL2 Network Using SRX Series Services Gateways**

In standard telephone cables of copper wires, voice signals use only a fraction of the available bandwidth. Like any other DSL technology, the VDSL2 technology utilizes the remaining capacity to carry the data and multimedia on the wire without interrupting the line’s ability to carry voice signals.

The following example depicts the typical VDSL2 network topology deployed using SRX Series Services Gateways.

A VDSL2 link between network devices is set up as follows:

1. Connect an end-user device such as a LAN, hub, or PC through an Ethernet interface to the customer premises equipment (CPE) (for example, an SRX Series device).
2. Use an RJ-11 cable to connect the CPE to a DSLAM.
3. The VDSL2 interface uses either Gigabit Ethernet or fiber as second mile to connect to the Broadband Remote Access Server (B-RAS) as shown in Figure 8 on page 43.
   - The ADSL interface uses either Gigabit Ethernet (in case of IP DSLAM) as the “second mile” to connect to the B-RAS or OC3/DS3 ATM as the second mile to connect the B-RAS as shown in Figure 9 on page 43.
NOTE: The VDSL2 technology is backward compatible with ADSL. VDSL2 provides an ADSL interface in an ATM DSLAM topology and provides a VDSL2 interface in an IP or VDSL DSLAM topology.

The DSLAM accepts connections from many customers and aggregates them to a single, high-capacity connection to the Internet.

Figure 8 on page 43 shows a typical VDSL2 network topology.

**Figure 8: Typical VDSL2 End-to-End Connectivity and Topology Diagram**

![Diagram](image)

Figure 9 on page 43 shows a backward-compatible ADSL topology using ATM DSLAM.

**Figure 9: Backward-Compatible ADSL Topology (ATM DSLAM)**

![Diagram](image)
**VDSL2 Mini-PIM Support on SRX210 and SRX240 Services Gateways**

The SRX210 and SRX240 Services Gateways support the VDSL2 Mini-PIM (Annex A). The VDSL2 Mini-Physical Interface Module (Mini-PIM) carries the Ethernet backplane. When the Mini-PIM is plugged into the chassis, the Mini-PIM connects to one of the ports of the baseboard switch. The VDSL2 Mini-PIM on the SRX Series devices provides ADSL backward compatibility.

The VDSL2 Mini-PIM (Annex A) is compatible with ITU-T G.993.2 (VDSL2) standard.

**Supported Profiles**

A profile is a table that contains a list of preconfigured VDSL2 settings. Table 13 on page 44 lists the different profiles supported on the VDSL2 Mini-PIM and their properties.

<table>
<thead>
<tr>
<th>Profiles</th>
<th>Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>8a</td>
<td>50</td>
</tr>
<tr>
<td>8b</td>
<td>50</td>
</tr>
<tr>
<td>8c</td>
<td>50</td>
</tr>
<tr>
<td>8d</td>
<td>50</td>
</tr>
<tr>
<td>12a</td>
<td>68</td>
</tr>
<tr>
<td>12b</td>
<td>68</td>
</tr>
<tr>
<td>17a</td>
<td>100</td>
</tr>
<tr>
<td>Auto</td>
<td>Auto mode (default)</td>
</tr>
</tbody>
</table>

**Supported Features**

The following features are supported on the VDSL2 Mini-PIM:

- ADSL/ADSL2/ADSL2+ backward compatibility with Annex-A, Annex-M support
- PTM or EFM (802.3ah) support
- Operation, Administration, and Maintenance (OAM) support for ADSL/ADSL/ADSL2+ mode
- ATM quality of service (QoS) (supported only when the VDSL2 Mini-PIM is operating in ADSL2 mode)
- Multilink Point-to-Point Protocol (MLPPP) (supported only when the VDSL2 Mini-PIM is operating in ADSL2 mode)
MTU size of 1500 bytes (maximum)

Support for maximum of 10 permanent virtual connections (PVCs) (only in ADSL/ADSL2/ADSL2+ mode)

Dying gasp support (ADSL and VDSL2 mode)

Related Topics

- ADSL Interface Overview on page 34
- Configuring the VDSL2 Interface with the CLI Configuration Editor on page 189

DOCSIS Mini-PIM Interface Overview

This section includes the following topics:

- Introduction on page 45
- Configuring DOCSIS Mini-PIM on page 46

Introduction

Data over Cable Service Interface Specifications (DOCSIS) define the communications and operation support interface requirements for a data-over-cable system. DOCSIS is used by cable operators to provide Internet access over their existing cable infrastructure for both residential and business customers. DOCSIS 3.0 is the latest interface standard allowing channel bonding to deliver speeds higher than 100 Mbps throughput in either direction, far surpassing other WAN technologies such as T1/E1, ADSL2+, ISDN, and DS3.

DOCSIS network architecture includes a cable modem on SRX Series Services Gateways with a DOCSIS Mini-Physical Interface Module (Mini-PIM) located at customer premises and a cable modem termination system (CMTS) located at the head-end or data center locations. Standards-based DOCSIS 3.0 Mini-PIM is interoperable with CMTS equipments. The DOCSIS Mini-PIM provides backward compatibility with CMTS equipment based on the following standards:

- DOCSIS 2.0
- DOCSIS 1.1
- DOCSIS 1.0

DOCSIS Mini-PIM is supported on SRX210 and SRX240 Services Gateways.

Software Features Supported on DOCSIS Mini-PIMs

Table 14 on page 46 lists the software features related to DOCSIS Mini-PIMs.
Table 14: Software Features Supported on DOCSIS Mini-PIMs

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP and DHCPv6 Clients</td>
<td>DHCP and DHCPv6 clients are used to get the IP address from the CMTS by using DHCP protocol. DHCP is supported on IPv4 and IPv6. One of the main components of the configuration file is the static public IP address, which CMTS assigns to the cable modem. The management IP address is configured on the Mini-PIM’s hybrid fiber coaxial (HFC) interface, which performs the following tasks:</td>
</tr>
<tr>
<td></td>
<td>- CMTS executes remote monitoring and management of the Mini-PIM’s cable interface.</td>
</tr>
<tr>
<td></td>
<td>- Downloads the configuration file from CMTS and uses it for configuring the cable interface.</td>
</tr>
<tr>
<td>QoS Support</td>
<td>The SRX Series device Routing Engine is configured through the existing QoS CLI. Because the configuration on the SRX Series device Routing Engine and Mini-PIM is done together, the QoS configuration has to be consistent between the SRX Series Routing Engine and the cable modem interface. The QoS mechanisms on the SRX Series Routing Engine are decoupled from the QoS mechanisms on the Mini-PIM. The configuration file downloaded from CMTS contains parameters for primary and secondary flows. These parameters are programmed in the DOCSIS Mini-PIM. The Mini-PIM sends these parameters to the SRX Series Routing Engine through the PIM infrastructure. The secondary flows are prioritized over primary flows in the DOCSIS Mini-PIM.</td>
</tr>
<tr>
<td>SNMP Support</td>
<td>The SNMP requests are issued by CMTS and go to the cable modem. The DOCSIS MIB on the SRX Series device Routing Engine displays the Ethernet interface of the cable modem. The following features are supported on the DOCSIS Mini-PIM:</td>
</tr>
<tr>
<td></td>
<td>- NAT support</td>
</tr>
<tr>
<td></td>
<td>- Dying gasp support</td>
</tr>
<tr>
<td></td>
<td>- Back pressure information</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the DOCSIS Mini-PIM is statically set at the factory and cannot be changed. The MAC address is retrieved from the Mini-PIM and assigned to the cable modem interface in the JUNOS Software.</td>
</tr>
<tr>
<td>Transparent Bridging</td>
<td>The DOCSIS Mini-PIM performs transparent bridging by sending the packets received on the Ethernet interface with the SRX Series device to the HFC interface and vice versa, without any modifications to the packet. All the other services such as webservice, DHCP server, and DNS server are disabled on the DOCSIS Mini-PIM during transparent bridging.</td>
</tr>
</tbody>
</table>

Configuring DOCSIS Mini-PIM

The cable modem interface of Mini-PIM is managed and monitored by CMTS through SNMP. This DOCSIS 3.0 Mini-PIM can be deployed in any multiple service operator (MSO) networks. The primary application is for distributed enterprise offices to connect to a CMTS network through the DOCSIS 3.0 (backward compatible to 2.0, 1.1, and 1.0) interface. The DOCSIS Mini-PIM uses PIM infrastructure developed for third-party PIMs.

The Mini-PIM can also be used with encapsulations other than GRE, PPPoE, and IP-in-IP.

Figure 10 on page 47 illustrates a typical use of this Mini-PIM in a multiple service operator (MSO) network.
The 10 Gigabit Ethernet (10GBASE-T), based on the IEEE 802.3a standard, is a telecommunication technology that offers data speeds up to 10 billion bits per second. The 10 Gigabit Ethernet is used to interconnect LANs, WANs, and metropolitan area networks (MANs). The 2-Port 10 Gigabit Ethernet XPIM can provide multiple service levels (1 Gigabit Ethernet to 10 Gigabit Ethernet in increments) and a single connection option for a wide range of customer needs and applications.

2-Port 10 Gigabit Ethernet XPIM Overview

- 10 Gigabit Ethernet Interface Overview on page 47
- 2-Port Gigabit Ethernet XPIM Overview on page 47
- 2-Port 10 Gigabit Ethernet XPIM Terminology on page 48
- Supported Features on page 49

10 Gigabit Ethernet Interface Overview

The 10 Gigabit Ethernet (10GBASE-T), based on the IEEE 802.3a standard, is a telecommunication technology that offers data speeds up to 10 billion bits per second.

The 10 Gigabit Ethernet is used to interconnect LANs, WANs, and metropolitan area networks (MANs). The 2-Port 10 Gigabit Ethernet XPIM can provide multiple service levels (1 Gigabit Ethernet to 10 Gigabit Ethernet in increments) and a single connection option for a wide range of customer needs and applications.

2-Port Gigabit Ethernet XPIM Overview

The 2-Port 10 Gigabit Ethernet XPIM is supported on the SRX650 Services Gateway.

The 2-Port 10 Gigabit Ethernet XPIM is a 2 x 10BASE-T / SFP+ XPIM line card that includes the following ports:
- 2 X copper ports. The copper ports support 10GBASE-T running with CAT6A or CAT7 Ethernet cable for up to 100 meters.
- 2 X fiber (SFP+) ports. The fiber ports support SFP+ multiple 10G modules.

**NOTE:**
- On the 2-Port 10 Gigabit Ethernet XPIM, one copper port and one fiber port is grouped together as port 0, and another copper port and fiber port are grouped as port 1.
- Only two ports can be active at the same time (one port from port 0 and another port from port 1).
- The 2-Port 10 Gigabit Ethernet XPIM can be configured to operate in two copper mode, two fiber mode, or mixed mode (one copper and one fiber). In mixed mode, two ports should be from different port groups (one port from port 0 and one port from port 1).
- The ports support the following link speeds for copper and fiber:
  - Copper – 10/100/1000Mbps/10G (full-duplex). Half duplex is only for 10/100 Mbps.
  - Fiber – 1000Mbps/10G (full-duplex)

### 2-Port 10 Gigabit Ethernet XPIM Terminology

Table 15 on page 48 lists the terms related to 2-Port 10 Gigabit Ethernet XPIM technology.

**Table 15: 2-Port 10 Gigabit Ethernet XPIM Terminology**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>10GBASE-T or IEEE 802.3an</td>
<td>Standard Ethernet specification that provides 10 Gbps connections over unshielded or shielded twisted pair cables.</td>
</tr>
<tr>
<td>1000BASE-T IEEE 802.3ab</td>
<td>Standard Ethernet specification that provides 1 Gbps connections over twisted pair.</td>
</tr>
<tr>
<td>100BASE-T IEEE 802.3u</td>
<td>Standard Ethernet specification that provides 100 Mbps connections over twisted pair.</td>
</tr>
<tr>
<td>SFP+</td>
<td>Fiber optic transceiver module designed for 10 Gigabit Ethernet and 8.5 Gbps fiber channel systems.</td>
</tr>
<tr>
<td>XPIM</td>
<td>Physical Interface Modules (PiMs) that provides 10 Gigabit Ethernet front end interface connection.</td>
</tr>
</tbody>
</table>
Supported Features

The following features are supported on the 2-Port 10 Gigabit Ethernet XPIM:

- Multiple SFP+ 10G modules support. The following SFP modules are supported:
  - SFPP-10GE-SR
  - SFPP-10GE-LR
  - SFPP-10GE-ER
  - SFPP-10GE-LRM
- Support for Copper TWIN-AX 1M and Copper TWIN-AX 3M
- Online Insertion and Removal (OIR) functionality
- Link speeds of up to 10 gigabits/second
- Full-duplex and half-duplex modes
- Flow control
- Autonegotiation and autosensing
- Support quality of service (QoS)

**NOTE:** By default, flow control is enabled on all ports, and link speed of 10 Gbps in full duplex is supported. By default autonegotiation disabled on the fiber ports whereas it is enabled on copper ports.

**NOTE:** Autonegotiation is not supported when the 2-Port 10 Gigabit Ethernet XPIM is operating in fiber mode at link speed of 10 Gbps.

ISDN Interface Overview

The Integrated Services Digital Network (ISDN) technology is a design for a completely digital telecommunications network. ISDN can carry voice, data, images, and video across a telephony network, using a single interface for all transmissions.

**ISDN Channels**

ISDN uses separate channels to transmit voice and data over the network. Channels operate at bandwidths of either 64 Kbps or 16 Kbps, depending on the type of channel.

Bearer channels (B-channels) use 64 Kbps to transmit voice, data, video, or multimedia information. This bandwidth is derived from the fact that analog voice lines are sampled at a rate of 64 Kbps (8,000 samples per second using 8 bits per sample).
Delta channels (D-channels) are control channels that operate at either 16 Kbps or 64 Kbps. D-channels are used primarily for ISDN signaling between switching equipment in an ISDN network.

**ISDN Interfaces**

ISDN provides two basic types of service, Basic Rate Interface (BRI) and Primary Rate Interface (PRI). J Series devices support both ISDN BRI and ISDN PRI.

ISDN BRI is designed for high-bandwidth data transmissions through existing telephone lines. The copper wires that make up much of the existing telephony infrastructure can support approximately 160 Kbps, which provides enough bandwidth for two B-channels and a D-channel, leaving 16 Kbps for any data framing, maintenance, and link control overhead.

ISDN PRI is designed for users with greater capacity requirements than can be met with ISDN BRI. In the United States, the most common PRI supports 23 B-channels and 1 D-channel, totalling 1,536 Kbps, which is roughly equivalent to a T1 link. In Europe, the most common PRI supports 30 B-channels and 1 D-channel, totalling 1,984 Kbps, which is roughly equivalent to an E1 link.

**Typical ISDN Network**

Figure 11 on page 50 shows a typical ISDN network.

In Figure 11 on page 50, two types of end-user devices are connected to the ISDN network:

- Terminal equipment type 1 (TE1) device—Designed to connect directly through an ISDN telephone line.
- Terminal equipment type 2 (TE2) device—Not designed for ISDN. TE2 devices—for example, analog telephones or modems—must connect to the ISDN network through a terminal adapter (TA).
A terminal adapter allows non-ISDN devices on the ISDN network.

**NT Devices and S and T Interfaces**

The interface between the ISDN network and a TE1 device or terminal adapter is called an S interface. The S interface connects to a network termination type 2 (NT2) device such as a PBX, or directly to the TE1 device or terminal adapter, as shown in Figure 11 on page 50. The NT2 device is then connected to a network termination type 1 (NT1) device through a T interface. The S and T interfaces are electrically equivalent.

An NT1 device is a physical layer device that connects a home telephone network to a service provider carrier network. ISDN devices that connect to an NT1 device from the home network side use a 4-wire S/T interface. The NT1 device converts the 4-wire S/T interface into the 2-wire U interface that telephone carriers use as their plain old telephone service (POTS) lines.

In the United States, NT1 devices are user owned. In many other countries, NT1 devices are owned by the telephone service providers.

**U Interface**

The U interface connects the ISDN network into the telephone switch through line termination (LT) equipment. The connection from LT equipment to other switches within the telephone network is called the exchange termination (ET).

**ISDN Call Setup**

Before traffic can pass through an ISDN network, an ISDN call must be set up. ISDN call setup requires a Layer 2 connection to be initialized and then a Layer 3 session to be established over the connection.

To specify the services and features to be provided by the service provider switch, you must set service profile identifiers (SPIDs) on TE1 devices before call setup and initialization. If you define SPIDs for features that are not available on the ISDN link, Layer 2 initialization takes place, but a Layer 3 connection is not established.

**Layer 2 ISDN Connection Initialization**

The TE device and the telephone network initialize a Layer 2 connection for ISDN as follows:

1. The TE device and the telephone network exchange Receive Ready (RR) frames, to indicate that they are available for data transmission. A call cannot be set up if either the TE device or telephone network does not transmit RR frames.

2. If both ends of the ISDN connection are available to receive data, the TE device sends an Unnumbered Information (UI) frame to all devices on the ISDN link.

3. When it receives the UI frame, the network responds with a message containing a unique terminal endpoint identifier (TEI) that identifies the endpoint on the ISDN link for all subsequent data transmissions.

4. When the TE device receives the TEI message, it sends out a call setup message.
5. The network sends an acknowledgement of the call setup message.
6. When the TE device receives the acknowledgement, a Layer 2 connection is initialized on the ISDN link.

Layer 3 ISDN Session Establishment

The caller, switch, and receiver establish a Layer 3 ISDN connection as follows:
1. When a Layer 2 connection is initialized, the caller sends a SETUP message to the switch in the telephone network.
2. If the setup is message is valid, the switch responds with a call proceeding (CALL PROC) message to the caller and a SETUP message to the receiver.
3. When the receiver receives the SETUP message, it responds with an ALERTING message to the telephone switch.
4. This ALERTING message is then forwarded to the caller.
5. The receiver then accepts the connection by sending a CONNECT message to the switch.
6. The switch forwards the CONNECT message to the caller.
7. The caller responds with an acknowledgement message (CONNECT ACK).
8. When the CONNECT ACK message is received by the receiver, the ISDN call is set up and traffic can pass.

Interface Physical Properties

The physical properties of a network interface are the characteristics associated with the physical link that affect the transmission of either link-layer signals or the data across the links. Physical properties include clocking properties, transmission properties, such as the maximum transmission unit (MTU), and encapsulation methods, such as point-to-point and Frame Relay encapsulation.

The default property values for an interface are usually sufficient to successfully enable a bidirectional link. However, if you configure a set of physical properties on an interface, those same properties must be set on all adjacent interfaces to which a direct connection is made.

Table 16 on page 52 summarizes some key physical properties of device interfaces.

<table>
<thead>
<tr>
<th>Physical Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bert-error-rate</td>
<td>Bit error rate (BER). The error rate specifies the number of bit errors in a particular bit error rate test (BERT) period required to generate a BERT error condition. See “Bit Error Rate Testing” on page 53.</td>
</tr>
<tr>
<td>bert-period</td>
<td>Bit error rate test (BERT) time period over which bit errors are sampled. See “Bit Error Rate Testing” on page 53.</td>
</tr>
</tbody>
</table>
### Table 16: Interface Physical Properties (continued)

<table>
<thead>
<tr>
<th>Physical Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clocking</td>
<td>Clock source for the link. Clocking can be provided by the local system (internal) or a remote endpoint on the link (external). By default, all interfaces use the internal clocking mode. If an interface is configured to accept an external clock source, one adjacent interface must be configured to act as a clock source. Under this configuration, the interface operates in a loop timing mode, in which the clocking signal is unique for that individual network segment or loop. See “Interface Clocking” on page 54.</td>
</tr>
<tr>
<td>description</td>
<td>A user-defined text description of the interface, often used to describe the interface's purpose.</td>
</tr>
<tr>
<td>disable</td>
<td>Administratively disables the interface.</td>
</tr>
<tr>
<td>encapsulation</td>
<td>Type of encapsulation on the interface. Common encapsulation types include PPP, Frame Relay, Cisco HDLC, and PPP over Ethernet (PPPoE). See “Physical Encapsulation on an Interface” on page 57.</td>
</tr>
<tr>
<td>fcs</td>
<td>Frame check sequence (FCS). FCS is an error-detection scheme that appends parity bits to a digital signal and uses decoding algorithms that detect errors in the received digital signal. See “Frame Check Sequences” on page 55.</td>
</tr>
<tr>
<td>mtu</td>
<td>Maximum transmission unit (MTU) size. The MTU is the largest size packet or frame, specified in bytes or octets, that can be sent in a packet-based or frame-based network. The Transmission Control Protocol (TCP) uses the MTU to determine the maximum size of each packet in any transmission. For MTU values on J Series interfaces, see “MTU Default and Maximum Values” on page 56.</td>
</tr>
<tr>
<td>no-keepalives</td>
<td>Disabling of keepalive messages across a physical link. A keepalive message is sent between network devices to indicate that they are still active. Keepalives help determine whether the interface is operating correctly. Except for ATM-over-ADSL interfaces, all interfaces use keepalives by default.</td>
</tr>
<tr>
<td>pap</td>
<td>Password Authentication Protocol (PAP). Specifying <code>pap</code> enables PAP authentication on the interface. To configure PAP, use the CLI or J-Web configuration editor. PAP is not available in the J-Web Quick Configuration pages.</td>
</tr>
<tr>
<td>payload-scrambler</td>
<td>Scrambling of traffic transmitted out the interface. Payload scrambling randomizes the data payload of transmitted packets. Scrambling eliminates nonvariable bit patterns (strings of all 1s or all 0s) that generate link-layer errors across some physical links.</td>
</tr>
</tbody>
</table>

### Bit Error Rate Testing

In telecommunication transmission, the bit error rate (BER) is the percentage of bits that have errors compared to the total number of bits received in a transmission, usually expressed as 10 to a negative power. For example, a transmission with a BER of $10^{-6}$ received 1 errored bit in 1,000,000 bits transmitted. The BER indicates how often a packet or other data unit must be retransmitted because of an error. If the BER is too high, a slower data rate might improve the overall transmission time for a given amount of data if it reduces the BER and thereby lowers the number of resent packets.
A bit error rate test (BERT) is a procedure or device that measures the BER for a given transmission. You can configure a device to act as a BERT device by configuring the interface with a bit error rate and a testing period. When the interface receives a BERT request from a BER tester, it generates a response in a well-known BERT pattern. The initiating device checks the BERT-patterned response to determine the number of bit errors.

**Interface Clocking**

Clocking determines how individual routing nodes or entire networks sample transmitted data. As streams of information are received by a device in a network, a clock source specifies when to sample the data. In asynchronous networks, the clock source is derived locally, and synchronous networks use a central, external clock source. Interface clocking indicates whether the device uses asynchronous or synchronous clocking.

NOTE: Because truly synchronous networks are difficult to design and maintain, most synchronous networks are really plesiochronous networks. In a plesiochronous network, different timing regions are controlled by local clocks that are synchronized (with very narrow constraints). Such networks approach synchronicity and are generally known as synchronous networks.

Most networks are designed to operate as asynchronous networks. Each device generates its own clock signal, or devices use clocks from more than one clock source. The clocks within the network are not synchronized to a single clock source. By default, devices generate their own clock signals to send and receive traffic.

The system clock allows the device to sample (or detect) and transmit data being received and transmitted through its interfaces. Clocking enables the device to detect and transmit the 0s and 1s that make up digital traffic through the interface. Failure to detect the bits within a data flow results in dropped traffic.

Short-term fluctuations in the clock signal are known as clock jitter. Long-term variations in the signal are known as clock wander.

Asynchronous clocking can either derive the clock signal from the data stream or transmit the clocking signal explicitly.

**Data Stream Clocking**

Common in T1 links, data stream clocking occurs when separate clock signals are not transmitted within the network. Instead, devices must extract the clock signal from the data stream. As bits are transmitted across the network, each bit has a time slot of 648 nanoseconds. Within a time slot, pulses are transmitted with alternating voltage peaks and drops. The receiving device uses the period of alternating voltages to determine the clock rate for the data stream.
Explicit Clocking Signal Transmission

Clock signals that are shared by hosts across a data link must be transmitted by one or both endpoints on the link. In a serial connection, for example, one host operates as a clock master and the other operates as a clock slave. The clock master internally generates a clock signal that is transmitted across the data link. The clock slave receives the clock signal and uses its period to determine when to sample data and how to transmit data across the link.

This type of clock signal controls only the connection on which it is active and is not visible to the rest of the network. An explicit clock signal does not control how other devices or even other interfaces on the same device sample or transmit data.

Frame Check Sequences

All packets or frames within a network can be damaged by crosstalk or interference in the network’s physical wires. The frame check sequence (FCS) is an extra field in each transmitted frame that can be analyzed to determine if errors have occurred. The FCS uses cyclic redundancy checks (CRCs), checksums, and two-dimensional parity bits to detect errors in the transmitted frames.

Cyclic Redundancy Checks and Checksums

On a link that uses CRCs for frame checking, the data source uses a predefined polynomial algorithm to calculate a CRC number from the data it is transmitting. The result is included in the FCS field of the frame and transmitted with the data. On the receiving end, the destination host performs the same calculation on the data it receives.

If the result of the second calculation matches the contents of the FCS field, the packet was sent and received without bit errors. If the values do not match, an FCS error is generated, the frame is discarded and the originating host is notified of the error.

Checksums function similarly to CRCs, but use a different algorithm.

Two-Dimensional Parity

On a link that uses two-dimensional parity bits for frame checking, the sending and receiving hosts examine each frame in the total packet transmission and create a parity byte that is evaluated to detect transmission errors.

For example, a host can create the parity byte for the following frame sequence by summing up each column (each bit position in the frame) and keeping only the least-significant bit:

Frame 1   0 1 0 1 0 0 1
Frame 2   1 1 0 1 0 0 1
Frame 3   1 0 1 1 1 1 0
Frame 4   0 0 0 1 1 1 0
Frame 5   0 1 1 0 1 0 0
Frame 6: 1 0 1 1 1 1 1
Parity Byte: 1 1 1 0 1 1 1

If the sum of the bit values in a bit position is even, the parity bit for the position is 0. If the sum is odd, the parity bit is 1. This method is called even parity. Matching parity bytes on the originating and receiving hosts indicate that the packet was received without error.

**MTU Default and Maximum Values**

Table 17 on page 56 lists MTU values for J Series devices.

**Table 17: MTU Values for J2320, J2350, J4350, and J6350 Interfaces**

<table>
<thead>
<tr>
<th>J4350 and J6350 Interfaces</th>
<th>Default Media MTU (bytes)</th>
<th>Maximum MTU (bytes)</th>
<th>Default IP MTU (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigabit Ethernet (10/100/1000) built-in interface</td>
<td>1514</td>
<td>9018</td>
<td>1500</td>
</tr>
<tr>
<td>6-Port, 8-Port, and 16-Port Gigabit Ethernet uPIMs</td>
<td>1514</td>
<td>9014</td>
<td>1500</td>
</tr>
<tr>
<td>Gigabit Ethernet (10/100/1000) ePIM</td>
<td>1514</td>
<td>9018</td>
<td>1500</td>
</tr>
<tr>
<td>Gigabit Ethernet (10/100/1000) SFP ePIM</td>
<td>1514</td>
<td>9018</td>
<td>1500</td>
</tr>
<tr>
<td>4-Port Fast Ethernet (10/100) ePIM</td>
<td>1514</td>
<td>1514</td>
<td>1500</td>
</tr>
<tr>
<td>Dual-Port Fast Ethernet (10/100) PIM</td>
<td>1514</td>
<td>9192</td>
<td>1500</td>
</tr>
<tr>
<td>Dual-Port Serial PIM</td>
<td>1504</td>
<td>9150</td>
<td>1500</td>
</tr>
<tr>
<td>Dual-Port T1 or E1 PIM</td>
<td>1504</td>
<td>9192</td>
<td>1500</td>
</tr>
<tr>
<td>Dual-Port Channelized T1/E1/ISDN PRI PIM (channelized to DS0s)</td>
<td>1504</td>
<td>4500</td>
<td>1500</td>
</tr>
<tr>
<td>Dual-Port Channelized T1/E1/ISDN PRI PIM (clear-channel T1 or E1)</td>
<td>1504</td>
<td>9150</td>
<td>1500</td>
</tr>
<tr>
<td>Dual-Port Channelized T1/E1/ISDN PRI PIM (ISDN PRI dialer interface)</td>
<td>1504</td>
<td>4098</td>
<td>1500</td>
</tr>
<tr>
<td>T3 (DS3) or E3 PIM</td>
<td>4474</td>
<td>9192</td>
<td>4470</td>
</tr>
<tr>
<td>4-Port ISDN BRI PIM</td>
<td>1504</td>
<td>4092</td>
<td>1500</td>
</tr>
<tr>
<td>ADSL+2 PIM</td>
<td>4482</td>
<td>9150</td>
<td>4470</td>
</tr>
<tr>
<td>G.SHDSL PIM</td>
<td>4482</td>
<td>9150</td>
<td>4470</td>
</tr>
</tbody>
</table>
**Physical Encapsulation on an Interface**

Encapsulation is the process by which a lower-level protocol accepts a message from a higher-level protocol and places it in the data portion of the lower-level frame. As a result, datagrams transmitted through a physical network have a sequence of headers: the first header for the physical network (or data link layer) protocol, the second header for the network layer protocol (IP, for example), the third header for the transport protocol, and so on.

The following encapsulation protocols are supported on device physical interfaces:

- Frame Relay on page 57
- Point-to-Point Protocol on page 59
- Point-to-Point Protocol over Ethernet on page 61
- High-Level Data Link Control on page 63

**Frame Relay**

The Frame Relay packet-switching protocol operates at the physical and data link layers in a network to optimize packet transmissions by creating virtual circuits between hosts. Figure 12 on page 57 shows a typical Frame Relay network.

**Figure 12: Frame Relay Network**

Figure 12 on page 57 shows multiple paths from Host A to Host B. In a typical routed network, traffic is sent from device to device with each device making routing decisions based on its own routing table. In a packet-switched network, the paths are predefined. Devices switch a packet through the network according to predetermined next-hops established when the virtual circuit is set up.
**Virtual Circuits**

A virtual circuit is a bidirectional path between two hosts in a network. Frame Relay virtual circuits are logical connections between two hosts that are established either by a call setup mechanism or by explicit configuration.

A virtual circuit created through a call setup mechanism is known as a switched virtual circuit (SVC). A virtual circuit created through explicit configuration is called a permanent virtual circuit (PVC).

**Switched and Permanent Virtual Circuits**

Before data can be transmitted across an SVC, a signaling protocol like ISDN must set up a call by the exchange of setup messages across the network. When a connection is established, data is transmitted across the SVC. After data transmission, the circuit is torn down and the connection is lost. For additional traffic to pass between the same two hosts, a subsequent SVC must be established, maintained, and terminated.

Because PVCs are explicitly configured, they do not require the setup and teardown of SVCS. Data can be switched across the PVC whenever a host is ready to transmit. SVCs are useful in networks where data transmission is sporadic and a permanent circuit is not needed.

**Data-Link Connection Identifiers**

An established virtual circuit is identified by a data-link connection identifier (DLCI). The DLCI is a value from 16 through 1022. (Values 1 through 15 are reserved.) The DLCI uniquely identifies a virtual circuit locally so that devices can switch packets to the appropriate next-hop address in the circuit. Multiple paths that pass through the same transit devices have different DLCIs and associated next-hop addresses.

**Congestion Control and Discard Eligibility**

Frame Relay uses the following types of congestion notification to control traffic within a Frame Relay network. Both are controlled by a single bit in the Frame Relay header.

- Forward-explicit congestion notification (FECN)
- Backward-explicit congestion notification (BECN)

Traffic congestion is typically defined in the buffer queues on a device. When the queues reach a predefined level of saturation, traffic is determined to be congested. When traffic congestion occurs in a virtual circuit, the device experiencing congestion sets the congestion bits in the Frame Relay header to 1. As a result, transmitted traffic has the FECN bit set to 1, and return traffic on the same virtual circuit has the BECN bit set to 1.

When the FECN and BECN bits are set to 1, they provide a congestion notification to the source and destination devices. The devices can respond in either of two ways:
to control traffic on the circuit by sending it through other routes, or to reduce the load on the circuit by discarding packets.

If devices discard packets as a means of congestion (flow) control, Frame Relay uses the discard eligibility (DE) bit to give preference to some packets in discard decisions. A DE value of 1 indicates that the frame is of lower importance than other frames and more likely to be dropped during congestion. Critical data (such as signaling protocol messages) without the DE bit set is less likely to be dropped.

**Point-to-Point Protocol**

The Point-to-Point Protocol (PPP) is an encapsulation protocol for transporting IP traffic across point-to-point links. PPP is made up of three primary components:

- Link control protocol (LCP)—Establishes working connections between two points.
- Authentication protocols—Enable secure connections between two points.
- Network control protocols (NCPs)—Initialize the PPP protocol stack to handle multiple network layer protocols, such as IPv4, IPv6, and Connectionless Network Protocol (CLNP).

**Link Control Protocol**

LCP is responsible for establishing, maintaining, and tearing down a connection between two endpoints. LCP also tests the link and determines whether it is active. LCP establishes a point-to-point connection as follows:

1. LCP must first detect a clocking signal on each endpoint. However, because the clocking signal can be generated by a network clock and shared with devices on the network, the presence of a clocking signal is only a preliminary indication that the link might be functioning.
2. When a clocking signal is detected, a PPP host begins transmitting PPP Configure-Request packets.
3. If the remote endpoint on the point-to-point link receives the Configure-Request packet, it transmits a Configure-Acknowledgement packet to the source of the request.
4. After receiving the acknowledgement, the initiating endpoint identifies the link as established. At the same time, the remote endpoint sends its own request packets and processes the acknowledgement packets. In a functioning network, both endpoints treat the connection as established.

During connection establishment, LCP also negotiates connection parameters such as FCS and HDLC framing. By default, PPP uses a 16-bit FCS, but you can configure PPP to use either a 32-bit FCS or a 0-bit FCS (no FCS). Alternatively, you can enable HDLC encapsulation across the PPP connection.

After a connection is established, PPP hosts generate Echo-Request and Echo-Response packets to maintain a PPP link.
PPP Authentication

PPP's authentication layer uses a protocol to help ensure that the endpoint of a PPP link is a valid device. Authentication protocols include the Password Authentication Protocol (PAP), the Extensible Authentication Protocol (EAP), and the Challenge Handshake Authentication Protocol (CHAP). CHAP is the most commonly used.

NOTE: EAP is not currently supported on J Series devices. PAP is supported, but must be configured from the CLI or J-Web configuration editor. PAP is not configurable from the J-Web Quick Configuration pages.

CHAP ensures secure connections across PPP links. After a PPP link is established by LCP, the PPP hosts at either end of the link initiate a three-way CHAP handshake. Two separate CHAP handshakes are required before both sides identify the PPP link as established.

CHAP configuration requires each endpoint on a PPP link to use a shared secret (password) to authenticate challenges. The shared secret is never transmitted over the wire. Instead, the hosts on the PPP connection exchange information that enables both to determine that they share the same secret. Challenges consist of a hash function calculated from the secret, a numeric identifier, and a randomly chosen challenge value that changes with each challenge. If the response value matches the challenge value, authentication is successful. Because the secret is never transmitted and is required to calculate the challenge response, CHAP is considered very secure.

PAP authentication protocol uses a simple 2-way handshake to establish identity. PAP is used after the link establishment phase (LCP up), during the authentication phase. JUNOS Software can support PAP in one direction (egress or ingress), and CHAP in the other.

Network Control Protocols

After authentication is completed, the PPP connection is fully established. At this point, any higher-level protocols (for example, IP protocols) can initialize and perform their own negotiations and authentication.

PPP NCPs include support for the following protocols. IPCP and IPV6CP are the most widely used on J Series devices.

- ATCP—AppleTalk Control Protocol
- BCP—Bridging Control Protocol
- BVCP—Banyan Vines Control Protocol
- DNCP—DECnet Phase IV Control Protocol
- IPCP—IP Control Protocol
- IPV6CP—IPv6 Control Protocol
- IPXCP—Novell IPX Control Protocol
- LECP—LAN Extension Control Protocol
- NBFCP—NetBIOS Frames Control Protocol
- OSINLCP—OSI Network Layer Control Protocol (includes IS-IS, ES-IS, CLNP, and IDRP)
- SDTP—Serial Data Transport Protocol
- SNACP—Systems Network Architecture (SNA) Control Protocol
- XNSCP—Xerox Network Systems (XNS) Internet Datagram Protocol (IDP) Control Protocol

Magic Numbers

Hosts running PPP can create “magic” numbers for diagnosing the health of a connection. A PPP host generates a random 32-bit number and sends it to the remote endpoint during LCP negotiation and echo exchanges.

In a typical network, each host's magic number is different. A magic number mismatch in an LCP message informs a host that the connection is not in loopback mode and traffic is being exchanged bidirectionally. If the magic number in the LCP message is the same as the configured magic number, the host determines that the connection is in loopback mode, with traffic looped back to the transmitting host.

Looping traffic back to the originating host is a valuable way to diagnose network health between the host and the loopback location. To enable loopback testing, telecommunications equipment typically supports channel service unit/data service unit (CSU/DSU) devices.

CSU/DSU Devices

A channel service unit (CSU) connects a terminal to a digital line. A data service unit (DSU) performs protective and diagnostic functions for a telecommunications line. Typically, the two devices are packaged as a single unit. A CSU/DSU device is required for both ends of a T1 or T3 connection, and the units at both ends must be set to the same communications standard.

A CSU/DSU device enables frames sent along a link to be looped back to the originating host. Receipt of the transmitted frames indicates that the link is functioning correctly up to the point of loopback. By configuring CSU/DSU devices to loop back at different points in a connection, network operators can diagnose and troubleshoot individual segments in a circuit.

Point-to-Point Protocol over Ethernet

Point-to-Point Protocol over Ethernet (PPPoE) combines PPP, which is typically run over broadband connections, with the Ethernet link-layer protocol that allows users to connect to a network of hosts over a bridge or access concentrator. PPPoE enables service providers to maintain access control through PPP connections and also manage multiple hosts at a remote site.

To provide a PPPoE connection, each PPP session must learn the Ethernet address of the remote peer and establish a unique session identifier during the PPPoE discovery and session stages.
**PPPoE Discovery**

To initiate a PPPoE session, a host must first identify the Ethernet MAC address of the remote peer and establish a unique PPPoE session ID for the session. Learning the remote Ethernet MAC address is called PPPoE discovery.

During the PPPoE discovery process, the host does not discover a remote endpoint on the Ethernet network. Instead, the host discovers the access concentrator through which all PPPoE sessions are established. Discovery is a client/server relationship, with the host (a J Series device) acting as the client and the access concentrator acting as the server.

The PPPoE discovery stage consists of the following steps:

1. **PPPoE Active Discovery Initiation (PADI)**—The client initiates a session by broadcasting a PADI packet to the LAN, to request a service.

2. **PPPoE Active Discovery Offer (PADO)**—Any access concentrator that can provide the service requested by the client in the PADI packet replies with a PADO packet that contains its own name, the unicast address of the client, and the service requested. An access concentrator can also use the PADO packet to offer other services to the client.

3. **PPPoE Active Discovery Request (PADR)**—From the PADOs it receives, the client selects one access concentrator based on its name or the services offered and sends it a PADR packet to indicate the service or services needed.

4. **PPPoE Active Discovery Session-Confirmation (PADS)**—When the selected access concentrator receives the PADR packet, it accepts or rejects the PPPoE session:
   - To accept the session, the access concentrator sends the client a PADS packet with a unique session ID for a PPPoE session and a service name that identifies the service under which it accepts the session.
   - To reject the session, the access concentrator sends the client a PADS packet with a service name error and resets the session ID to zero.

**PPPoE Sessions**

The PPPoE session stage starts after the PPPoE discovery stage is over. Each PPPoE session is uniquely identified by the Ethernet address of the peer and the session ID. After the PPPoE session is established, data is sent as in any other PPP encapsulation. The PPPoE information is encapsulated within an Ethernet frame and is sent to a unicast address. Magic numbers, echo requests, and all other PPP traffic behave exactly as in normal PPP sessions. In this stage, both the client and the server must allocate resources for the PPPoE logical interface.

After a session is established, the client or the access concentrator can send a PPPoE Active Discovery Termination (PADT) packet anytime to terminate the session. The PADT packet contains the destination address of the peer and the session ID of the session to be terminated. After this packet is sent, the session is closed to PPPoE traffic.
High-Level Data Link Control

High-Level Data Link Control (HDLC) is a bit-oriented, switched and nonswitched link-layer protocol. HDLC is widely used because it supports half-duplex and full-duplex connections, point-to-point and point-to-multipoint networks, and switched and nonswitched channels.

HDLC Stations

Nodes within a network running HDLC are called stations. HDLC supports three types of stations for data link control:

- **Primary stations**—Responsible for controlling the secondary and combined other stations on the link. Depending on the HDLC mode, the primary station is responsible for issuing acknowledgement packets to allow data transmission from secondary stations.

- **Secondary stations**—Controlled by the primary station. Under normal circumstances, secondary stations cannot control data transmission across the link with the primary station, are active only when requested by the primary station, and can respond to the primary station only (not to other secondary stations). All secondary station frames are response frames.

- **Combined stations**—A combination of primary and secondary stations. On an HDLC link, all combined stations can send and receive commands and responses without any permission from any other stations on the link and cannot be controlled by any other station.

HDLC Operational Modes

HDLC runs in three separate modes:

- **Normal Response Mode (NRM)**—The primary station on the HDLC link initiates all information transfers with secondary stations. A secondary station on the link can transmit a response of one or more information frames only when it receives explicit permission from the primary station. When the last frame is transmitted, the secondary station must wait for explicit permission before it can transmit more frames.

  NRM is used most widely for point-to-multipoint links, in which a single primary station controls many secondary stations.

- **Asynchronous Response Mode (ARM)**—The secondary station can transmit either data or control traffic at any time, without explicit permission from the primary station. The primary station is responsible for error recovery and link setup, but the secondary station can transmit information at any time.

  ARM is used most commonly with point-to-point links, because it reduces the overhead on the link by eliminating the need for control packets.

- **Asynchronous Balance Mode (ABM)**—All stations are combined stations. Because no other station can control a combined station, all stations can transmit information without explicit permission from any other station. ABM is not a widely used HDLC mode.
Interface Logical Properties

The logical properties of an interface are the characteristics that do not apply to the physical interface or the wires connected to it. Logical properties include the protocol families running on the interface (including any protocol-specific MTUs), the IP address or addresses associated with the interface, virtual LAN (VLAN) tagging, and any firewall filters or routing policies that are operating on the interface.

The IP specification requires a unique address on every interface of each system attached to an IP network, so that traffic can be correctly routed. Individual hosts such as home computers must have a single IP address assigned. Devices must have a unique IP address for every interface.

This section contains the following topics:
- Protocol Families on page 64
- IPv4 Addressing on page 65
- IPv6 Addressing on page 68
- Virtual LANs on page 72

Protocol Families

A protocol family is a group of logical properties within an interface configuration. Protocol families include all the protocols that make up a protocol suite. To use a protocol within a particular suite, you must configure the entire protocol family as a logical property for an interface. The protocol families include common and not-so-common protocol suites.

Common Protocol Suites

JUNOS protocol families include the following common protocol suites:
- Inet—Supports IP protocol traffic, including Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Internet Control Message Protocol (ICMP).
- Inet6—Supports IPv6 protocol traffic, including Routing Information Protocol for IPv6 (RIPng), Intermediate System-to-Intermediate System (IS-IS), and BGP.
- ISO—Supports IS-IS traffic.
- MPLS—Supports Multiprotocol Label Switching (MPLS).

NOTE: JUNOS Software security features are flow-based—meaning the device sets up a flow in order to examine the traffic. Flow-based processing is not supported for ISO or MPLS protocol families.
Other Protocol Suites

In addition to the common protocol suites, JUNOS protocol families sometimes use the following protocol suites:

- **ccc**—Circuit cross-connect (CCC).
- **mlfr-uni-nni**—Multilink Frame Relay (MLFR) FRF.16 user-to-network network-to-network (UNI NNI).
- **mlfr-end-to-end**—Multilink Frame Relay end-to-end.
- **mlppp**—Multilink Point-to-Point Protocol.
- **tcc**—Translational cross-connect (TCC).
- **tnp**—Trivial Network Protocol. This Juniper Networks proprietary protocol provides communication between the Routing Engine and the device’s packet forwarding components. JUNOS Software automatically configures this protocol family on the device’s internal interfaces only.

IPv4 Addressing

IPv4 addresses are 32-bit numbers that are typically displayed in dotted decimal notation. A 32-bit address contains two primary parts: the network prefix and the host number.

All hosts within a single network share the same network address. Each host also has an address that uniquely identifies it. Depending on the scope of the network and the type of device, the address is either globally or locally unique. Devices that are visible to users outside the network (webservers, for example) must have a globally unique IP address. Devices that are visible only within the network (J Series devices, for example) must have locally unique IP addresses.

IP addresses are assigned by a central numbering authority called the Internet Assigned Numbers Authority (IANA). IANA ensures that addresses are globally unique where needed and has a large address space reserved for use by devices not visible outside their own networks.

IPv4 Classful Addressing

To provide flexibility in the number of addresses distributed to networks of different sizes, 4-octet (32-bit) IP addresses were originally divided into three different categories or classes: class A, class B, and class C. Each address class specifies a different number of bits for its network prefix and host number:

- **Class A addresses** use only the first byte (octet) to specify the network prefix, leaving 3 bytes to define individual host numbers.
- **Class B addresses** use the first 2 bytes to specify the network prefix, leaving 2 bytes to define host addresses.
- **Class C addresses** use the first 3 bytes to specify the network prefix, leaving only the last byte to identify hosts.
In binary format, with an x representing each bit in the host number, the three address classes can be represented as follows:

- 00000000 xxxxxxxx xxxxxxxx xxxxxxxx (Class A)
- 00000000 00000000 xxxxxxxx xxxxxxxx (Class B)
- 00000000 00000000 00000000 xxxxxxxx (Class C)

Because each bit (x) in a host number can have a 0 or 1 value, each represents a power of 2. For example, if only 3 bits are available for specifying the host number, only the following host numbers are possible:

111 110 101 100 011 010 001 000

In each IP address class, the number of host-number bits raised to the power of 2 indicates how many host numbers can be created for a particular network prefix. Class A addresses have $2^{24}$ (or 16,777,216) possible host numbers, class B addresses have $2^{16}$ (or 65,536) host numbers, and class C addresses have $2^{8}$ (or 256) possible host numbers.

**IPv4 Dotted Decimal Notation**

The 32-bit IPv4 addresses are most often expressed in dotted decimal notation, in which each octet (or byte) is treated as a separate number. Within an octet, the rightmost bit represents $2^0$ (or 1), increasing to the left until the first bit in the octet is $2^7$ (or 128). Following are IP addresses in binary format and their dotted decimal equivalents:

```
11010000 01100010 11000000 10101010 = 208.98.192.170
01110110 00001111 11110000 01010101 = 118.15.240.85
00110011 11001100 00111100 00111011 = 51.204.60.59
```

**IPv4 Subnetting**

Because of the physical and architectural limitations on the size of networks, you often must break large networks into smaller subnetworks. Within a network, each wire or ring requires its own network number and identifying subnet address.

Figure 13 on page 67 shows two subnets in a network.
Figure 13 shows three devices connected to one subnet and three more devices connected to a second subnet. Collectively, the six devices and two subnets make up the larger network. In this example, the network is assigned the network prefix 192.14.0.0, a class B address. Each device has an IP address that falls within this network prefix.

In addition to sharing a network prefix (the first two octets), the devices on each subnet share a third octet. The third octet identifies the subnet. All devices on a subnet must have the same subnet address. In this case, the alpha subnet has the IP address 192.14.126.0 and the beta subnet has the IP address 192.14.17.0.

The subnet address 192.14.17.0 can be represented as follows in binary notation:

```
11000000 . 00001110 . 00010001 . x x x x x x
```

Because the first 24 bits in the 32-bit address identify the subnet, the last 8 bits are not significant. To indicate the subnet, the address is written as 192.14.17.0/24 (or just 192.14.17/24). The /24 is the subnet mask (sometimes shown as 255.255.255.0).

### IPv4 Variable-Length Subnet Masks

Traditionally, subnets were divided by address class. Subnets had either 8, 16, or 24 significant bits, corresponding to $2^{24}$, $2^{16}$, or $2^8$ possible hosts. As a result, an entire /16 subnet had to be allocated for a network that required only 400 addresses, wasting 65,136 ($2^{16} - 400 = 65,136$) addresses.

To help allocate address spaces more efficiently, variable-length subnet masks (VLSMs) were introduced. Using VLSM, network architects can allocate more precisely the number of addresses required for a particular subnet.

For example, suppose a network with the prefix 192.14.17/24 is divided into two smaller subnets, one consisting of 18 devices and the other of 46 devices.
To accommodate 18 devices, the first subnet must have \(2^5\) (32) host numbers. Having 5 bits assigned to the host number leaves 27 bits of the 32-bit address for the subnet. The IP address of the first subnet is therefore 192.14.17.128/27, or the following in binary notation:

\[
11000000 \ . \ 00001110 \ . \ 00010001 \ . \ 100xxxxx
\]

The subnet mask includes 27 significant digits.

To create the second subnet of 46 devices, the network must accommodate \(2^6\) (64) host numbers. The IP address of the second subnet is 192.14.17.64/26, or

\[
11000000 \ . \ 00001110 \ . \ 00010001 \ . \ 01xxxxxx
\]

By assigning address bits within the larger /24 subnet mask, you create two smaller subnets that use the allocated address space more efficiently.

**IPv6 Addressing**

To create a much larger address space and relieve a projected future shortage of IP addresses, IPv6 was created. IPv6 addresses consist of 128 bits, instead of 32 bits, and include a scope field that identifies the type of application suitable for the address. IPv6 does not support broadcast addresses, but instead uses multicast addresses for broadcast. In addition, IPv6 defines a new type of address called anycast.

- IPv6 Address Representation on page 68
- IPv6 Address Types on page 69
- IPv6 Address Scope on page 69
- IPv6 Address Structure on page 69
- IPv6 Protocol Family: inet6 on page 70
- Enabling Flow-Based Processing for IPv6 Traffic on page 71

**IPv6 Address Representation**

IPv6 addresses consist of 8 groups of 16-bit hexadecimal values separated by colons (:). IPv6 addresses have the following format:

```
```

Each `aaaa` is a 16-bit hexadecimal value, and each `a` is a 4-bit hexadecimal value. Following is a sample IPv6 address:

```
3ffe:0000:0000:0001:0200:f8ff:fe75:50df
```

You can omit the leading zeros of each 16-bit group, as follows:

```
3ffe:0:0:1:0200:f8ff:fe75:50df
```

You can compress 16-bit groups of zeros to double colons (::) as shown in the following example, but only once per address:

```
3ffe::1:200:f8ff:fe75:50df
```
An IPv6 address prefix is a combination of an IPv6 prefix (address) and a prefix length. The prefix takes the form \( \text{ipv6-prefix}/\text{prefix-length} \) and represents a block of address space (or a network). The \( \text{ipv6-prefix} \) variable follows general IPv6 addressing rules. The \( \text{prefix-length} \) variable is a decimal value that indicates the number of contiguous, higher-order bits of the address that make up the network portion of the address. For example, 10FA:6604:8136:6502::/64 is a possible IPv6 prefix.

For more information on the text representation of IPv6 addresses and address prefixes, see RFC 4291, *IP Version 6 Addressing Architecture*.

**IPv6 Address Types**

IPv6 has three types of addresses:

- **Unicast**—For a single interface.
- **Multicast**—For a set of interfaces on the same physical medium. A packet is sent to all interfaces associated with the address.
- **Anycast**—For a set of interfaces on different physical media. A packet is sent to only one of the interfaces associated with this address, not to all the interfaces.

**IPv6 Address Scope**

Unicast and multicast IPv6 addresses support address scoping, which identifies the application suitable for the address.

Unicast addresses support global address scope and two types of local address scope:

- **Link-local unicast addresses**—Used only on a single network link. The first 10 bits of the prefix identify the address as a link-local address. Link-local addresses cannot be used outside the link.
- **Site-local unicast addresses**—Used only within a site or intranet. A site consists of multiple network links. Site-local addresses identify nodes inside the intranet and cannot be used outside the site.

Multicast addresses support 16 different types of address scope, including node, link, site, organization, and global scope. A 4-bit field in the prefix identifies the address scope.

**IPv6 Address Structure**

Unicast addresses identify a single interface. Each unicast address consists of \( n \) bits for the prefix, and \( 128 - n \) bits for the interface ID.

Multicast addresses identify a set of interfaces. Each multicast address consists of the first 8 bits of all 1s, a 4-bit flags field, a 4-bit scope field, and a 112-bit group ID:

\[
11111111 | \text{flags} | \text{scope} | \text{group ID}
\]

The first octet of 1s identifies the address as a multicast address. The flags field identifies whether the multicast address is a well-known address or a transient...
multicast address. The scope field identifies the scope of the multicast address. The 112-bit group ID identifies the multicast group.

Similar to multicast addresses, anycast addresses identify a set of interfaces. However, packets are sent to only one of the interfaces, not to all interfaces. Anycast addresses are allocated from the normal unicast address space and cannot be distinguished from a unicast address in format. Therefore, each member of an anycast group must be configured to recognize certain addresses as anycast addresses.

**IPv6 Protocol Family: inet6**

A logical interface can be configured with an IPv6 address, IPv4 address, or both.

In configuration commands, the protocol family for IPv6 is named `inet6`. In the configuration hierarchy, instances of `inet6` are parallel to instances of `inet`, the protocol family for IPv4. In general, you configure `inet6` settings and specify IPv6 addresses in parallel to `inet` settings and IPv4 addresses.

The following example shows the CLI commands you use to configure an IPv6 address for an interface:

```
[edit]
user@host# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 10.100.37.178/24;
        }
    }
}

[edit]
user@host# set interfaces ge-0/0/0 unit 0 family ?
Possible completions:
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
> ccc                  Circuit cross-connect parameters
> ethernet-switching   Ethernet switching parameters
> inet                 IPv4 parameters
> inet6                IPv6 protocol parameters
> iso                  OSI ISO protocol parameters
> mpls                 MPLS protocol parameters
> tcc                  Translational cross-connect parameters
> vpls                 Virtual private LAN service parameters

[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet6 address 8d8d:8d01::1/64
user@host# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 10.100.37.178/24;
        }
        family inet6 {
            address 8d8d:8d01::1/64;
        }
    }
}
```
For complete information about configuring interfaces, see the Junos Network Interfaces Configuration Guide.

**Enabling Flow-Based Processing for IPv6 Traffic**

You have the following options for handling IPv6 traffic:

- **Drop**—Do not forward IPv6 packets. This is the default behavior.
- **Packet-based forwarding**—Do not create a session and process according to packet-based features only (includes firewall filters and class of service).
- **Flow-based forwarding**—Create a session and process according to packet-based features (including firewall filters and class of service) but also flow-based security features, such as screens and firewall security policy.

**NOTE:** Packet-based forwarding is not supported for SRX3400, SRX3600, SRX5600, or SRX5800 devices; and the option is unavailable in the CLI.

To enable flow-based processing for IPv6 traffic, modify the `mode` statement at the `[edit security forwarding-options family inet6]` hierarchy level:

```plaintext
security {
    forwarding-options {
        family {
            inet6 {
                mode flow-based;
            }
        }
    }
}
```

The following example shows the CLI commands you use to configure forwarding for IPv6 traffic:

```plaintext
[edit]
user@host# set security forwarding-options family inet6 mode ?
Possible completions:
    drop Disable forwarding
    flow-based Enable flow-based forwarding
    packet-based Enable packet-based forwarding
[edit]
user@host# set security forwarding-options family inet6 mode flow-based
user@host# show security forwarding-options
family {
    inet6 {
        mode flow-based;
    }
}
```

If you change the forwarding option mode for IPv6, you might need to perform a reboot to initialize the configuration change. Table 18 on page 72 summarizes device status upon configuration change.
### Table 18: Device Status Upon Configuration Change

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop to flow-based</td>
<td>Yes</td>
<td>Yes</td>
<td>Dropped</td>
<td>Dropped</td>
</tr>
<tr>
<td>Drop to packet-based</td>
<td>No</td>
<td>No</td>
<td>Packet-based</td>
<td>Packet-based</td>
</tr>
<tr>
<td>Flow-based to packet-based</td>
<td>Yes</td>
<td>Yes</td>
<td>None</td>
<td>Flow sessions created</td>
</tr>
<tr>
<td>Flow-based to drop</td>
<td>Yes</td>
<td>Yes</td>
<td>None</td>
<td>Flow sessions created</td>
</tr>
<tr>
<td>Packet-based to flow-based</td>
<td>Yes</td>
<td>Yes</td>
<td>Packet-based</td>
<td>Packet-based</td>
</tr>
<tr>
<td>Packet-based to drop</td>
<td>No</td>
<td>No</td>
<td>Dropped</td>
<td>Dropped</td>
</tr>
</tbody>
</table>

For details on packet-based and flow-based processing, see the *Junos OS Security Configuration Guide*.

### Virtual LANs

A local area network (LAN) is a single broadcast domain. When traffic is broadcast, all hosts within the LAN receive the broadcast traffic. A LAN is determined by the physical connectivity of devices within the domain.

Within a traditional LAN, hosts are connected by a hub or repeater that propagates any incoming traffic throughout the network. Each host and its connecting hubs or repeaters make up a LAN segment. LAN segments are connected through switches and bridges to form the broadcast domain of the LAN. Figure 14 on page 73 shows a typical LAN topology.
Virtual LANs (VLANs) allow network architects to segment LANs into different broadcast domains based on logical groupings. Because the groupings are logical, the broadcast domains are not determined by the physical connectivity of the devices in the network. Hosts can be grouped according to a logical function, to limit the traffic broadcast within the VLAN to only the devices for which the traffic is intended.

Suppose a corporate network has three major organizations: engineering, sales, and support. Using VLAN tagging, hosts within each organization can be tagged with a different VLAN identifier. Traffic sent to the broadcast domain is then checked against the VLAN identifier and broadcast to only the devices in the appropriate VLAN. Figure 15 on page 73 shows a typical VLAN topology.
**Special Interfaces**

In addition to the configured network interfaces associated with the physical ports and wires that make up much of the network, devices have special interfaces. Table 19 on page 74 lists each special interface and briefly describes its use.

For information about interface names, See “Network Interface Naming” on page 9.

**Table 19: Special Interfaces**

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dsc</td>
<td>Discard interface. See “Discard Interface” on page 76.</td>
</tr>
<tr>
<td>fxp0</td>
<td>In a J Series chassis cluster configuration, configurable management interfaces are created from built-in interfaces on the connected J Series chassis. The fxp0 interface is the management port, and fxp1 is used as the control link interface in a chassis cluster.</td>
</tr>
<tr>
<td></td>
<td>In an SRX Series device, the fxp0 management interface is a dedicated port located on the Routing Engine. In an SRX Series chassis cluster configuration, the control link interface must be port 0 on an SPC. For each node in the chassis cluster, you must configure the SPC that is used for the control link interface.</td>
</tr>
<tr>
<td></td>
<td>For more information about chassis clusters, see the Junos OS Security Configuration Guide.</td>
</tr>
<tr>
<td></td>
<td>For more information about the device management port interfaces, see “Management Interface” on page 77.</td>
</tr>
<tr>
<td>gr-0/0/0</td>
<td>Configurable generic routing encapsulation (GRE) interface. GRE allows the encapsulation of one routing protocol over another routing protocol.</td>
</tr>
<tr>
<td></td>
<td>Within a J Series device, packets are routed to this internal interface, where they are first encapsulated with a GRE packet and then re-encapsulated with another protocol packet to complete the GRE. The GRE interface is an internal interface only and is not associated with a physical medium or PIM. You must configure the interface for it to perform GRE.</td>
</tr>
<tr>
<td>gre</td>
<td>Internally generated GRE interface. This interface is generated by JUNOS Software to handle GRE. It is not a configurable interface.</td>
</tr>
<tr>
<td>ip-0/0/0</td>
<td>Configurable IP-over-IP encapsulation (also called IP tunneling) interface. IP tunneling allows the encapsulation of one IP packet over another IP packet.</td>
</tr>
<tr>
<td></td>
<td>Generally, IP routing allows packets to be routed directly to a particular address. However, in some instances you might need to route an IP packet to one address and then encapsulate it for forwarding to a different address. In a mobile environment in which the location of the end device changes, a different IP address might be used as the end device migrates between networks.</td>
</tr>
<tr>
<td></td>
<td>Within a J Series device, packets are routed to this internal interface where they are encapsulated with an IP packet and then forwarded to the encapsulating packet’s destination address. The IP-IP interface is an internal interface only and is not associated with a physical medium or PIM. You must configure the interface for it to perform IP tunneling.</td>
</tr>
<tr>
<td>ipip</td>
<td>Internally generated IP-over-IP interface. This interface is generated by JUNOS Software to handle IP-over-IP encapsulation. It is not a configurable interface.</td>
</tr>
<tr>
<td>Interface Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>lo0</td>
<td>Loopback address. The loopback address has several uses, depending on the particular JUNOS feature being configured. See “Loopback Interface” on page 76.</td>
</tr>
<tr>
<td>lo0.16384</td>
<td>Internal loopback address. The internal loopback address is a particular instance of the loopback address with the logical unit number 16384. It is created by JUNOS Software as the loopback interface for the internal routing instance. This interface prevents any filter on lo0.0 from disrupting internal traffic.</td>
</tr>
<tr>
<td>lsq-0/0/0</td>
<td>Configurable link services queuing interface. Link services include the multilink services MLPPP, MLFR, and Compressed Real-Time Transport Protocol (CRTP). Within a J Series device, packets are routed to this internal interface for link bundling or compression. The link services interface is an internal interface only and is not associated with a physical medium or PIM. You must configure the interface for it to perform multilink services. <strong>NOTE:</strong> The ls-0/0/0 interface has been deprecated. All multiclass multilink features supported by ls-0/0/0 are now supported by lsq-0/0/0. For more information about multilink services, see “Services Interfaces” on page 78.</td>
</tr>
<tr>
<td>lsi</td>
<td>Internally generated link services interface. This interface is generated by JUNOS Software to handle multilink services like MLPPP, MLFR, and CRTP. It is not a configurable interface.</td>
</tr>
<tr>
<td>lt-0/0/0</td>
<td>Interface used to provide class-of-service (CoS) support for real-time performance monitoring (RPM) probe packets. Within a J Series device, packets are routed to this internal interface for services. The lt interface is an internal interface only and is not associated with a physical medium or PIM. You must configure the interface for it to perform CoS for RPM services. <strong>NOTE:</strong> The lt interface on the M Series and T Series routing platforms supports configuration of logical devices—the capability to partition a single physical device into multiple logical devices that perform independent routing tasks. However, the lt interface on the J Series device does not support logical devices.</td>
</tr>
<tr>
<td>pc-pim/0/0</td>
<td>Internally configured interface used by the system as a control path between the WXC Integrated Services Module and the Routing Engine.</td>
</tr>
<tr>
<td>pd-0/0/0</td>
<td>Protocol Independent Multicast (PIM) de-encapsulation interface. In PIM sparse mode, the first-hop routing platform encapsulates packets destined for the rendezvous point device. The packets are encapsulated with a unicast header and are forwarded through a unicast tunnel to the rendezvous point. The rendezvous point then de-encapsulates the packets and transmits them through its multicast tree. Within a device, packets are routed to this internal interface for de-encapsulation. The PIM de-encapsulation interface is an internal interface only and is not associated with a physical interface. You must configure PIM with the [edit protocol pim] hierarchy to perform PIM de-encapsulation.</td>
</tr>
</tbody>
</table>
### Table 19: Special Interfaces (continued)

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>pe-0/0/0</code></td>
<td>Protocol Independent Multicast (PIM) encapsulation interface. In PIM sparse mode, the first-hop routing platform encapsulates packets destined for the rendezvous point device. The packets are encapsulated with a unicast header and are forwarded through a unicast tunnel to the rendezvous point. The rendezvous point then de-encapsulates the packets and transmits them through its multicast tree. Within a device, packets are routed to this internal interface for encapsulation. The PIM encapsulation interface is an internal interface only and is not associated with a physical interface. You must configure PIM with the <code>[edit protocol pim]</code> hierarchy to perform PIM encapsulation.</td>
</tr>
<tr>
<td><code>pimd</code></td>
<td>Internally generated Protocol Independent Multicast (PIM) de-encapsulation interface. This interface is generated by JUNOS Software to handle PIM de-encapsulation. It is not a configurable interface.</td>
</tr>
<tr>
<td><code>pime</code></td>
<td>Internally generated Protocol Independent Multicast (PIM) encapsulation interface. This interface is generated by JUNOS Software to handle PIM encapsulation. It is not a configurable interface.</td>
</tr>
<tr>
<td><code>pp0</code></td>
<td>Configurable PPPoE encapsulation interface. PPP packets being routed in an Ethernet network use PPPoE encapsulation. Within a J Series device, packets are routed to this internal interface for PPPoE encapsulation. The PPPoE encapsulation interface is an internal interface only and is not associated with a physical medium or PIM. You must configure the interface for it to forward PPPoE traffic. For more information about PPPoE interfaces, see “Configuring Point-to-Point Protocol over Ethernet” on page 289.</td>
</tr>
<tr>
<td><code>st0</code></td>
<td>Secure tunnel interface used for IPSec VPNs.</td>
</tr>
<tr>
<td><code>tap</code></td>
<td>Internally generated interface. This interface is generated by JUNOS Software to monitor and record traffic during passive monitoring. When packets are discarded by the Packet Forwarding Engine, they are placed on this interface. It is not a configurable interface.</td>
</tr>
<tr>
<td><code>umd0</code></td>
<td>Configurable USB modem physical interface. This interface is detected when an USB modem is connected to the USB port on the device. <strong>NOTE:</strong> The J4350 and J6350 devices have two USB ports. However, you can connect only one USB modem to the USB ports on these devices. If you connect USB modems to both the USB ports, only the first USB modem connected to the device is recognized.</td>
</tr>
</tbody>
</table>

### Discard Interface

The discard (`dsc`) interface is not a physical interface, but a virtual interface that discards packets. You can configure one discard interface. This interface allows you to identify the ingress (inbound) point of a denial-of-service (DoS) attack. When your network is under attack, the target host IP address is identified, and the local policy forwards attacking packets to the discard interface. Traffic routed out the discard interface is silently discarded.

### Loopback Interface

The Internet Protocol (IP) specifies a loopback network with the (IPv4) address `127.0.0.0/8`. Most IP implementations support a loopback interface (`lo0`) to represent...
the loopback facility. Any traffic that a computer program sends on the loopback network is addressed to the same computer. The most commonly used IP address on the loopback network is **127.0.0.1** for IPv4 and **::1** for IPv6. The standard domain name for the address is **localhost**.

The loopback interface can perform the following functions:

- **Device identification**—The loopback interface is used to identify the device. While any interface address can be used to determine if the device is online, the loopback address is the preferred method. Whereas interfaces might be removed or addresses changed based on network topology changes, the loopback address **never changes**.

  When you ping an individual interface address, the results do not always indicate the health of the device. For example, a subnet mismatch in the configuration of two endpoints on a point-to-point link makes the link appear to be inoperable. Pinging the interface to determine whether the device is online provides a misleading result. An interface might be unavailable because of a problem unrelated to the device's configuration or operation.

- **Routing information**—The loopback address is used by protocols such as OSPF to determine protocol-specific properties for the device or network. Further, some commands such as **ping mpls** require a loopback address to function correctly.

- **Packet filtering**—Stateless firewall filters can be applied to the loopback address to filter packets originating from, or destined for, the Routing Engine.

### Management Interface

Management interfaces are the primary interfaces for accessing the device remotely. Typically, a management interface is not connected to the in-band network, but is connected instead to the device’s internal network. Through a management interface you can access the device over the network using utilities such as **ssh** and **telnet** and configure it from anywhere, regardless of its physical location. Simple Network Management Protocol (SNMP) can use the management interface to gather statistics from the device.

Management interfaces vary based on device type:

- **The J Series devices** include four built-in Gigabit Ethernet interfaces located on the front panel of the router chassis named **ge-0/0/0**, **ge-0/0/1**, **ge-0/0/2**, and **ge-0/0/3** from left to right. These are not physically dedicated management interfaces, although the factory configuration for these routers automatically enables the J-Web user interface on these interfaces. You can use them to pass traffic or you can segregate one off and place it in the management zone to be used as a management interface. To use a built-in interface as a management Ethernet interface, configure it with a valid IP address.

- **The SRX5600 and SRX5800 devices** include a 10/100-Mbps Ethernet port on the Routing Engine (RE). This port, which is labeled ETHERNET, is a dedicated out-of-band management interface for the device. JUNOS Software automatically creates the device’s management interface **fxp0**. To use **fxp0** as a management port, you must configure its logical port **fxp0.0** with a valid IP address. While you
can use fxp0 to connect to a management network, you cannot place it into the management zone.

**NOTE:** On the SRX5600 and SRX5800 devices, you must first connect to the device through the serial console port before assigning a unique IP address to the management interface.

As a security feature, users cannot log in as root through a management interface. To access the device as root, you must use the console port.

**Services Interfaces**

On Juniper Networks M Series and T Series routing platforms, individual services such as IP-over-IP encapsulation, link services such as multilink protocols, adaptive services such as stateful firewall filters and NAT, and sampling and logging capabilities are implemented by services Physical Interface Cards (PICs). On a J Series device, these same features are implemented by the general-purpose CPU on the main circuit board.

Although the same JUNOS Software image supports the services features across all routing platforms, on a J Series device no Physical Interface Module (PIM) is associated with services features.

To configure services on a J Series device, you must configure one or more internal interfaces by specifying PIM slot 0 and port 0—for example, gr-0/0/0 for GRE.

J Series devices support multilink protocol services on the lsq-0/0/0 interface. At the logical level, the lsq-0/0/0 interface supports the Multilink Point-to-Point Protocol (MLPPP) and Multilink Frame Relay (MLFR) FRF.15 encapsulation types, and at the physical level, the interface supports the MLRF FRF.16 encapsulation type and Compressed Real-Time Transport Protocol (CRTP). lsq-0/0/0 supports multilink classes similar to the link services intelligent queuing interface (LSQ) PIC on M Series routing platforms. Configuring multilink classes is same as that off LSQ PIC.

**MLPPP and MLFR**

Multilink Point-to-Point Protocol (MLPPP) is a protocol for aggregating multiple constituent links into one larger PPP bundle. Multilink Frame Relay (MLFR) allows you to aggregate multiple Frame Relay links by inverse multiplexing. MLPPP and MLFR provide service options between low-speed T1 and E1 services. In addition to providing additional bandwidth, bundling multiple links can add a level of fault tolerance to your dedicated access service. Because you can implement bundling across multiple interfaces, you can protect users against loss of access when a single interface fails.

**MLFR Frame Relay Forum**

JUNOS supports FRF.12 fragmentation header formats for both FRF.15 (MLFR) and FRF.16 (MFR).
MLFR Frame Relay Forum 15 (FRF.15) combines multiple permanent virtual circuits (PVCs) into one aggregated virtual circuit (AVC). This process provides fragmentation over multiple PVCs on one end and reassembly of the AVC on the other end. MLFR FRF.15 is supported on the lsq:0/0/0 interface.

MLFR FRF.16 is supported on the lsq:0/0/0:channel, which carries a single MLFR FRF.16 bundle. MLFR FRF.16 combines multiple links to form one logical link. Packet fragmentation and reassembly occur on each virtual circuit. Each bundle can support multiple virtual circuits.

**NOTE:** If you configure a permanent virtual circuit (PVC) between T1, E1, T3, or E3 interfaces in J Series device and another vendor, and the other vendor does not have the same FRF.12 support or supports FRF.12 in a different way, the devices interface might discard a fragmented packet containing FRF.12 headers and count it as a "Policed Discard." Therefore, when you configure a PVC between T1, E1, T3, or E3 interfaces in the devices and another vendor, you should configure multilink bundles on both peers and configure fragmentation thresholds on the multilink bundle.

**CRTP**

Real-Time Transport Protocol (RTP) can help achieve interoperability among different implementations of network audio and video applications. However, the header can be too large a payload for networks using low-speed lines such as dial-up modems. Compressed Real-Time Transport Protocol (CRTP) can reduce network overhead on a low-speed link. On a J Series device, CRTP can operate on a T1 or E1 interface with PPP encapsulation.
Chapter 2
Configuring Ethernet, DS1, DS3, and Serial Interfaces

Juniper Networks devices can use network interfaces such as DS1, DS3, Fast Ethernet, Gigabit Ethernet, and serial interfaces to transmit and receive network traffic. For network interfaces to operate, you must configure properties such as logical interfaces, the encapsulation type, and certain settings specific to the interface type.

In most cases, you can use either J-Web Quick Configuration or a configuration editor to configure network interfaces.

**NOTE:** You cannot configure channelized T1 or E1 interfaces through a J-Web Quick Configuration page. You must use the J-Web or CLI configuration editor. Even after configuration, channelized interfaces do not appear on the Quick Configuration Interfaces page.

For more information about interfaces, see “Interfaces Overview” on page 3 and the Junos Network Interfaces Configuration Guide. To configure channelized interfaces, see “Configuring Channelized T1/E1/ISDN PRI Interfaces” on page 117. To configure DSL interfaces, see “Configuring Digital Subscriber Line Interfaces” on page 133. To configure PPPoE interfaces, see “Configuring Point-to-Point Protocol over Ethernet” on page 289. To configure ISDN interfaces, see “Configuring ISDN” on page 309.

For information about which devices support the features documented in this chapter, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.

This chapter contains the following topics:

- Before You Begin on page 81
- Configuring Interfaces—Quick Configuration on page 82
- Enabling and Disabling Promiscuous Mode on Ethernet Interfaces on page 108
- Configuring Network Interfaces with a Configuration Editor on page 109
- Verifying Interface Configuration on page 113

**Before You Begin**

Before you configure network interfaces, you need to perform the following tasks:
- Install your Juniper Networks device. For more information, see the Hardware Guide for your device.
- Establish basic connectivity. For more information, see the Getting Started Guide for your device.
- If you do not already have a basic understanding of physical and logical interfaces and Juniper Networks interface conventions, read “Interfaces Overview” on page 3.

Although it is not a requirement, you might also want to plan how you are going to use the various network interfaces before you start configuring them. You can see a list of the physical interfaces installed on the device by displaying the Quick Configuration page, as shown in Figure 16 on page 82.

**Configuring Interfaces—Quick Configuration**

You can use J-Web Quick Configuration to quickly configure most network interfaces, as shown in Figure 16 on page 82.

**Figure 16: Quick Configuration Interfaces Page**

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Link State</th>
<th>Configured</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0</td>
<td>Down</td>
<td>No</td>
<td>Gigabit Ethernet Interface 'ge-0/0/0'</td>
</tr>
<tr>
<td>te-0/0</td>
<td>Up</td>
<td>No</td>
<td>Link Services Interface 'ts-0/0/0'</td>
</tr>
<tr>
<td>ge-0/1</td>
<td>Up</td>
<td>No</td>
<td>Gigabit Ethernet Interface 'ge-0/0/1'</td>
</tr>
<tr>
<td>ge-0/2</td>
<td>Up</td>
<td>No</td>
<td>Gigabit Ethernet Interface 'ge-0/0/2'</td>
</tr>
<tr>
<td>ge-0/3</td>
<td>Down</td>
<td>No</td>
<td>Gigabit Ethernet Interface 'ge-0/0/3'</td>
</tr>
<tr>
<td>fxp0</td>
<td>Up</td>
<td>Yes</td>
<td>Management Interface 'fxp0'</td>
</tr>
<tr>
<td>fxp10</td>
<td>Up</td>
<td>Yes</td>
<td>Logical Unit 0 on Management Interface 'fxp0'</td>
</tr>
<tr>
<td>lo0</td>
<td>Up</td>
<td>Yes</td>
<td>Loopback Interface 'lo0'</td>
</tr>
<tr>
<td>lo1</td>
<td>Up</td>
<td>Yes</td>
<td>Logical Unit 0 on Loopback Interface 'lo0'</td>
</tr>
<tr>
<td>lo4.16384</td>
<td>Up</td>
<td>No</td>
<td>Logical Unit 16384 on Loopback Interface 'lo0'</td>
</tr>
<tr>
<td>ppp0</td>
<td>Up</td>
<td>No</td>
<td>Point to Point Protocol over Ethernet Interface 'ppp0'</td>
</tr>
</tbody>
</table>

To configure a network interface with Quick Configuration:

1. Select **Configure > Interfaces**. For information about interface names, see “Network Interface Naming” on page 9.

   A list of the network interfaces available on the routing platform appears, as shown in Figure 16 on page 82. The third column indicates whether the interface has been configured.
**NOTE:** Channelized T1 and E1 interfaces are not displayed in the list of interfaces on the J-Web Quick Configuration Interfaces page. However, you can configure and view channelized T1/E1/ISDN PRI interfaces with the J-Web configuration editor. For details, see “Configuring Channelized T1/E1/ISDN PRI Interfaces” on page 117.

2. Configure properties for a network interface by selecting the interface name and following the instructions in one of the following topics.

   - Configuring an E1 Interface with Quick Configuration on page 84
   - Configuring an E3 Interface with Quick Configuration on page 87
   - Configuring a Fast Ethernet Interface with Quick Configuration on page 90
   - Configuring Gigabit Ethernet Interfaces—Quick Configuration on page 94
   - Configuring T1 Interfaces with Quick Configuration on page 97
   - Configuring T3 Interfaces with Quick Configuration on page 101
   - Configuring Serial Interfaces with Quick Configuration on page 104
**Configuring an E1 Interface with Quick Configuration**

To configure properties on an E1 interface:

1. From the Quick Configuration page, as shown in Figure 16 on page 82, select the E1 interface you want to configure.

   The properties you can configure on an E1 interface are displayed, as shown in Figure 17 on page 84. (See “Network Interface Naming” on page 9.)

2. Enter information into the Quick Configuration page, as described in Table 20 on page 85.

3. Click one of the following buttons:
   - To apply the configuration and stay on the Quick Configuration page, click **Apply**.
   - To apply the configuration and return to the main configuration page, click **OK**.
To cancel your entries and return to the main page, click **Cancel**.

4. To verify that the E1 interface is configured correctly, see “Verifying Interface Configuration” on page 113.

### Table 20: E1 Quick Configuration Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logical Interfaces</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add logical interfaces</td>
<td>Defines one or more logical units that you connect to this physical E1 interface. You must define at least one logical unit for an E1 interface. You can define multiple units if the encapsulation type is Frame Relay.</td>
<td>Click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Logical Interface Description</td>
<td>(Optional) Describes the logical interface.</td>
<td></td>
</tr>
<tr>
<td>IPv4 Addresses and Prefixes</td>
<td>Specifies one or more IPv4 addresses for the interface.</td>
<td>1. Type one or more IPv4 addresses and prefixes. For example: 10.10.10.10/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Physical Interface Description</td>
<td>(Optional) Adds supplementary information about the physical E1 interface.</td>
<td></td>
</tr>
<tr>
<td>MTU (bytes)</td>
<td>Specifies the maximum transmission unit size for the E1 interface.</td>
<td>Type a value between 256 and 9192 bytes. The default MTU for E1 interfaces is 1504.</td>
</tr>
<tr>
<td>Clocking</td>
<td>Specifies the transmit clock source for the E1 line.</td>
<td>From the list, select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>internal</strong>—device’s own system clock (the default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>external</strong>—Clock received from the E1 interface</td>
</tr>
<tr>
<td>Per unit scheduler</td>
<td>Enables scheduling on logical interfaces.</td>
<td>■ To enable scheduling, select the check box.</td>
</tr>
<tr>
<td></td>
<td>Allows you to configure multiple output queues on a logical interface and associate an output scheduler and shaping rate with the queues.</td>
<td>■ To disable scheduling, clear the check box.</td>
</tr>
</tbody>
</table>

**Encapsulation**
Table 20: E1 Quick Configuration Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encapsulation</td>
<td>Specifies the encapsulation type for traffic on the interface.</td>
<td>From the list, select the encapsulation for this E1 interface:</td>
</tr>
<tr>
<td></td>
<td>■ PPP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Frame Relay</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Cisco HDLC</td>
<td></td>
</tr>
<tr>
<td>Enable CHAP</td>
<td>Enables or disables CHAP authentication on an E1 interface with PPP</td>
<td>■ To enable CHAP, select the check box.</td>
</tr>
<tr>
<td></td>
<td>encapsulation only.</td>
<td>■ To disable CHAP, clear the check box.</td>
</tr>
<tr>
<td>CHAP Local Identity (available if CHAP is enabled)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use System Host Name</td>
<td>Specifies that the E1 interface uses the device’s system hostname in CHAP challenge and response packets.</td>
<td>■ To enable, select the check box (the default).</td>
</tr>
<tr>
<td></td>
<td>■ To disable, clear the check box.</td>
<td></td>
</tr>
<tr>
<td>Local Name</td>
<td>If Use System Host Name is disabled, specifies the local name for CHAP to use.</td>
<td>Type a local name for this E1 interface.</td>
</tr>
<tr>
<td>CHAP Peer Identity</td>
<td>Identifies the client or peer with which the device communicates on this E1 interface.</td>
<td>Type the CHAP client name.</td>
</tr>
<tr>
<td>CHAP Secret</td>
<td>Specifies the secret password for CHAP authentication, known to both sides of the connection.</td>
<td>Type a password that is known to the other side of the connection. Use a combination of letters and numbers that is difficult for others to guess.</td>
</tr>
<tr>
<td>E1 Options</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Framing Mode</td>
<td>Specifies the framing mode for the E1 line.</td>
<td>From the list, select one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ g704—The default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ g704–no-crc4—G704 without cyclic redundancy check 4 (CRC4)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ unframed—Unframed transmission format</td>
<td></td>
</tr>
<tr>
<td>Invert Data</td>
<td>Enables or disables data inversion. Data inversion is normally used only in alternate mark inversion (AMI) mode.</td>
<td>■ To enable, select the check box.</td>
</tr>
<tr>
<td></td>
<td>■ To disable, clear the check box.</td>
<td></td>
</tr>
<tr>
<td>Timeslots</td>
<td>Specifies the number of time slots allocated to a fractional E1 interface. By default, an E1 interface uses all the time slots.</td>
<td>Type numeric values from 2 through 32. Separate discontinuous entries with commas, and use hyphens to indicate ranges. For example:</td>
</tr>
<tr>
<td></td>
<td>■ 2,4,7–9</td>
<td></td>
</tr>
<tr>
<td>Frame Checksum</td>
<td>Specifies the number of bits in the frame checksum.</td>
<td>Select 16 or 32. The default checksum is 16.</td>
</tr>
</tbody>
</table>
Configuring an E3 Interface with Quick Configuration

To configure properties on an E3 interface:

1. From the Quick Configuration page, as shown in Figure 16 on page 82, select the E3 interface you want to configure.

   The properties you can configure on an E3 interface are displayed, as shown in Figure 18 on page 87. (See “Network Interface Naming” on page 9.)

   **Figure 18: E3 Interfaces Quick Configuration Page**

   ![E3 Interfaces Quick Configuration Page]

<table>
<thead>
<tr>
<th>Quick Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="E3 Options Table" /></td>
</tr>
</tbody>
</table>

2. Enter information into the Quick Configuration page, as described in Table 21 on page 88.

3. Click one of the following buttons:
   - To apply the configuration and stay on the Quick Configuration page, click **Apply**.
   - To apply the configuration and return to the main configuration page, click **OK**.
   - To cancel your entries and return to the main page, click **Cancel**.

4. To verify that the E3 interface is configured correctly, see “Verifying Interface Configuration” on page 113.
### Table 21: E3 Quick Configuration Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logical Interfaces</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add logical interfaces</td>
<td>Defines one or more logical units that you connect to this physical E3</td>
<td>Click <strong>Add</strong></td>
</tr>
<tr>
<td></td>
<td>interface. You must define at least one logical unit for an E3 interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can define multiple units if the encapsulation type is Frame Relay.</td>
<td></td>
</tr>
<tr>
<td>Logical Interface Description</td>
<td>(Optional) Describes the logical interface.</td>
<td>Type a text description of the logical interface to more clearly identify it in monitoring displays.</td>
</tr>
<tr>
<td>IPv4 Addresses and Prefixes</td>
<td>Specifies one or more IPv4 addresses for the interface.</td>
<td>1. Type one or more IPv4 addresses and prefixes. For example: 10.10.10.10/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click <strong>Add</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click <strong>OK</strong></td>
</tr>
<tr>
<td>Physical Interface Description</td>
<td>(Optional) Adds supplementary information about the physical E3 interface.</td>
<td>Type a text description of the E3 interface to more clearly identify it in monitoring displays.</td>
</tr>
<tr>
<td>MTU (bytes)</td>
<td>Specifies the maximum transmission unit size for the E3 interface.</td>
<td>Type a value between 256 and 9192 bytes. The default MTU for E3 interfaces is 4474.</td>
</tr>
<tr>
<td>Clocking</td>
<td>Specifies the transmit clock source for the E3 line.</td>
<td>From the list, select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>internal</strong>—device’s own system clock (the default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>external</strong>—Clock received from the E3 interface</td>
</tr>
<tr>
<td><strong>Encapsulation</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Specifies the encapsulation type for traffic on the interface.</td>
<td>From the list, select the encapsulation for this E3 interface:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>PPP</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>Frame Relay</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>Cisco HDLC</strong></td>
</tr>
<tr>
<td>Enable CHAP</td>
<td>Enables or disables CHAP authentication on an E3 interface with PPP</td>
<td>■ To enable CHAP, select the check box.</td>
</tr>
<tr>
<td></td>
<td>encapsulation only.</td>
<td>■ To disable CHAP, clear the check box.</td>
</tr>
<tr>
<td>CHAP Local Identity (available if CHAP is enabled)</td>
<td>Specifies that the E3 interface uses the device’s system hostname in CHAP challenge and response packets.</td>
<td>■ To enable, select the check box (the default).</td>
</tr>
<tr>
<td>Use System Host Name</td>
<td></td>
<td>■ To disable, clear the check box.</td>
</tr>
<tr>
<td></td>
<td>Specifies that the E3 interface uses the device’s system hostname in CHAP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>challenge and response packets.</td>
<td></td>
</tr>
<tr>
<td>Local Name</td>
<td>If Use System Host Name is disabled, specifies the local name for CHAP</td>
<td>Type a local name for this E3 interface.</td>
</tr>
<tr>
<td></td>
<td>to use.</td>
<td></td>
</tr>
<tr>
<td>CHAP Peer Identity</td>
<td>Identifies the client or peer with which the device communicates on this</td>
<td>Type the CHAP client name.</td>
</tr>
<tr>
<td></td>
<td>E3 interface.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 21: E3 Quick Configuration Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAP Secret</td>
<td>Specifies the secret password for CHAP authentication, known to both sides of the connection.</td>
<td>Type a password that is known to the other side of the connection. Use a combination of letters and numbers that is difficult for others to guess.</td>
<td>CHAP Secret</td>
</tr>
<tr>
<td>E3 Options</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BERT is supported only when transmission is unframed. (See the Unframed option.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bert Error Rate</td>
<td>Specifies the exponent n in the bit error rate $10^{-n}$.</td>
<td>Type a value between 3 and 7, or 0. For example, a value of 6 specifies that 1 bit out of 1,000,000 is transmitted in error. The default is 0 (no bits are transmitted in error).</td>
<td></td>
</tr>
<tr>
<td>Bert Period</td>
<td>Specifies the length of time—in seconds—of the BERT.</td>
<td>Type a value between 1 and 240. The default is 10.</td>
<td></td>
</tr>
<tr>
<td>Compatibility</td>
<td>Defines the transmission mode and subrating to use on the E3 interface.</td>
<td>Select one of the following check boxes:</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>The mode must be set to the type of channel service unit (CSU) connected to the interface. The subrating specified must be the same subrating configured on the CSU.</td>
<td>Off—CSU compatibility is disabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CSU compatibility mode and subrating are supported only when transmission is unframed. (See the Unframed option.)</td>
<td>Digital-Link—Compatible with a Digital Link CSU.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kentrox—Compatible with a Kentrox CSU.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frame Checksum</td>
<td>Specifies the number of bits in the frame checksum. A 32-bit checksum provides more reliable packet verification, but is not supported by some older equipment.</td>
<td>From the Frame Checksum list, select 16 or 32. The default value is 16.</td>
<td></td>
</tr>
</tbody>
</table>
**Table 21: E3 Quick Configuration Summary (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle Cycle Flag</td>
<td>Specifies the value to transmit during idle cycles.</td>
<td>From the Idle Cycle Flag list, select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ flags—Transmits the value 0x7E during idle cycles. This is the default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ ones—Transmits the value 0xFF during idle cycles.</td>
</tr>
<tr>
<td>Loopback</td>
<td>Configures the E3 interface as a loopback interface for testing purposes.</td>
<td>From the Loopback list, select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ local—Traffic loops from the transmitter to the receiver at the E3 interface during tests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ remote—Traffic loops from the receiver to the transmitter at the E3 interface during tests.</td>
</tr>
<tr>
<td></td>
<td>When E3 is configured as a local loopback interface, the device transmits test traffic simultaneously to the CSU and to the receiver at the E3 interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When E3 is configured as a remote loopback interface, test traffic transmitted by the CSU is simultaneously received at the E3 interface and transmitted back to the CSU.</td>
<td></td>
</tr>
<tr>
<td>Payload Scrambler</td>
<td>Specifies whether the payload of the packet is to be scrambled, or randomized, when transmitted. Scrambling eliminates nonvariable bit patterns in the transmission, which can generate link-layer errors across an E3 link.</td>
<td>Select one of the following check boxes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Yes—Transmission is scrambled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ No—Transmission is not scrambled.</td>
</tr>
<tr>
<td>Start End Flag</td>
<td>Specifies whether the end and start flags are separated.</td>
<td>From the Start End Flag list, select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ filler—Flags are separated by idle cycles.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ shared—Flags overlap (no separation).</td>
</tr>
<tr>
<td>Unframed</td>
<td>Specifies whether the transmission is framed (G.751 framing) or unframed.</td>
<td>Select one of the following check boxes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Yes—Unframed transmission.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ No—Framed transmission.</td>
</tr>
</tbody>
</table>

**Configuring a Fast Ethernet Interface with Quick Configuration**

To configure properties on a Fast Ethernet interface:
1. From the Quick Configuration page, as shown in Figure 16 on page 82, select the Fast Ethernet interface you want to configure.

The properties you can configure on a Fast Ethernet interface are displayed, as shown in Figure 19 on page 91. (See “Network Interface Naming” on page 9.)

**Figure 19: Fast Ethernet Interfaces Quick Configuration Page**

2. Enter information into the Quick Configuration page, as described in Table 22 on page 91.

3. Click one of the following buttons:
   - To apply the configuration and stay on the Quick Configuration page, click **Apply**.
   - To apply the configuration and return to the main configuration page, click **OK**.
   - To cancel your entries and return to the main page, click **Cancel**.

4. To verify that the Fast Ethernet interface is configured correctly, see “Verifying Interface Configuration” on page 113.

**Table 22: Fast Ethernet Quick Configuration Summary**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Interfaces</td>
<td>Defines one or more logical units that you connect to this physical Fast Ethernet interface. You must define at least one logical unit for a Fast Ethernet interface. You can define multiple units if the encapsulation type is Frame Relay.</td>
<td>Click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Logical Interface Description</td>
<td>(Optional) Describes the logical interface.</td>
<td>Type a text description of the logical interface to more clearly identify it in monitoring displays.</td>
</tr>
</tbody>
</table>
Table 22: Fast Ethernet Quick Configuration Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Addresses and Prefixes</td>
<td>Specifies one or more IPv4 addresses for the interface.</td>
<td>1. Type one or more IPv4 addresses and prefixes. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.10.10.10/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>ARP Address</td>
<td>Enables the device to create a static Address Resolution Protocol (ARP) entry for this interface by specifying the IP address of a node to associate with its media access control (MAC) address. The IP address must be in the same subnet as the IPv4 address or prefix of the interface you are configuring. Static ARP entries associate the IP addresses and MAC addresses of nodes on the same subnet, enabling a device to respond to ARP requests having destination addresses that are not local to the incoming interface.</td>
<td>Type an IPv4 address that you want to associate with the MAC address—for example, <strong>10.10.10.1</strong>.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Specifies the hardware media access control (MAC) address associated with the ARP address. The MAC address uniquely identifies the system and is expressed in the following format: mm:mm:mm:ss:ss:ss. The first three octets denote the hardware manufacturer ID, and the last three are serial numbers identifying the device.</td>
<td>Type the MAC address to be mapped to the ARP entry—for example, <strong>00:12:1E:A9:8A:80</strong>.</td>
</tr>
<tr>
<td>Publish</td>
<td>Enables the device to reply to ARP requests for the specified address.</td>
<td>■ To enable publishing, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ To disable publishing, clear the check box.</td>
</tr>
<tr>
<td>Physical Interface Description</td>
<td>(Optional) Adds supplementary information about the physical Fast Ethernet interface.</td>
<td>Type a text description of the Fast Ethernet interface to more clearly identify it in monitoring displays.</td>
</tr>
</tbody>
</table>
Table 22: Fast Ethernet Quick Configuration Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU (bytes)</td>
<td>Specifies the maximum transmission unit size for the Fast Ethernet interface.</td>
<td>Type a value between 256 bytes and one of the following values:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ For built-in Fast Ethernet interfaces and Dual-Port Fast Ethernet PIM interfaces, 9192 bytes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ For 4-Port Fast Ethernet ePIM interfaces, 1514 bytes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default MTU for Fast Ethernet interfaces is 1514.</td>
<td></td>
</tr>
<tr>
<td>Per unit scheduler</td>
<td>Enables scheduling on logical interfaces.</td>
<td>■ To enable scheduling, select the check box.</td>
<td>■ To disable scheduling, clear the check box.</td>
</tr>
<tr>
<td></td>
<td>Allows you to configure multiple output queues on a logical interface and associate an output scheduler and shaping rate with the queues.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** You can also manually set the speed and link mode for a Fast Ethernet interface using the CLI commands `set interfaces fe-pim/0/port speed 10m | 100m` and `set interfaces fe-pim/0/port link-mode half-duplex | full-duplex`. 
Configuring Gigabit Ethernet Interfaces—Quick Configuration

You can use J-Web Quick Configuration to quickly configure a Gigabit Ethernet interface.

1. Select Configure > Interfaces. The properties you can configure on a Gigabit Ethernet interface appear as shown in Figure 20 on page 94.

Figure 20: Gigabit Ethernet Interface Quick Configuration

2. Fill in the information as described in Table 23 on page 95.

3. Click one of the following buttons:
   - To apply the configuration and stay on the Quick Configuration page, click Apply.
   - To apply the configuration and return to the main Configuration page, click OK.
To cancel your entries and return to the main page, click **Cancel**.

4. To verify that the Gigabit Ethernet interface is configured correctly, see “Verifying Interface Configuration” on page 113.

**Table 23: Gigabit Ethernet Quick Configuration Page Summary**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logical Interfaces</strong></td>
<td></td>
</tr>
<tr>
<td>Add logical interfaces</td>
<td>Defines one or more logical units that you connect to this physical</td>
</tr>
<tr>
<td></td>
<td>Gigabit Ethernet interface. You must define at least one logical unit</td>
</tr>
<tr>
<td></td>
<td>for a Gigabit Ethernet interface.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Add</strong></td>
</tr>
<tr>
<td>Logical Interface</td>
<td>(Optional) Describes the logical interface.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a text description of the logical interface to more clearly identify</td>
</tr>
<tr>
<td></td>
<td>it in monitoring displays.</td>
</tr>
<tr>
<td><strong>IPv4 Addresses and</strong></td>
<td>Specifies one or more IPv4 addresses for the interface.</td>
</tr>
<tr>
<td><strong>Prefixes</strong></td>
<td>Type one or more IPv4 addresses and prefixes.</td>
</tr>
<tr>
<td></td>
<td>For example: 10.10.10.10/24</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add</strong></td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>OK</strong></td>
</tr>
<tr>
<td></td>
<td>To delete an IP address and prefix, select them in the Source Addresses</td>
</tr>
<tr>
<td></td>
<td>and Prefixes box, then click <strong>Delete</strong>.</td>
</tr>
<tr>
<td><strong>ARP Address</strong></td>
<td>Enables the device to create a static Address Resolution Protocol (ARP)</td>
</tr>
<tr>
<td></td>
<td>entry for this interface by specifying the IP address of a node to</td>
</tr>
<tr>
<td></td>
<td>associate with its media access control (MAC) address. The IP address</td>
</tr>
<tr>
<td></td>
<td>must be in the same subnet as the IPv4 address or prefix of the</td>
</tr>
<tr>
<td></td>
<td>interface you are configuring.</td>
</tr>
<tr>
<td></td>
<td>Static ARP entries associate the IP addresses and MAC addresses of</td>
</tr>
<tr>
<td></td>
<td>nodes on the same subnet, enabling a device to respond to ARP requests</td>
</tr>
<tr>
<td></td>
<td>having destination addresses that are not local to the incoming</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
</tr>
<tr>
<td></td>
<td>Type an IPv4 address that you want to associate with the MAC address—</td>
</tr>
<tr>
<td></td>
<td>for example, 10.10.10.1</td>
</tr>
<tr>
<td><strong>MAC Address</strong></td>
<td>Specifies the hardware media access control (MAC) address associated</td>
</tr>
<tr>
<td></td>
<td>with the ARP address.</td>
</tr>
<tr>
<td></td>
<td>The MAC address uniquely identifies the system and is expressed in the</td>
</tr>
<tr>
<td></td>
<td>following format: mmm:mmm:mmm:ss:ss:ssss. The first three octets denote</td>
</tr>
<tr>
<td></td>
<td>the hardware manufacturer ID, and the last three are serial numbers</td>
</tr>
<tr>
<td></td>
<td>identifying the device.</td>
</tr>
<tr>
<td></td>
<td>Type the MAC address to be mapped to the ARP entry—for example, 00:12:1E</td>
</tr>
<tr>
<td></td>
<td>A9:8A:80</td>
</tr>
<tr>
<td><strong>Publish</strong></td>
<td>Enables the device to reply to ARP requests for the specified address.</td>
</tr>
<tr>
<td></td>
<td>For more information, see “Configuring Static ARP Entries on Ethernet</td>
</tr>
<tr>
<td></td>
<td>Interfaces” on page 111</td>
</tr>
<tr>
<td></td>
<td>■ To enable publishing, select the check box.</td>
</tr>
<tr>
<td></td>
<td>■ To disable publishing, clear the check box.</td>
</tr>
</tbody>
</table>
Table 23: Gigabit Ethernet Quick Configuration Page Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface Description</td>
<td>(Optional) Adds supplementary information about the physical Gigabit Ethernet interface.</td>
<td>Type a text description of the Gigabit Ethernet interface to more clearly identify it in monitoring displays.</td>
</tr>
<tr>
<td>MTU (bytes)</td>
<td>Specifies the maximum transmission unit size for the Gigabit Ethernet interface.</td>
<td>Type a value between 256 and 9014 bytes. The default MTU for Gigabit Ethernet interfaces is 1514. The default MTU for Fast Ethernet interfaces is 1518.</td>
</tr>
<tr>
<td>Per unit scheduler</td>
<td>Enables scheduling on logical interfaces.</td>
<td>■ To enable scheduling, select the check box.</td>
</tr>
<tr>
<td></td>
<td>Allows you to configure multiple output queues on a logical interface and associate an output scheduler and shaping rate with the queues.</td>
<td>■ To disable scheduling, clear the check box.</td>
</tr>
</tbody>
</table>

### Gigabit Ethernet Options/ Fast Ethernet Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback</td>
<td>Enables or disables the loopback option.</td>
<td>Select Yes to enable the loopback diagnostic option, or select No to disable the loopback option. By default, loopback is disabled.</td>
</tr>
<tr>
<td>Auto Negotiation</td>
<td>Enables or disables autonegotiation.</td>
<td>Select Yes to enable autonegotiation, or select No to disable it. By default, autonegotiation is enabled.</td>
</tr>
<tr>
<td></td>
<td>By default, Gigabit Ethernet interfaces autonegotiate the link mode and speed settings. If you disable autonegotiation and do not manually configure link mode and speed, the link is negotiated at 1000 Mbps, full duplex.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When you configure both the link mode and the speed, the link negotiates with the manually configured settings whether autonegotiation is enabled or disabled.</td>
<td></td>
</tr>
<tr>
<td>Auto Negotiation Remote Fault</td>
<td>Indicates the autonegotiation remote fault value.</td>
<td>Select the autonegotiation remote fault value from the list of options given. This field is enabled only if autonegotiation is enabled.</td>
</tr>
<tr>
<td>Source MAC Address Filters</td>
<td>Displays the list of media access control (MAC) addresses from which you want to receive packets on this interface.</td>
<td>To add MAC addresses, type them in the boxes above the Add button, then click Add.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To delete a MAC address, select it in the Source Addresses box, then click Delete.</td>
</tr>
</tbody>
</table>
NOTE: You can also manually set the speed and link mode for built-in and copper PIM Gigabit Ethernet interfaces on J4350 and J6350 devices using the CLI commands set interfaces ge-pim/0/port speed 10m | 100m | 1000m and set interfaces ge-pim/0/port link-mode half-duplex | full-duplex. (You cannot manually configure speed and link mode on SFP Gigabit Ethernet PIMs.) You must configure both link mode and speed—if you configure only one or the other, the system ignores the configuration and generates a system log message.

Configuring T1 Interfaces with Quick Configuration

To configure properties on a T1 interface:
1. From the Quick Configuration page, as shown in Figure 16 on page 82, select the T1 interface you want to configure.

    The properties you can configure on a T1 interface are displayed, as shown in Figure 21 on page 98. (See “Network Interface Naming” on page 9.)

    Figure 21: T1 Interfaces Quick Configuration Page

2. Enter information into the Quick Configuration page, as described in Table 24 on page 99.

3. Click one of the following buttons:
   - To apply the configuration and stay on the Quick Configuration page, click Apply.
   - To apply the configuration and return to the main configuration page, click OK.
To cancel your entries and return to the main page, click **Cancel**.

4. To verify that the T1 interface is configured correctly, see “Verifying Interface Configuration” on page 113.

**Table 24: T1 Quick Configuration Summary**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logical Interfaces</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add logical interfaces</td>
<td>Defines one or more logical units that you connect to this physical T1 interface. You must define at least one logical unit for a T1 interface. You can define multiple units if the encapsulation type is Frame Relay.</td>
<td>Click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Logical Interface Description</td>
<td>(Optional) Describes the logical interface.</td>
<td>Type a text description of the logical interface to more clearly identify it in monitoring displays.</td>
</tr>
</tbody>
</table>
| IPv4 Addresses and Prefixes   | Specifies one or more IPv4 addresses for the interface.                  | 1. Type one or more IPv4 addresses and prefixes. For example: 10.10.10.10/24  
                                         2. Click **Add**.                                                            |
| Physical Interface Description| (Optional) Adds supplementary information about the physical T1 interface.| Type a text description of the T1 interface to more clearly identify it in monitoring displays. |
| MTU (bytes)                   | Specifies the maximum transmission unit size for the T1 interface.       | Type a value between 256 and 9192 bytes. The default MTU for T1 interfaces is 1504. |
| Clocking                      | Specifies the transmit clock source for the T1 line.                     | From the list, select one of the following:  
                                         ■ **internal**—device’s own system clock (the default)  
                                         ■ **external**—Clock received from the T1 interface |
| Per unit scheduler            | Enables scheduling on logical interfaces.                                | ■ To enable scheduling, select the check box.  
                                         ■ To disable scheduling, clear the check box. |
|                               | Allows you to configure multiple output queues on a logical interface and associate an output scheduler and shaping rate with the queues. |                                                                            |
| **Encapsulation**             |                                                                          |                                                                            |
| Encapsulation                 | Specifies the encapsulation type for traffic on the interface.           | From the list, select the encapsulation for this T1 interface:  
                                         ■ **PPP**  
                                         ■ Frame Relay  
                                         ■ Cisco HDLC |
| Enable CHAP                   | Enables or disables CHAP authentication on a T1 interface with PPP encapsulation only. | ■ To enable CHAP, select the check box.  
                                         ■ To disable CHAP, clear the check box. |
### CHAP Local Identity (available if CHAP is enabled)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use System Host Name</td>
<td>Specifies that the T1 interface uses the device’s system hostname in CHAP challenge and response packets.</td>
<td>To enable, select the check box (the default). To disable, clear the check box.</td>
</tr>
<tr>
<td>Local Name</td>
<td>If Use System Host Name is disabled, specifies the local name for CHAP to use.</td>
<td>Type a local name for this T1 interface.</td>
</tr>
<tr>
<td>CHAP Peer Identity</td>
<td>Identifies the client or peer with which the device communicates on this T1 interface.</td>
<td>Type the CHAP client name.</td>
</tr>
<tr>
<td>CHAP Secret</td>
<td>Specifies the secret password for CHAP authentication, known to both sides of the connection.</td>
<td>Type a password that is known to the other side of the connection. Use a combination of letters and numbers that is difficult for others to guess.</td>
</tr>
</tbody>
</table>

### T1 Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Framing Mode</td>
<td>Specifies the framing mode for the T1 line.</td>
<td>From the list, select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ esf—Extended superframe (the default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ sf—Superframe</td>
</tr>
<tr>
<td>Line Encoding</td>
<td>Specifies the line encoding method.</td>
<td>From the list, select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ ami—Alternate mark inversion</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ b8zs—Binary 8 zero substitution (the default)</td>
</tr>
<tr>
<td>Byte Encoding</td>
<td>Specifies the byte encoding method.</td>
<td>From the list, select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ nx56—7 bits per byte</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ nx64—8 bits per byte (the default)</td>
</tr>
<tr>
<td>Invert Data</td>
<td>Enables or disables data inversion. Data inversion is normally used only in alternate mark inversion (AMI) mode.</td>
<td>To enable, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To disable, clear the check box.</td>
</tr>
<tr>
<td>Timeslots</td>
<td>Specifies the number of time slots allocated to a fractional T1 interface. By default, a T1 interface uses all the time slots.</td>
<td>Type numeric values from 1 through 24. You can use any combination of time slots. To configure ranges, use hyphens. To configure discontinuous slots, use commas. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1–5,10,24</td>
</tr>
<tr>
<td>Frame Checksum</td>
<td>Specifies the number of bits in the frame checksum. A 32-bit checksum provides more reliable packet verification, but is not supported by some older equipment.</td>
<td>Select 16 or 32. The default value is 16.</td>
</tr>
</tbody>
</table>
Table 24: T1 Quick Configuration Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line Buildout</td>
<td>Specifies the T1 line buildout in feet for cables 655 feet (200 m) or shorter, or in decibels for longer cables.</td>
<td>From the list, select one of the following line buildouts:</td>
</tr>
<tr>
<td></td>
<td>Line buildout compensates for the loss in decibels based on the distance from the device to the first repeater in the circuit.</td>
<td>■ 0–132 (0 m–40 m) (the default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 133–265 (40 m–81 m)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 266–398 (81 m–121 m)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 399–551 (121 m–162 m)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 532–655 (162 m–200 m)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ long-0db</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ long-7.5db</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ long-15db</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ long-22.5db</td>
</tr>
</tbody>
</table>

Configuring T3 Interfaces with Quick Configuration

To configure properties on a T3 (DS3) interface:
1. From the Quick Configuration page, as shown in Figure 16 on page 82, select the T3 interface you want to configure.

   The properties you can configure on a T3 interface are displayed, as shown in Figure 22 on page 102. (See “Network Interface Naming” on page 9.)

   **Figure 22: T3 Interfaces Quick Configuration Page**

   ![T3 Interfaces Quick Configuration Page](image)

   2. Enter information into the Quick Configuration page, as described in Table 25 on page 103.

   3. Click one of the following buttons:
      - To apply the configuration and stay on the Quick Configuration page, click **Apply**.
      - To apply the configuration and return to the main configuration page, click **OK**.
      - To cancel your entries and return to the main page, click **Cancel**.

   4. To verify that the T3 interface is configured correctly, see “Verifying Interface Configuration” on page 113.
### Table 25: T3 Quick Configuration Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logical Interfaces</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add logical interfaces</td>
<td>Defines one or more logical units that you connect</td>
<td>Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>to this physical T3 interface. You must define at least one logical unit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>for a T3 interface. You can define multiple units if the encapsulation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>type is Frame Relay.</td>
<td></td>
</tr>
<tr>
<td>Logical Interface Description</td>
<td>(Optional) Describes the logical interface.</td>
<td>Type a text description of the logical interface to more clearly identify it</td>
</tr>
<tr>
<td></td>
<td></td>
<td>in monitoring displays.</td>
</tr>
<tr>
<td>IPv4 Addresses and Prefixes</td>
<td>Specifies one or more IPv4 addresses for the interface.</td>
<td>1. Type one or more IPv4 addresses and prefixes. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.10.10.10/24.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Physical Interface Description</td>
<td>(Optional) Adds supplementary information about the physical T3</td>
<td>Type a text description of the T3 interface to more clearly identify it in</td>
</tr>
<tr>
<td></td>
<td>interface.</td>
<td>monitoring displays.</td>
</tr>
<tr>
<td>MTU (bytes)</td>
<td>Specifies the maximum transmission unit size for the T3 interface.</td>
<td>Type a value between 256 and 9192 bytes. The default MTU for T3 interfaces</td>
</tr>
<tr>
<td></td>
<td></td>
<td>is 4474.</td>
</tr>
<tr>
<td>Clocking</td>
<td>Specifies the transmit clock source for the T3 line.</td>
<td>From the list, select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>internal</strong>—device’s own system clock (the default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>external</strong>—Clock received from the T3 interface</td>
</tr>
<tr>
<td>Per unit scheduler</td>
<td>Enables scheduling on logical interfaces.</td>
<td>To enable scheduling, select the check box.</td>
</tr>
<tr>
<td></td>
<td>Allows you to configure multiple output queues on a logical interface</td>
<td>To disable scheduling, clear the check box.</td>
</tr>
<tr>
<td></td>
<td>and associate an output scheduler and shaping rate with the queues.</td>
<td></td>
</tr>
<tr>
<td><strong>Encapsulation</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Specifies the encapsulation type for traffic on the interface.</td>
<td>From the list, select the encapsulation for this T3 interface:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>PPP</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>Frame Relay</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>Cisco HDLC</strong></td>
</tr>
<tr>
<td>Enable CHAP</td>
<td>Enables or disables CHAP authentication on a T3 interface with PPP</td>
<td>To enable CHAP, select the check box.</td>
</tr>
<tr>
<td></td>
<td>encapsulation only.</td>
<td>To disable CHAP, clear the check box.</td>
</tr>
<tr>
<td><strong>CHAP Local Identity (available if CHAP is enabled)</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 25: T3 Quick Configuration Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use System Host Name</td>
<td>Specifies that the T3 interface uses the device’s system hostname in CHAP challenge and response packets.</td>
<td>■ To enable, select the check box (the default).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ To disable, clear the check box.</td>
</tr>
<tr>
<td>Local Name</td>
<td>If Use System Host Name is disabled, specifies the local name for CHAP to use.</td>
<td>Type a local name for this T3 interface.</td>
</tr>
<tr>
<td>CHAP Peer Identity</td>
<td>Identifies the client or peer with which the device communicates on this T3 interface.</td>
<td>Type the CHAP client name.</td>
</tr>
<tr>
<td>CHAP Secret</td>
<td>Specifies the secret password for CHAP authentication, known to both sides of the connection.</td>
<td>Type a password that is known to the other side of the connection. Use a combination of letters and numbers that is difficult for others to guess.</td>
</tr>
</tbody>
</table>

**T3 Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Select 16 or 32. The default value is 16.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Checksum</td>
<td>Specifies the number of bits in the frame checksum. A 32-bit checksum provides more reliable packet verification, but is not supported by some older equipment.</td>
<td>Select 16 or 32. The default value is 16.</td>
</tr>
<tr>
<td>Enable Long Buildout</td>
<td>Specifies a short or long cable length for copper-cable-based T3 interfaces. A long cable is longer than 225 feet (68.6m).</td>
<td>■ To enable long buildout, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ To disable long buildout, clear the check box.</td>
</tr>
<tr>
<td>Disable C-Bit Parity Mode</td>
<td>Enables or disables C-bit parity mode, which controls the type of framing that is present on the transmitted T3 signal.</td>
<td>■ To disable, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ To enable, clear the check box.</td>
</tr>
</tbody>
</table>

**Configuring Serial Interfaces with Quick Configuration**

A serial interface uses a serial line protocol—such as EIA-530, X.21, RS-449/422, RS-232, or V.35—to control the transmission of signals across the interface. You do not need to explicitly configure the serial line protocol, because it is automatically detected by the Juniper Networks device based on the cable plugged into the serial interface.

To configure properties on a serial interface:
1. From the Quick Configuration page, as shown in Figure 16 on page 82, select the serial interface you want to configure.

   The properties you can configure on a serial interface are displayed, as shown in Figure 23 on page 105. (See “Network Interface Naming” on page 9.)

   **Figure 23: Serial Interfaces Quick Configuration Page**

   ![Serial Interfaces Quick Configuration Page](image)

2. Enter information into the Quick Configuration page, as described in Table 26 on page 106.

3. Click one of the following buttons:
   - To apply the configuration and stay on the Quick Configuration page, click **Apply**.
   - To apply the configuration and return to the main configuration page, click **OK**.
   - To cancel your entries and return to the main page, click **Cancel**.

4. To verify that the serial interface is configured correctly, see “Verifying Interface Configuration” on page 113.
# Table 26: Serial Quick Configuration Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logical Interfaces</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add logical interfaces</td>
<td>Defines one or more logical units that you connect to this physical serial interface. You must define at least one logical unit for a serial interface. You can define multiple units if the encapsulation type is Frame Relay.</td>
<td>Click Add</td>
</tr>
<tr>
<td>Logical Interface Description</td>
<td>(Optional) Describes the logical interface.</td>
<td></td>
</tr>
</tbody>
</table>
| IPv4 Addresses and Prefixes   | Specifies one or more IPv4 addresses for the interface.                  | 1. Type one or more IPv4 addresses and prefixes. For example: 10.10.10.10/24  
  2. Click Add  
  3. Click OK |
| Physical Interface Description| (Optional) Adds supplementary information about the physical serial interface. |             |
| MTU (bytes)                   | Specifies the maximum transmission unit size for a serial interface.     | Type a value between 256 and 9192 bytes. The default MTU for serial interfaces is 1504. |
| Per unit scheduler            | Enables scheduling on logical interfaces.                                |             |
| Encapsulation                 | Specifies the encapsulation type for traffic on the interface.          |             |
| Encapsulation                 | From the list, select the encapsulation for this serial interface:       |             |
| Enable CHAP                   | Enables or disables CHAP authentication on a serial interface with PPP encapsulation only. |             |
| CHAP Local Identity (available if CHAP is enabled) | Specifies that the serial interface use the device’s system hostname in CHAP challenge and response packets. |             |
| Use System Host Name          | To enable, select the check box (the default).                           |             |
| Local Name                    | To disable, clear the check box.                                        |             |
|                              | Type a local name for this serial interface.                            |             |
Table 26: Serial Quick Configuration Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAP Peer Identity</td>
<td>Identifies the client or peer with which the device communicates on this serial interface.</td>
<td>Type the CHAP client name.</td>
</tr>
<tr>
<td>CHAP Secret</td>
<td>Specifies the secret password for CHAP authentication, known to both sides of the connection.</td>
<td>Type a password that is known to the other side of the connection. Use a combination of letters and numbers that is difficult for others to guess.</td>
</tr>
</tbody>
</table>

**Serial Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clocking Mode</td>
<td>Specifies the clock source to determine the timing on serial interfaces.</td>
<td>From the list, select one of the following timing sources.</td>
</tr>
<tr>
<td></td>
<td>If you use an externally timed clocking mode—dce or loop—long cables might introduce a phase shift of DTE-transmitted clock and data. At high speeds, this phase shift might cause errors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inverting the transmit clock corrects the phase shift, thereby reducing error rates. By default, the transmit clock is not inverted. To invert the transmit clock, do either of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ In the J-Web configuration editor, set the Transmit clock value to invert on the Interfaces &gt; interface-name &gt; Serial options page.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ In the CLI configuration editor, include the transmit-clock invert statement at the [edit interfaces s-pim/0/port serial-options] hierarchy level.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For X.21 serial interfaces, you must use the loop clocking mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When the device is functioning as DTE, you must use the dce clocking mode for all interfaces except X.21 serial interfaces</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When the device is functioning as DCE, we recommend using the internal clocking mode for all interfaces.</td>
<td></td>
</tr>
</tbody>
</table>
Table 26: Serial Quick Configuration Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clock Rate</td>
<td>Specifies the line speed in kilohertz or megahertz for serial interfaces that use the DTE clocking mode.</td>
<td>From the list, select one of the following clock rates:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 1.2 KHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 2.4 KHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 9.6 KHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 19.2 KHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 38.4 KHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 56.0 KHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 64.0 KHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 72.0 KHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 125.0 KHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 148.0 KHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 250.0 KHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 500.0 KHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 800.0 KHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 1.0 MHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 1.5 MHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 2.0 MHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 4.0 MHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 8.0 MHz</td>
</tr>
</tbody>
</table>

**Enabling and Disabling Promiscuous Mode on Ethernet Interfaces**

This section contains the following topics:

- Understanding Promiscuous Mode on page 108
- Enabling and Disabling Promiscuous Mode on page 109

**Understanding Promiscuous Mode**

When promiscuous mode is enabled on a Layer 3 Ethernet interface, all packets received on the interface are sent to the central point or Services Processing Unit regardless of the destination MAC address of the packet. You can also enable promiscuous mode on chassis cluster redundant Ethernet interfaces and aggregated Ethernet interfaces. If you enable promiscuous mode on a redundant Ethernet interface, promiscuous mode is then enabled on any child physical interfaces. If you enable promiscuous mode on an aggregated Ethernet interface, promiscuous mode is then enabled on all member interfaces.
Enabling and Disabling Promiscuous Mode

You can use either J-Web or the CLI configuration editor to enable or disable promiscuous mode on an interface.

- J-Web Point and Click CLI Configuration on page 109
- CLI Configuration on page 109

J-Web Point and Click CLI Configuration

To enable promiscuous mode on an interface:
1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Interfaces, click Configure or Edit.
3. Under Interface, click the Interface name ge-0/0/0.
4. Select the Promiscuous Mode check box.
5. Click OK.

To disable promiscuous mode on an interface:
1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Interfaces, click Configure or Edit.
3. Under Interface, click the Interface name ge-0/0/0.
4. Clear the Promiscuous Mode check box.
5. Click OK.

CLI Configuration

To enable promiscuous mode on an interface:

user@host# set interfaces ge-0/0/0 promiscuous-mode

To disable promiscuous mode on an interface:

user@host# delete interfaces ge-0/0/0 promiscuous-mode

Configuring Network Interfaces with a Configuration Editor

To enable the interfaces installed on your device to work properly, you must configure their properties. You can perform basic interface configuration using the J-Web Quick Configuration pages, as described in “Configuring Interfaces—Quick Configuration” on page 82. You can perform the same configuration tasks using the J-Web or CLI configuration editor. In addition, you can configure a wider variety of options that are encountered less frequently.
You can perform the following tasks to configure interfaces:
- Adding a Network Interface with a Configuration Editor on page 110
- Configuring Static ARP Entries on Ethernet Interfaces on page 111
- Deleting a Network Interface with a Configuration Editor on page 112

For information about using the J-Web and CLI configuration editors, see the J-Web Interface User Guide and the Junos CLI User Guide.

### Adding a Network Interface with a Configuration Editor

After you install a PIM, connect the interface cables to the ports, and power on the device, you must complete initial configuration of each network interface, as described in the following procedure:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 27 on page 110.
3. When you are finished configuring the device, commit the configuration.
4. To verify that the network interface is configured correctly, see “Verifying Interface Configuration” on page 113.

#### Table 27: Adding an Interface

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Interfaces level in the</td>
<td>In the J-Web interface, select Configure &gt; Configure &gt; CLI Tools &gt; Point and Click CLI</td>
<td>From the [edit] hierarchy level, enter edit interfaces interface-name</td>
</tr>
<tr>
<td>configuration hierarchy</td>
<td>2. Next to Interfaces, click Configure or Edit.</td>
<td>For information about interface names, see “Network Interface Naming” on page 9.</td>
</tr>
<tr>
<td>Create the new interface.</td>
<td>Next to Interface, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Enter the name of the new interface in the Interface name box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Make sure the name conforms to the interface naming rules. For more information, see “Network Interface Naming” on page 9.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Click OK.</td>
<td></td>
</tr>
<tr>
<td>Create the basic configuration for the</td>
<td>Under Interface Name in the table, click the name of the new interface.</td>
<td>Enter values for physical interface properties as needed. Examples include changes to the default values for physical encapsulation or MTU. For example:</td>
</tr>
<tr>
<td>new interface.</td>
<td>2. Enter values in the other fields on this page if warranted.</td>
<td>set interface-name encapsulation ppp</td>
</tr>
<tr>
<td></td>
<td>All these entries are optional, but you need to set values for Clocking and Encapsulation in particular if the default values are not suitable.</td>
<td></td>
</tr>
</tbody>
</table>
Table 27: Adding an Interface (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add values for interface-specific options.</td>
<td>1. Under Nested configuration, click <strong>Configure</strong> for the appropriate interface type.</td>
<td>1. From the [edit interfaces interface-name] hierarchy level, type <strong>edit interface-options</strong>.</td>
</tr>
<tr>
<td>Most interface types have optional parameters that are specific to the interface type.</td>
<td>2. In the interface-specific page that appears, enter the values you need to supply or change the default values.</td>
<td>2. Enter the statement for each interface-specific property for which you need to change the default value.</td>
</tr>
<tr>
<td>Add logical interfaces.</td>
<td>3. When you are finished, click <strong>OK</strong> to confirm your changes or <strong>Cancel</strong> to cancel them and return to the previous page.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. In the main Interface page for this interface, next to <strong>Unit</strong>, click <strong>Add new entry</strong>.</td>
<td>1. From the [edit interfaces interface-name] hierarchy level, type <strong>set unit logical-unit-number</strong>. Replace <strong>logical-unit-number</strong> with a value from 0 through 16384.</td>
</tr>
<tr>
<td></td>
<td>2. On the Unit page for logical interfaces that appears, type a number from 0 through 16384 in the Interface unit number box.</td>
<td>2. Enter additional values for properties you need to configure on the logical interface, such as logical encapsulation or protocol family.</td>
</tr>
<tr>
<td></td>
<td>3. Enter values in other fields as required for your network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. To configure protocol family values if needed, under <strong>Family</strong>, click <strong>Configure</strong> next to the appropriate protocol.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. To access additional subordinate hierarchies under Nested configuration, click <strong>Configure</strong> next to any parameter you want to configure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. When you are finished, click <strong>OK</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Static ARP Entries on Ethernet Interfaces

By default, the device responds to an Address Resolution Protocol (ARP) request only if the destination address of the ARP request is on the local network of the incoming interface. For Fast Ethernet or Gigabit Ethernet interfaces, you can configure static ARP entries that associate the IP addresses of nodes on the same Ethernet subnet with their media access control (MAC) addresses. These static ARP entries enable the device to respond to ARP requests even if the destination address of the ARP request is not local to the incoming Ethernet interface.

In this example, you configure a static ARP entry on Gigabit Ethernet interface ge-0/0/3 of the device consisting of the IP address and corresponding MAC address of a node on the same Ethernet subnet. The ge-0/0/3 interface has the IP address 10.1.1.1/24. The node has the IP address 10.1.1.3 and the MAC address 00:ff:85:7f:78:03. If the node on your network is another device running JUNOS Software, you can enter the `show interfaces interface-name` command to learn the IP and MAC (hardware) address of the node.

For more information about configuring static ARP entries, see the *Junos Network Interfaces Configuration Guide*.

To configure a static ARP entry on the ge-0/0/3 interface:
1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 28 on page 112.
3. If you are finished configuring the device, commit the configuration.
4. To verify the configuration, see “Verifying Interface Configuration” on page 113.

### Table 28: Configuring Static ARP Entries

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Interfaces level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit interfaces ge-0/0/3</td>
</tr>
<tr>
<td></td>
<td>2. Next to Interfaces, click Edit.</td>
<td></td>
</tr>
<tr>
<td>Select the Gigabit Ethernet interface ge-0/0/3.</td>
<td>In the Interface name column, click ge-0/0/3.</td>
<td></td>
</tr>
<tr>
<td>Configure a static ARP entry on logical unit 0 with the source address 10.1.1.1/24 on the ge-0/0/3 interface.</td>
<td>1. Under Unit, next to 0, click Edit.</td>
<td>1. Enter edit unit 0</td>
</tr>
<tr>
<td></td>
<td>2. Under Family, next to Inet, click Edit.</td>
<td>2. Enter edit family inet address 10.1.1.1/24</td>
</tr>
<tr>
<td></td>
<td>3. Under Address, next to 10.1.1.1/24, click Edit.</td>
<td>3. Enter set arp 10.1.1.3 mac 00:ff:85:7f:78:03 publish</td>
</tr>
<tr>
<td></td>
<td>4. Next to Arp, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td>Set the IP address of the subnet node to 10.1.1.3 and the corresponding MAC address to 00:ff:85:7f:78:03.</td>
<td>5. In the Address box, type the IP address of the node—10.1.1.3.</td>
<td></td>
</tr>
<tr>
<td>To have the device reply to ARP requests from the node, use the publish option.</td>
<td>6. Select the Publish check box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. From the Mac address type list, select Mac.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. In the Mac box, type the MAC address 00:ff:85:7f:78:03 of node.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9. Click OK until you return to the Interfaces page.</td>
<td></td>
</tr>
</tbody>
</table>

### Deleting a Network Interface with a Configuration Editor

To delete an interface:
1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 29 on page 113.
**NOTE:** Performing this action removes the interface from the software configuration and disables it. Network interfaces remain physically present, and their identifiers continue to appear on the J-Web Monitor and Quick Configuration pages.

### Table 29: Deleting an Interface

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Interfaces</strong> level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select <strong>Configure &gt; CLI Tools &gt; Point and Click CLI</strong>.</td>
<td>From the [edit] hierarchy level, enter <strong>edit interfaces</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Next to Interfaces, click <strong>Edit</strong>.</td>
<td></td>
</tr>
<tr>
<td>Select the interface you want to delete.</td>
<td>In the Interface table, under Interface name, select the name of the interface you want to delete.</td>
<td>Enter <strong>delete interface-name</strong>.</td>
</tr>
<tr>
<td></td>
<td>For information about interface names, see “Network Interface Naming” on page 9.</td>
<td></td>
</tr>
<tr>
<td>Execute the selection.</td>
<td>1. Click <strong>Discard</strong>.</td>
<td>Commit the configuration change: <strong>commit</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the page that appears, select the appropriate option button.</td>
<td>If you have not made any previous changes, the only selection available is <strong>Delete Configuration Below This Point</strong>.</td>
</tr>
</tbody>
</table>

### Verifying Interface Configuration

To verify an interface configuration, perform these tasks:

- Verifying the Link State of All Interfaces on page 113
- Verifying Interface Properties on page 114

#### Verifying the Link State of All Interfaces

**Purpose**

By using the ping tool on each peer address in the network, verify that all interfaces on the device are operational.

**Action**

For each interface on the device:

1. In the J-Web interface, select **Troubleshoot > Ping Host**.
2. In the Remote Host box, type the address of the interface for which you want to verify the link state.
3. Click **Start**. Output appears on a separate page.

**Sample Output**

```
PING 10.10.10.10 : 56 data bytes
```
64 bytes from 10.10.10.10: icmp_seq=0 ttl=255 time=0.382 ms
64 bytes from 10.10.10.10: icmp_seq=1 ttl=255 time=0.266 ms

**Meaning**  If the interface is operational, it generates an ICMP response. If this response is received, the round-trip time in milliseconds is listed in the `time` field. For more information about the output, see the *Junos OS Administration Guide for Security Devices*.

**Related Topics**  For more information about using the J-Web interface to ping a host, see the *Junos OS Administration Guide for Security Devices*.

For information about the `ping` command, see the *Junos OS Administration Guide for Security Devices* or the *Junos System Basics and Services Command Reference*.

**Verifying Interface Properties**

**Purpose**  Verify that the interface properties are correct.

**Action**  From the CLI, enter the `show interfaces detail` command.

**Sample Output**

```
user@host> show interfaces detail
Physical interface: ge-1/0/0, Enabled, Physical link is Up
  Interface index: 134, SNMP ifIndex: 27, Generation: 17
  Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled
  Device flags : Present Running
  Interface flags: SNMP-Traps 16384
  Link flags : None
  CoS queues : 4 supported
  Hold-times : Up 0 ms, Down 0 ms
  Current address: 00:90:69:87:44:9d, Hardware address: 00:90:69:87:44:9d
  Last flapped : 2004-08-25 15:42:30 PDT (4w5d 22:49 ago)
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes : 0 0 bps
    Output bytes : 0 0 bps
    Input packets: 0 0 pps
    Output packets: 0 0 pps
  Queue counters: Queued packets Transmitted packets Dropped packets
    0 best-effort 0 0 0
    1 expedited-fo 0 0 0
    2 assured-forw 0 0 0
    3 network-cont 0 0 0
  Active alarms : None
  Active defects : None
```
Meaning  The output shows a summary of interface information. Verify the following information:

- The physical interface is Enabled. If the interface is shown as Disabled, do one of the following:
  - In the CLI configuration editor, delete the disable statement at the [edit interfaces interface-name] level of the configuration hierarchy.
  - In the J-Web configuration editor, clear the Disable check box on the Interfaces > interface-name page.

- The physical link is Up. A link state of Down indicates a problem with the interface module, interface port, or physical connection (link-layer errors).

- The Last Flapped time is an expected value. The Last Flapped time indicates the last time the physical interface became unavailable and then available again. Unexpected flapping indicates likely link-layer errors.

- The traffic statistics reflect expected input and output rates. Verify that the number of inbound and outbound bytes and packets matches expected throughput for the physical interface. To clear the statistics and see only new changes, use the clear interfaces statistics interface-name command.

Related Topics  For a complete description of show interfaces detail output, see the Junos Interfaces Command Reference.
Chapter 3
Configuring Channelized T1/E1/ISDN PRI Interfaces

The J Series device supports the software-configurable interfaces on the Dual-Port Channelized T1/E1/ISDN PRI PIM. Each interface can be partitioned into T1 or E1 DS0 channels, or into a combination of T1 or E1 and ISDN Primary Rate Interface (PRI) B-channels and a D-channel.

**NOTE:** You cannot configure channelized T1/E1/ISDN/PRI interfaces through a J-Web Quick Configuration page. You must use the J-Web or CLI configuration editor. Even after configuration, channelized interfaces do not appear on the Quick Configuration Interfaces page.

For more information about interfaces, see “Interfaces Overview” on page 3 and the Junos Network Interfaces Configuration Guide. For ISDN information, see “Configuring ISDN” on page 309.

For information about which devices support the features documented in this chapter, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.

This chapter contains the following topics:

- Channelized T1/E1/ISDN PRI Terms on page 117
- Channelized T1/E1/ISDN PRI Overview on page 118
- Before You Begin on page 120
- Configuring Channelized T1/E1/ISDN PRI interfaces with a Configuration Editor on page 120
- Verifying Channelized T1/E1/ISDN PRI Interfaces on page 128
- Frequently Asked Questions About Channelized T1/E1/ISDN PRI Interfaces on page 130

Channelized T1/E1/ISDN PRI Terms

Before configuring channelized T1/E1/ISDN PRI interfaces on a J Series device, become familiar with the terms defined in Table 30 on page 118.
Table 30: Channelized T1/E1/ISDN PRI Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel group</td>
<td>Combination of DS0 or ISDN PRI B-channels interfaces partitioned from a channelized interface into a single logical bundle.</td>
</tr>
<tr>
<td>channelized E1</td>
<td>2.048-Mbps interface that can be configured as a single clear-channel E1 interface or channelized into as many as 31 discrete DS0 interfaces, or up to 30 ISDN PRI B-channels and 1 D-channel. On J Series channelized T1/E1/ISDN PRI interfaces, time slots are numbered from 1 through 31, and time slot 1 is reserved for framing. When the interface is configured for ISDN PRI service, time slot 16 is reserved for the D-channel.</td>
</tr>
<tr>
<td>channelized interface</td>
<td>Interface that is a subdivision of a larger interface, minimizing the number of Physical Interface Modules (PIMs) that an installation requires. On a channelized PIM, each port can be configured as a single T1 or E1 clear channel or partitioned into multiple discrete DS0 interfaces or ISDN PRI channels.</td>
</tr>
<tr>
<td>channelized T1</td>
<td>1.544-Mbps interface that can be configured as a single clear-channel T1 interface or channelized into as many as 24 discrete DS0 interfaces, or up to 23 ISDN PRI B-channels and 1 D-channel. When the interface is configured for ISDN PRI service, time slot 24 is reserved for the D-channel.</td>
</tr>
<tr>
<td>E1 interface</td>
<td>Physical WAN interface for transmitting signals in European digital transmission (E1) format. The E1 signal format transmits information at a rate of 2.048 Mbps and can carry 32 channels of 64 Kbps each.</td>
</tr>
<tr>
<td>Primary Rate Interface (PRI)</td>
<td>ISDN service intended for higher-bandwidth applications than ISDN BRI. ISDN PRI consists of a single D-channel for control and signaling, plus a number of 64-Kbps B-channels—either 23 B-channels on a T1 line or 30 B-channels on an E1 line—to carry network traffic.</td>
</tr>
<tr>
<td>T1 interface</td>
<td>Physical WAN interface for transmitting digital signals in the T-carrier system used in the United States, Japan, and Canada. The T1 signal format carries 24 pulse code modulation (PCM) signals using time-division multiplexing (TDM) at an overall rate of 1.544 Mbps.</td>
</tr>
</tbody>
</table>

Channelized T1/E1/ISDN PRI Overview

You can configure a channelized T1/E1/ISDN PRI interface for T1 or E1 or ISDN PRI service.

On a channelized T1/E1/ISDN PRI PIM configured for channelized operation, you can use the "drop-and-insert" feature to integrate voice and data on a single T1 or E1 link, and save the cost of two lines.

This overview contains the following topics:
- Channelized T1/E1/ISDN PRI Interfaces on page 118
- Drop and Insert on page 119
- ISDN PRI Transmission on Channelized Interfaces on page 119

Channelized T1/E1/ISDN PRI Interfaces

Each port on a channelized T1/E1/ISDN PRI PIM is software configurable for T1, E1, or ISDN PRI service. Each channelized T1 or E1 interface can be configured as a
single clear channel, or for fractional (NxDS0) or channelized operation, where \( N \) is channels 1 to 31 for an E1 interface and channels 1 to 24 for a T1 interface.

Each channelized interface can be configured as ISDN PRI B-channels and one D-channel or as a combination of T1 or E1 DS0 channels and ISDN PRI channels.

J Series ISDN PRI interfaces support the following switch types:

- **ATT5E**—AT&T 5ESS
- **ETSI**—NET3 for the United Kingdom and Europe
- **NI2**—National ISDN-2
- **NTDMS100**—Northern Telecom DMS-100
- **NTT**—NTT Group switch for Japan

For more information, see “ISDN PRI Transmission on Channelized Interfaces” on page 119.

Channelized T1/E1/ISDN PRI interfaces are configured through a configuration editor only.

A channelized T1/E1/ISDN PRI interface supports CoS configuration. For information about CoS features, see *Junos OS Class of Service Configuration Guide for Security Devices*.

**Drop and Insert**

On channelized T1/E1 interfaces configured for channelized operation, you can insert channels (time slots) from one port (for example, channels carrying voice) directly into the other port on the PIM, to replace channels coming through the Routing Engine. This feature, known as drop and insert, allows you to integrate voice and data on a single T1 or E1 link by removing the DS0 time slots of one T1 or E1 port and replacing them by inserting the time slots of another T1 or E1 port. You need not use the same time slots on both interfaces, but the time slots count must be the same.

The channels that are not configured for the drop-and-insert feature are used for normal traffic.

**ISDN PRI Transmission on Channelized Interfaces**

The Dual-Port Channelized T1/E1/ISDN PRI PIM provides support for ISDN PRI services such as dial-in at the central office, callback from the central office, and primary or backup network connections from branch offices. For more information about the services, see “Configuring ISDN” on page 309.

You can configure up to 23 time slots in a channelized T1 PRI interface and up to 30 time slots in a channelized E1 PRI interface as B-channels. The 24th time slot in a T1 interface and the 16th time slot in an E1 interface are configured as the D-channel interface for signaling purposes. Each B-channel supports 64 Kbps of traffic. The unconfigured time slots can be used as regular DS0 interfaces on top of the T1 or E1 physical layer.
You can install channelized T1/E1/ISDN PRI PIMs and ISDN BRI PIMs and configure both ISDN PRI and ISDN BRI service on the same J Series device.

**Before You Begin**

Before you configure network interfaces, you need to perform the following tasks:

- Install J Series device hardware. For more information, see the *J Series Services Routers Hardware Guide*.
- Establish basic connectivity. For more information, see the Getting Started Guide for your device.
- If you do not already have a basic understanding of physical and logical interfaces and Juniper Networks interface conventions, read “Interfaces Overview” on page 3.

Although it is not a requirement, you might also want to plan how you are going to use the various network interfaces before you start configuring them.

**Configuring Channelized T1/E1/ISDN PRI interfaces with a Configuration Editor**

Each port on a channelized T1/E1/ISDN PRI PIM is software configurable as a T1 or E1 clear channel. You can partition each port into up to 24 DS0 channels on a T1 interface or up to 31 DS0 channels on an E1 interface, and can insert channels from one port into another with the drop-and-insert feature.

Channelized T1/E1/ISDN PRI ports can also be partitioned into channels for ISDN PRI service.

Channelized T1/E1/ISDN PRI interfaces are configured through a configuration editor only.

This section includes the following topics:

- Configuring Channelized T1/E1/ISDN PRI Interface as a Clear Channel on page 120
- Configuring Channelized T1/E1/ISDN PRI Interface to Drop and Insert Time Slots on page 123
- Configuring Channelized T1/E1/ISDN PRI Interfaces for ISDN PRI Operation on page 125

**Configuring Channelized T1/E1/ISDN PRI Interface as a Clear Channel**

To configure or edit a channelized T1/E1/ISDN PRI interface as a clear channel:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 31 on page 121.
3. If you are finished configuring the J Series device, commit the configuration.
4. To verify the configuration, see “Verifying Interface Configuration” on page 113.
NOTE: When you configure a T1 or an E1 interface on the SRX-GP-QUAD-T1-E1 or SRX-GP-DUAL-T1-E1, the line encoding and the framing must be specified under the ct1-n/n/n interface, whereas the remaining T1 or E1 specific configuration items must be configured under the t1-n/n/n or e1-n/n/n interface, respectively.

Table 31: Configuring a Channelized T1/E1/ISDN PRI interface as a Clear Channel

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Interfaces level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter one of the following:</td>
</tr>
<tr>
<td>For information about interface names, see “Network Interface Naming” on page 9.</td>
<td>2. Next to Interfaces, click Edit.</td>
<td>edit interfaces ct1-3/0/0</td>
</tr>
<tr>
<td>Create the new interface—for example, ct1-3/0/0 or ce1-3/0/0.</td>
<td>1. Next to Interfaces, click Add new entry.</td>
<td>edit interfaces ce1-3/0/0</td>
</tr>
<tr>
<td>Configure interface options:</td>
<td>2. In the Interface name box, type one of the following interface names:</td>
<td></td>
</tr>
<tr>
<td>■ Specify a transmit clock source—for example, internal. Internal clocking uses the device’s own system clock (the default).</td>
<td>■ ct1-3/0/0</td>
<td></td>
</tr>
<tr>
<td>■ External clocking uses a signal received from the T1 or E1 interface.</td>
<td>■ ce1-3/0/0</td>
<td></td>
</tr>
<tr>
<td>■ Describe the physical interface.</td>
<td>3. Click OK.</td>
<td></td>
</tr>
<tr>
<td>■ To delay the advertisement of interface transitions from up to down or down to up, set the link hold down time or link hold up time, or both. Set a value in milliseconds from 0 (the default) through 65534—for example, 500.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ To use the channelizable interface as a single clear channel, specify no partition.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ To use subunit queuing on Frame Relay or virtual LAN (VLAN) IQ interfaces, enable the per-unit scheduler.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. In the Interface table, under Interface name, click the interface you are configuring:</td>
<td>1. Enter set clocking internal</td>
<td></td>
</tr>
<tr>
<td>■ ct1-3/0/0</td>
<td>2. Add a description:</td>
<td>■ For T1 interfaces, enter set description clear t1 interface.</td>
</tr>
<tr>
<td>■ ce1-3/0/0</td>
<td>■ For E1 interfaces, enter set description clear e1 interface.</td>
<td>■ For E1 interfaces, enter set description clear e1 interface.</td>
</tr>
<tr>
<td>2. From the Clocking list, select internal</td>
<td>3. Enter set hold-time down 500 up 500</td>
<td></td>
</tr>
<tr>
<td>3. In the Description box, type one of the following descriptions:</td>
<td>4. Specify a clear channel:</td>
<td>■ For T1 interfaces, enter set no-partition interface-type t1.</td>
</tr>
<tr>
<td>■ clear t1 interface</td>
<td>■ For E1 interfaces, enter set no-partition interface-type e1.</td>
<td>■ For E1 interfaces, enter set no-partition interface-type e1.</td>
</tr>
<tr>
<td>■ clear e1 interface</td>
<td>5. Enter set per-unit-scheduler</td>
<td></td>
</tr>
<tr>
<td>4. Under Hold time:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Next to Down, type 500.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Next to Up, type 500.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Under No partition, from the Interface type list, select the type of interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ t1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ e1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. From the Scheduler type list, select Per unit scheduler.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 31: Configuring a Channelized T1/E1/ISDN PRI interface as a Clear Channel (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure T1 or E1 options:</td>
<td>1. Next to T1 options or E1 options, click <strong>Configure</strong>.</td>
<td>1. Enter <strong>set bert-algorithm all-ones-repeating</strong></td>
</tr>
<tr>
<td>■ Bit error rate test (BERT) algorithm—for example, all ones repeating.</td>
<td>2. From the Bert algorithm list, select <strong>all-ones-repeating</strong>.</td>
<td>2. Enter <strong>set bert-error-rate 5</strong></td>
</tr>
<tr>
<td>■ BERT error rate, a value from 0 through 7—for example, 5.</td>
<td>3. In the Bert error rate box, type 5.</td>
<td>3. Enter <strong>set bert-period 5</strong></td>
</tr>
<tr>
<td>■ BERT period, in seconds, a value from 1 through 240—for example, 5.</td>
<td>4. In the Bert period box, type 5.</td>
<td>4. For T1 interfaces only, enter <strong>set buildout 0-132</strong></td>
</tr>
<tr>
<td>■ (T1 interfaces only) Line buildout, in feet for cables 655 ft (200 m) or shorter—for example, 0-132—or in decibels for longer cables.</td>
<td>5. For T1 interfaces only, from the Buildout list, select <strong>0-132</strong>.</td>
<td>5. Set the framing mode:</td>
</tr>
<tr>
<td>■ Framing mode:</td>
<td>6. From the Framing list:</td>
<td>■ For T1 interfaces, enter <strong>set framing esf</strong></td>
</tr>
<tr>
<td>■ For T1 interfaces, either superframe or extended superframe (ESF)—for example, ESF</td>
<td>• For T1 interfaces, select <strong>esf</strong>.</td>
<td>• For E1 interfaces, select <strong>g704</strong>.</td>
</tr>
<tr>
<td>■ For E1 interfaces, G704, G704 without cyclic redundancy check 4 (CRC4), or G703 unframed—for example, G704.</td>
<td>7. For T1 interfaces only, from the Line encoding list, select <strong>ami</strong>.</td>
<td>6. For T1 interfaces only, enter <strong>set line encoding ami</strong></td>
</tr>
<tr>
<td>■ (T1 interfaces only) Line encoding method—for example, alternate mark inversion (AMI).</td>
<td>8. From the Loopback list, select <strong>local</strong>.</td>
<td>7. Enter <strong>set loopback local</strong></td>
</tr>
<tr>
<td>■ Loopback mode—for example, local.</td>
<td>9. Click <strong>OK</strong></td>
<td></td>
</tr>
</tbody>
</table>

Configure trace options. | 1. Next to Traceoptions, select the check box and click **Configure**. | Enter **set traceoptions flag all** |
| 2. Next to Flag, click **Add new entry**. | | |
| 3. From the Flag name list, select **all**. | | |
| 4. Click **OK** until you return to the Interface page. | | |

Configure advanced options. | 1. Next to Advanced, click the expand (+) icon. | Enter **set interfaces apply-groups test** |
| For example, apply configuration settings from one or more groups except the test group. | 2. Next to Apply groups except, click **Add new entry**. | |
| 3. In the Value box, type **test**. | | |
| 4. Click **OK**. | | |
Configuring Channelized T1/E1/ISDN PRI Interface to Drop and Insert Time Slots

On channelized T1/E1/ISDN PRI interfaces configured for channelized operation, you can insert channels (time slots) from one port (for example, channels carrying voice) directly into the other port on the PIM, to replace channels coming through the Routing Engine. Although you need not use the same time slots on both interfaces, the time slots count must be the same. The channels that are not configured for the drop-and-insert feature are used for normal traffic.

You must ensure that the signaling channels (port 16 for an E1 interface and port 24 for a T1 interface) are also part of the channels that are being switched through the drop-and-insert functionality. JUNOS Software does not support switching of voice and data between ports by default.

Both ports involved in the drop-and-insert configuration must use the same clock source—either the device’s internal clock or an external clock. The following clock source settings are valid:

- When port 0 is set to use the internal clock, port 1 must also be set to use it, and vice versa.
- When port 0 is set to use its external clock, port 1 must be set to run on the same clock—the external clock for port 0.
- When port 1 is set to use its external clock, port 0 must be set to run on the same clock—the external clock for port 1.

For more details about valid clock combinations, see “Frequently Asked Questions About Channelized T1/E1/ISDN PRI Interfaces” on page 130.

To configure or edit the drop-and-insert feature on a channelized T1/E1/ISDN PRI interface:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 32 on page 124.
3. If you are finished configuring the device, commit the configuration.
4. To verify the configuration, see “Verifying Interface Configuration” on page 113.
### Table 32: Configuring a Channelized T1/E1/ISDN PRI Interface to Drop and Insert Time Slots

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Interfaces</strong> level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select <strong>Configure &gt; CLI Tools &gt; Point and Click CLI</strong>.</td>
<td>From the <strong>[edit]</strong> hierarchy level, enter <strong>edit interfaces ct1-3/0/0</strong>.</td>
</tr>
<tr>
<td>For information about interface names, see “Network Interface Naming” on page 9.</td>
<td>2. Next to Interfaces, click <strong>Edit</strong>.</td>
<td></td>
</tr>
<tr>
<td>Create a new interface—for example, <strong>ct1-3/0/0</strong>.</td>
<td>1. Next to Interfaces, click <strong>Add new entry</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. In the Interface name box, type <strong>ct1-3/0/0</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td>Configure the clock source and partition on <strong>ct1-3/0/0</strong>.</td>
<td>1. In the Interface name column, click <strong>ct1-3/0/0</strong>.</td>
<td>From the <strong>[edit]</strong> hierarchy level, enter <strong>set interfaces ct1-3/0/0 clocking external</strong>.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> While configuring the drop-and-insert feature, you must ensure that both ports on the channelized T1/E1 PIM run on the same clock.</td>
<td>2. On the Interfaces page, next to Clocking, select the check box and click <strong>Configure</strong>.</td>
<td>set interfaces ct1-3/0/0 partition 1 timeslots 1-10</td>
</tr>
<tr>
<td>For more details about valid clock combinations, see “Frequently Asked Questions About Channelized T1/E1/ISDN PRI Interfaces” on page 130.</td>
<td>3. From the Clocking choices list, select <strong>external</strong>.</td>
<td>set interfaces ct1-3/0/0 partition 1 interface-type ds</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. On the Interfaces page, next to Partition, click <strong>Add new entry</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. On the Interface Partition page, type 1 in the Partition number box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. From the Interface type list, Select <strong>ds</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. In the Timeslots box, type 1-10.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9. Click <strong>OK</strong> twice.</td>
<td></td>
</tr>
<tr>
<td>Create a new interface—for example, <strong>ct1-3/0/1</strong>.</td>
<td>1. On the Interfaces Configuration page, next to Interface, click <strong>Add new entry</strong>.</td>
<td>From the <strong>[edit]</strong> hierarchy level, enter <strong>edit interfaces ct1-3/0/1</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. In the Interface name box, type <strong>ct1-3/0/1</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>OK</strong>.</td>
<td></td>
</tr>
</tbody>
</table>
Table 32: Configuring a Channelized T1/E1/ISDN PRI Interface to Drop and Insert Time Slots (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the clock source and partition on ct1-3/0/1.</td>
<td>1. On the Interfaces Configuration page, click ct1-3/0/1 in the Interface name column.</td>
<td>From the [edit] hierarchy level, enter set interfaces ct1-3/0/1 clocking external interface ct1-3/0/0</td>
</tr>
<tr>
<td>NOTE: While configuring the drop-and-insert feature, you must ensure that both ports on the channelized T1/E1 PIM run on the same clock.</td>
<td>2. Next to Clocking, select the Yes check box, and click Configure.</td>
<td>set interfaces ct1-3/0/1 partition 1 timeslots 1-10</td>
</tr>
<tr>
<td>For more details about valid clock combinations, see “Frequently Asked Questions About Channelized T1/E1/ISDN PRI Interfaces” on page 130.</td>
<td>3. From the Clocking choices list, select external.</td>
<td>set interfaces ct1-3/0/1 partition 1 interface-type ds</td>
</tr>
<tr>
<td>Create new interfaces—for example, ds-3/0/0:1, ds-3/0/1:1 and configure drop-and-insert feature.</td>
<td>4. Next to External, click Configure.</td>
<td></td>
</tr>
<tr>
<td>NOTE: Both interfaces configured for the drop-and-insert feature must exist on the same PIM. For example, you can configure ds-3/0/0:1 as the data input interface for ds-3/0/1:1, but not for ds-4/0/0:1.</td>
<td>5. In the Interface box, type ct1-3/0/0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Click OK twice.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. On the Interfaces page, next to Partition, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. On the Interface Partition page, type 1 in the Partition number box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9. From the Interface type list, Select ds</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10. In the Timeslots box, type 1-10.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>11. Click OK twice</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Channelized T1/E1/ISDN PRI Interfaces for ISDN PRI Operation

On a J Series device with Dual-Port Channelized T1/E1/ISDN PRI PIMs, you can configure each port for either T1, E1, or ISDN PRI service, or for a combination of ISDN PRI and either channelized T1 or E1 service. For a channelized T1 interface with ISDN PRI service, you can configure 23 B-channels and for a channelized E1 interface with ISDN PRI service, you can configure 30 B-channels.
You must also explicitly configure a D-channel: time slot 24 on a channelized T1 interface and time slot 16 on a channelized E1 interface. In addition, you select a switch type and trace options.

Setting up the J Series device for ISDN PRI operation is a multipart process. First, you add ISDN PRI service on a channelized interface as shown here. Second, you follow the instructions in “Configuring Dialer Interfaces (Required)” on page 324 to configure a dialer interface. You can then configure ISDN services such as dial-in, callback, and backup. For details, see “Configuring ISDN” on page 309.

To configure an ISDN PRI network service on a channelized T1 or E1 interface for the J Series device:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 33 on page 126.
3. Go on to “Configuring Dialer Interfaces (Required)” on page 324.

### Table 33: Adding an ISDN PRI Service to a Channelized T1/E1/ISDN PRI Interface

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Navigate to the **Interfaces** level in the configuration hierarchy. | 1. In the J-Web interface, select Configure > CLI Tools > Point and Click CLI.  
2. Next to Interfaces, click **Edit**. | From the [edit] hierarchy level, enter edit interfaces ct1-2/0/0 |
| Create a new interface—for example, ct1-2/0/0. | 1. Next to Interfaces, click **Add new entry**.  
2. In the Interface name box, type ct1–2/0/0.  
3. Click **OK**. | |

For information about interface names, see “Network Interface Naming” on page 9.
Table 33: Adding an ISDN PRI Service to a Channelized T1/E1/ISDN PRI Interface (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the partition and interface type. For example, partition the interface into time slots 1 through 23 for B-channels and time slot 24 for the D-channel. For a channelized T1 interface, you can configure 1 through 23 as B-channels and the 24th channel as the signaling channel (D-channel). For a channelized E1 interface, you can configure 1 through 15 and 17 through 31 as B-channels and the 16th channel as the signaling channel (D-channel).</td>
<td>1. In the Interface name column, click ct1-2/0/0. 2. On the Interfaces page, next to Partition, click Add new entry. 3. In the Partition number box, type 1-23. 4. In the Timeslots box, type 1-23. 5. From the Interface type list, Select bc. 6. Click OK. 7. On the Interfaces page, next to Partition, click Add new entry. 8. In the Partition number box, type 24. 9. In the Timeslots box, type 24. 10. From the Interface type list, Select dc. 11. Click OK.</td>
<td>From the [edit] hierarchy level, enter set interfaces ct1-2/0/0 partition 1-23 timeslots 1-23 set interfaces ct1-2/0/0 partition 1-23 interface-type bc set interfaces ct1-2/0/0 partition 24 timeslots 24 set interfaces ct1-2/0/0 partition 24 interface-type dc</td>
</tr>
<tr>
<td>Configure a trace options flag.</td>
<td>1. Next to Traceoptions, select the check box and click Configure. 2. Next to Flag, click Add new entry. 3. From the Flag name list, select q921. 4. Click OK until you return to the Interface page.</td>
<td>From the [edit] hierarchy level, enter set interfaces ct1-2/0/0 traceoptions flag q921</td>
</tr>
<tr>
<td>Configure B-channel allocation order for allocating a free B-channel for dial-out calls. You can allocate from the lowest-numbered or highest-numbered time slot. The default value is descending.</td>
<td>1. On the Interfaces page, next to Isdn options, click Configure. 2. From the Bchannel allocation list, select ascending. 3. Click OK.</td>
<td>To set the ISDN options, from the [edit] hierarchy level, enter set interfaces ct1-2/0/0 isdn-options bchannel-allocation ascending</td>
</tr>
<tr>
<td>Select the type of ISDN switch—for example, Ni2. The following switches are compatible with J Series devices: ATT5E—AT&amp;T 5ESS ETSI—NET3 for the UK and Europe Ni2—National ISDN-2 NTDMS-100—Northern Telecom DMS-100 NTT—NTT Group switch for Japan</td>
<td>From the Switch type list, select ni2</td>
<td>From the [edit] hierarchy level, enter set interfaces ct1-2/0/0 isdn-options switch-type ni2</td>
</tr>
</tbody>
</table>
Table 33: Adding an ISDN PRI Service to a Channelized T1/E1/ISDN PRI Interface (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Q.931 timers. Q.931 is a Layer 3 protocol for the setup and termination of connections. The default value for each timer is 10 seconds, but can be configured between 1 and 65536 seconds—for example, 15.</td>
<td>1. In the T310 box, type 15. 2. Click OK.</td>
<td>From the [edit] hierarchy level, enter set isdn-options t310 15</td>
</tr>
<tr>
<td>Configure dialer options.</td>
<td>1. On the Interfaces page, next to Dialer options, select Yes and then click configure. 2. Next to Pool, click Add new entry. 3. In the Pool identifier box, type isdn-dialer-group. 4. In the Priority box, type 1. 5. Click OK.</td>
<td>From the [edit interfaces ct1-2/0/0] hierarchy level, enter set dialer-options pool isdn-dialer-group priority 1</td>
</tr>
<tr>
<td>Dialer pool priority has a range from 1 to 255, with 1 designating lowest-priority interfaces and 255 designating the highest-priority interfaces.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To configure a dialer interface, see “Configuring Dialer Interfaces (Required)” on page 324.

Verifying Channelized T1/E1/ISDN PRI Interfaces

To verify an interface configuration, perform these tasks:
- Verifying Channelized Interfaces on page 128
- Verifying Clear-Channel Interfaces on page 129
- Verifying ISDN PRI Configuration on Channelized T1/E1/ISDN PRI Interfaces on page 130

Verifying Channelized Interfaces

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Verify that your configurations for the channelized interfaces are correct.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>From the CLI, enter the show interfaces ct1-3/0/1 command.</td>
</tr>
<tr>
<td>Sample Output</td>
<td>user@host&gt; show interfaces ct1-3/0/1</td>
</tr>
</tbody>
</table>

Physical interface: ct1-3/0/1, Enabled, Physical link is Up
Interface index: 151, SNMP ifIndex: 28
Link-level type: Controller, Clocking: Internal, Speed: E1, Loopback: None,
Framing: G704, Parent: None
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Last flapped : 2006-10-05 21:11:48 PDT (06:45:04 ago)
DS1 alarms : None
DS1 defects : None
Line encoding: HDB3

Meaning The output shows a summary of information about the physical parent interface—a channelized T1 interface in this example.

Related Topics For a complete description of `show interfaces` output, see the Junos Interfaces Command Reference.

Verifying Clear-Channel Interfaces

Purpose Verify that your configurations for the clear-channel interfaces are correct.

Action From the CLI, enter the `show interfaces e1-3/0/1` command.

Sample Output

```
user@host> show interfaces e1-3/0/1

Physical interface: e1-3/0/1, Enabled, Physical link is Up
   Interface index: 212, SNMP ifIndex: 237
   Link-level type: PPP, MTU: 1504, Speed: E1, Loopback: None, FCS: 16,
   Parent: ce1-3/0/1 Interface index 151
   Device flags   : Present Running
   Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
   Link flags     : Keepalives
   Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
   Keepalive: Input: 1066 (00:00:02 ago), Output: 1066 (00:00:02 ago)
   LCP state: Opened
   CHAP state: Closed
   CoS queues     : 8 supported, 8 maximum usable queues
   Last flapped   : 2006-10-06 01:01:36 PDT (02:57:27 ago)
   Input rate     : 88 bps (0 pps)
   Output rate    : 58144 bps (157 pps)
   DS1 alarms     : None
   DS1 defects    : None

Logical interface e1-3/0/1.0 (Index 66) (SNMP ifIndex 238)
   Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
   Bandwidth: 1984kbps
   Protocol inet, MTU: 1500
      Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
         Destination: 47.47.47.0/30, Local: 47.47.47.2, Broadcast: 47.47.47.3
   Protocol inet6, MTU: 1500
      Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
         Destination: 8b8b:8b01::/64, Local: 8b8b:8b01::2
      Addresses, Flags: Is-Preferred
         Destination: fe80::/64, Local: fe80::205:85ff:fece:d3d0
```
Meaning The output shows a summary of interface information. Although the parent interface is ce1-3/0/1, the physical and logical clear-channel interfaces are named e1-3/0/1 and e1-3/0/1.0.

Related Topics For a complete description of show interfaces output, see the Junos Interfaces Command Reference.

Verifying ISDN PRI Configuration on Channelized T1/E1/ISDN PRI Interfaces

Purpose Verify that your configuration of ISDN PRI service on a channelized interface is correct.

Action From the J-Web interface, select Configure > CLI Tools > CLI Viewer. Alternatively, from configuration mode in the CLI, enter the show interfaces ct1-2/0/0 command.

Sample Output user@host# show interfaces ct1-2/0/0

```
traceoptions {
  flag q921;
  file {
    isdnback;
  }
}
clocking external;
isdn-options {
  switch-type ni2;
}
dialer-options {
  isdn-dialer-group priority 1;
}
partition 24 timeslots 24 interface-type dc;
payment 1-23 timeslots 1-23 interface-type bc;
```

[edit]

Meaning Verify that the output shows your intended ISDN PRI interface configuration.

Related Topics For more information about the format of a configuration file, see the J-Web Interface User Guide or the Junos CLI User Guide.

To additionally verify ISDN PRI configuration, see Verifying the ISDN Configuration on page 343.

Frequently Asked Questions About Channelized T1/E1/ISDN PRI Interfaces

Use answers to the following question to solve configuration problems on a channelized T1/E1/ISDN PRI interface:

- What Clock Combinations Are Possible for Channelized T1/E1/ISDN PRI Drop and Insert? on page 131
What Clock Combinations Are Possible for Channelized T1/E1/ISDN PRI Drop and Insert?

When you configure the drop-and-insert feature on a channelized T1/E1/ISDN PRI PIM, you must ensure that both ports run on the same clock. The following clock combinations are valid:

- When port 0 is configured to use the *internal* clock, port 1 must also be configured to use the *internal* clock.
- When port 0 is configured to use the *external* clock, port 1 must be configured to run on the same clock, the *external clock for port 0*.
- When port 1 is configured to use the *external* clock, port 0 must be configured to run on the same clock, the *external clock for port 1*.

J Series devices connected to one another must have complementary clock sources configured. Consider a scenario where Device R1 is connected to Devices R2 and R3. Port 0 on the channelized T1/E1/ISDN PRI PIM of R1 is connected to R2, and port 1 is connected to R3. The drop-and-insert feature is configured on R1 to insert input coming from R2 on port 0 into port 1 for transmission to R3.

Devices R1, R2, and R3 can be configured in three ways, according to whether the drop-and-insert clock source on R1 is the external clock for port 0, the external clock for port 1, or the device’s internal clock.

To configure the drop-and-insert interfaces on Device R1 to use the external clock for port 0:

1. On Device R2, configure:
   ```
   user@hostR2# set interfaces ct1-6/0/0 partition 1 timeslots 1-10
   user@hostR2# set interfaces ct1-6/0/0 partition 1 interface-type ds
   user@hostR2# set interfaces ds-6/0/0:1 unit 0 family inet address 10.46.46.1/30
   ```

2. On Device R3, configure:
   ```
   user@hostR3# set interfaces ct1-3/0/0 clocking external
   user@hostR3# set interfaces ct1-3/0/0 partition 1 timeslots 1-10
   user@hostR3# set interfaces ct1-3/0/0 partition 1 interface-type ds
   user@hostR3# set interfaces ds-3/0/0:1 unit 0 family inet address 10.46.46.2/30
   ```

3. On Device R1, configure:
   ```
   user@hostR1# set interfaces ct1-3/0/0 clocking external
   user@hostR1# set interfaces ct1-3/0/0 partition 1 timeslots 1-10
   user@hostR1# set interfaces ct1-3/0/0 partition 1 interface-type ds
   user@hostR1# set interfaces ds-3/0/0:1 data-input interface ds-3/0/1:1
   user@hostR1# set interfaces ct1-3/0/1 clocking external interface ct1-3/0/0
   user@hostR1# set interfaces ct1-3/0/1 partition 1 timeslots 1-10
   user@hostR1# set interfaces ct1-3/0/1 partition 1 interface-type ds
   ```

To configure the drop-and-insert interfaces on Device R1 to use the external clock for port 1:

1. On Device R2, configure:
   ```
   user@hostR2# set interfaces ct1-6/0/0 clocking external
   ```
2. On Device R3, configure:

    user@hostR3# set interfaces ct1-3/0/0 partition 1 timeslots 1-10
    user@hostR3# set interfaces ct1-3/0/0 partition 1 interface-type ds
    user@hostR3# set interfaces ds-3/0/0:1 unit 0 family inet address 10.46.46.2/30

3. On Device R1, configure:

    user@hostR1# set interfaces ct1-3/0/0 clocking external interface ct1-3/0/1
    user@hostR1# set interfaces ct1-3/0/0 partition 1 timeslots 1-10
    user@hostR1# set interfaces ct1-3/0/0 partition 1 interface-type ds
    user@hostR1# set interfaces ds-3/0/0:1 data-input interface ds-3/0/1:1
    user@hostR1# set interfaces ct1-3/0/1 clocking external
    user@hostR1# set interfaces ct1-3/0/1 partition 1 timeslots 1-10
    user@hostR1# set interfaces ct1-3/0/1 partition 1 interface-type ds

To configure the drop-and-insert interfaces on Device R1 to use the device’s internal clock:

1. On Device R2, configure:

    user@hostR2# set interfaces ct1-6/0/0 clocking external
    user@hostR2# set interfaces ct1-6/0/0 partition 1 timeslots 1-10
    user@hostR2# set interfaces ct1-6/0/0 partition 1 interface-type ds
    user@hostR2# set interfaces ds-6/0/0:1 unit 0 family inet address 10.46.46.1/30

2. On Device R3, configure:

    user@hostR3# set interfaces ct1-3/0/0 clocking external
    user@hostR3# set interfaces ct1-3/0/0 partition 1 timeslots 1-10
    user@hostR3# set interfaces ct1-3/0/0 partition 1 interface-type ds
    user@hostR3# set interfaces ds-3/0/0:1 unit 0 family inet address 10.46.46.2/30

3. On Device R1, configure:

    user@hostR1# set interfaces ct1-3/0/0 clocking internal
    user@hostR1# set interfaces ct1-3/0/0 partition 1 timeslots 1-10
    user@hostR1# set interfaces ct1-3/0/0 partition 1 interface-type ds
    user@hostR1# set interfaces ds-3/0/0:1 data-input interface ds-3/0/1:1
    user@hostR1# set interfaces ct1-3/0/1 clocking internal
    user@hostR1# set interfaces ct1-3/0/1 partition 1 timeslots 1-10
    user@hostR1# set interfaces ct1-3/0/1 partition 1 interface-type ds
The J Series and SRX210 devices support DSL features including ATM-over-ADSL and ATM-over-SHDSL interfaces.

You can use either J-Web Quick Configuration or a configuration editor to configure ATM-over-ADSL or ATM-over-SHDSL interfaces.

**NOTE:** Payload loopback functionality is not supported on ATM-over-SHDSL interfaces.

For information about which devices support the features documented in this chapter, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.

This chapter contains the following topics:

- DSL Terms on page 133
- Before You Begin on page 135
- Configuring ATM-over-ADSL Interfaces on page 135
- Configuring ATM-over-SHDSL Interfaces on page 145
- Configuring CHAP on DSL Interfaces (Optional) on page 155
- Verifying DSL Interface Configuration on page 156
- Configuring MLPPP over ADSL Interfaces on page 164

**DSL Terms**

Before configuring DSL on J Series or SRX210 devices, become familiar with the terms defined in Table 34 on page 134.
**Table 34: DSL Terms**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>asymmetric digital subscriber line (ADSL) interface</td>
<td>Physical WAN interface for connecting a J Series device to a digital subscriber line access multiplexer (DSLAM). An ADSL interface allocates line bandwidth asymmetrically with downstream (provider-to-customer) data rates of up to 8 Mbps for ADSL, 12 Mbps for ADSL2, and 25 Mbps for ADSL2 +, and upstream (customer-to-provider) rates of up to 800 Kbps for ADSL and 1 Mbps for ADSL2 and ADSL2 +, depending on the implementation.</td>
</tr>
<tr>
<td>ADSL2 interface</td>
<td>An ADSL interface that supports ITU-T Standards G.992.3 and G.992.4 and allocates downstream (provider-to-customer) data rates of up to 12 Mbps and upstream (customer-to-provider) rates of up to 1 Mbps.</td>
</tr>
<tr>
<td>ADSL2+ interface</td>
<td>An ADSL interface that supports ITU-T Standard G.992.5 and allocates downstream (provider-to-customer) data rates of up to 25 Mbps and upstream (customer-to-provider) rates of up to 1 Mbps.</td>
</tr>
<tr>
<td>Annex A</td>
<td>ITU-T Standard G.992.1 that defines how ADSL works over plain old telephone service (POTS) lines.</td>
</tr>
<tr>
<td>Annex B</td>
<td>ITU-T Standard G.992.1 that defines how ADSL works over Integrated Services Digital Network (ISDN) lines.</td>
</tr>
<tr>
<td>Annex M</td>
<td>ITU-DMT-BIS Standard G.992.3 and ADSL2PLUS Standard G.992.5 that extends the capability of basic ADSL2 by doubling the number of upstream bits.</td>
</tr>
<tr>
<td>ITU-T G.991.2</td>
<td>International Telecommunication Union standard describing a data transmission method for symmetric high-speed digital subscriber line (SHDSL) as a means for data transport in telecommunications access networks. The standard also describes the functionality required for interoperability of equipment from various manufacturers.</td>
</tr>
<tr>
<td>ITU-T G.992.1</td>
<td>International Telecommunication Union standard that requires the downstream (provider-to-customer) data transmission to consist of full-duplex low-speed bearer channels and simplex high-speed bearer channels. In the upstream (customer-to-provider) transmissions, only low-speed bearer channels are provided.</td>
</tr>
<tr>
<td>ITU-T G.994.1</td>
<td>International Telecommunication Union standard describing the types of signals, messages, and procedures exchanged between digital subscriber line (DSL) equipment when the operational modes of equipment need to be automatically established and selected.</td>
</tr>
<tr>
<td>ITU-T G.997.1</td>
<td>International Telecommunication Union standard describing the physical layer management for asymmetric digital subscriber line (ADSL) transmission systems. The standard specifies the means of communication on a transport transmission channel defined in the physical layer recommendations. In addition, the standard describes the content and syntax of network elements for configuration, fault management, and performance management.</td>
</tr>
<tr>
<td>symmetric high-speed digital subscriber line (G.SHDSL)</td>
<td>Physical WAN symmetric DSL interface capable of sending and receiving high-speed symmetrical data streams over a single pair of copper wires at rates between 192 Kbps and 2.31 Mbps. G.SHDSL incorporates features of other DSL technologies such as asymmetric DSL and transports T1, E1, ISDN, Asynchronous Transfer Mode (ATM), and IP signals.</td>
</tr>
<tr>
<td>symmetric high-speed digital subscriber line (SHDSL) transceiver unit–remote (STU–R)</td>
<td>Equipment that provides symmetric high-speed digital subscriber line (SHDSL) connections to remote user terminals such as data terminals or telecommunications equipment.</td>
</tr>
</tbody>
</table>

---

**JUNOS Software Interfaces and Routing Configuration Guide**
Before You Begin

Before you begin configuring DSL interfaces, complete the following tasks:

- Establish basic connectivity. See the Getting Started Guide for your device.
- If you do not already have a basic understanding of physical and logical interfaces and Juniper Networks interface conventions, read “Interfaces Overview” on page 3.
- Configure network interfaces as necessary. See “Configuring Ethernet, DS1, DS3, and Serial Interfaces” on page 81.

Configuring ATM-over-ADSL Interfaces

J Series devices with ADSL Annex A or Annex B PIMs can use an Asynchronous Transfer Mode (ATM) interface to send network traffic through a point-to-point connection to a DSL access multiplexer (DSLAM).

NOTE: You can configure J Series devices with ADSL PIMs for connections through ADSL only, not for direct ATM connections.

To configure Point-to-Point Protocol (PPP), see the Junos Network Interfaces Configuration Guide.

You configure the underlying ADSL interface as an ATM interface, with an interface name of at-pim/0/port. (For information about interface names, see “Network Interface Naming” on page 9.) Multiple encapsulation types are supported on both the physical and logical ATM-over-ADSL interface.

This section contains the following topics:

- Configuring an ATM-over-ADSL Interface with Quick Configuration on page 135
- Adding an ATM-over-ADSL Network Interface with a Configuration Editor on page 140

Configuring an ATM-over-ADSL Interface with Quick Configuration

The Quick Configuration pages allow you to configure ATM-over-ADSL interfaces on J Series devices.

To configure an ATM-over-ADSL interface with Quick Configuration:

1. In the J-Web user interface, select Configure > Interfaces.

   A list of the network interfaces present on the device is displayed. (See “Network Interface Naming” on page 9.)

2. Select the at-pim/0/port interface name for the ADSL port you want to configure.
The ATM-over-ADSL Quick Configuration page is displayed, as shown in Figure 24 on page 136.

**Figure 24: ATM-over-ADSL Interfaces Quick Configuration Page**

3. Enter information into the ATM-over-ADSL Quick Configuration pages, as described in Table 35 on page 136.

4. From the ATM-over-ADSL Quick Configuration main page, click one of the following buttons:
   - To apply the configuration and stay on the ATM-over-ADSL Quick Configuration main page, click **Apply**.
   - To apply the configuration and return to the Interfaces Quick Configuration page, click **OK**.
   - To cancel your entries and return to the Interfaces Quick Configuration page, click **Cancel**.

5. To verify that the ATM-over-ADSL interface is configured properly, see “Verifying DSL Interface Configuration” on page 156.

**Table 35: ATM-over-ADSL Interface Quick Configuration Pages Summary**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuring Logical Interfaces</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Interfaces</td>
<td>Lists the logical interfaces for this ATM-over-ADSL physical interface.</td>
<td>■ To add a logical interface, click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ To edit a logical interface, select the interface from the list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ To delete a logical interface, select the check box next to the name and click <strong>Delete</strong>.</td>
</tr>
<tr>
<td><strong>Adding or Editing a Logical Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add logical interfaces</td>
<td>Defines one or more logical units that you connect to this physical ADSL interface.</td>
<td>Click <strong>Add</strong>.</td>
</tr>
</tbody>
</table>
Table 35: ATM-over-ADSL Interface Quick Configuration Pages Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Interface Description</td>
<td>(Optional) Describes the logical interface.</td>
<td>Type a text description of the logical interface to more clearly identify it in monitoring displays.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Specifies the type of encapsulation on the DSL logical interface.</td>
<td>From the list, select one of the following types of encapsulations.</td>
</tr>
</tbody>
</table>

For ATM-over-ADSL interfaces that use inet (IPv4) protocols only, select one of the following:

- **ATM VC multiplexing**—Use ATM virtual circuit multiplex encapsulation.
- **ATM NLPID**—Use ATM network layer protocol identifier (NLPID) encapsulation.
- **Cisco-compatible ATM NLPID**—Use Cisco NLPID encapsulation.
- **Ethernet over ATM (LLC/SNAP)**—For interfaces that carry IPv4 traffic, use Ethernet over logical link control (LLC) encapsulation. You cannot configure multipoint interfaces if you use this type of encapsulation.

For ATM-over-ADSL for PPP-over-ATM (PPPoA) interfaces only, select one of the following:

- **ATM PPP over AAL5/LLC**—Use AAL5 logical link control (LLC) encapsulation.
- **ATM PPP over Raw AAL5**—Use AAL5 multiplex encapsulation.

For other encapsulation types on the ATM-over-ADSL interfaces, select one of the following:

- **PPPoE over ATM (LLC/SNAP)**—Use PPP over Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead you configure the interface address on the PPP interface.
- **Ethernet over ATM (LLC/SNAP)**—Use ATM subnetwork attachment point (SNAP) encapsulation.

<table>
<thead>
<tr>
<th>VCI</th>
<th>Configures the ATM virtual circuit identifier (VCI) for the interface.</th>
<th>In the VCI box, type the number for the VCI.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add IPv4 address prefixes and destinations</td>
<td>Specifies one or more IPv4 addresses and destination addresses.</td>
<td>Click Add.</td>
</tr>
</tbody>
</table>
### Table 35: ATM-over-ADSL Interface Quick Configuration Pages Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Address Prefix</td>
<td>Specifies an IPv4 address for the interface.</td>
<td>Type an IPv4 address and prefix. For example: 10.10.10.10/24.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Specifies the destination address.</td>
<td>1. Type an IPv4 address for the destination.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

### Configuring Physical Interface Properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface Description</td>
<td>(Optional) Adds supplementary information about the physical ATM-over-ADSL interface.</td>
<td>Type a text description of the physical ATM-over-ADSL interface to more clearly identify it in monitoring displays. Specify that it is an ADSL interface.</td>
</tr>
<tr>
<td>MTU (bytes)</td>
<td>Specifies the maximum transmit size of a packet for the ATM-over-ADSL interface.</td>
<td>Type a value from <strong>256</strong> to <strong>9192</strong>.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Selects the type of encapsulation for traffic on this physical interface.</td>
<td>From the list, select the type of encapsulation for this ATM-over-ADSL interface:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>ATM permanent virtual circuits</strong>—Use this type of encapsulation for PPP over ATM (PPPoA) over ADSL interfaces. This is the default encapsulation for ATM-over-ADSL interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Ethernet over ATM encapsulation</strong>—Use this type of encapsulation for PPP over Ethernet (PPPoE) over ATM-over-ADSL interfaces that carry IPv4 traffic.</td>
</tr>
<tr>
<td>VPI</td>
<td>Configures the ATM virtual path identifier for the interface.</td>
<td>Type a VPI value between <strong>0</strong> and <strong>255</strong>.</td>
</tr>
</tbody>
</table>

### Configuring ADSL Options
<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
<th>For Annex A or Annex B, or Annex M (applicable to SRX210 devices), select one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Mode</td>
<td>Specifies the type of DSL operating mode for the ATM-over-ADSL interface.</td>
<td>From the list, select one of the following types of DSL operating modes—for example auto.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>auto—Configure the ADSL interface to auto negotiate settings with the DSLAM located at the central office. For Annex A, the ADSL interface trains in either ANSI T1.413 Issue II mode or ITU G.992.1 mode. For Annex B, the ADSL interface trains in ITU G.992.1 mode. For Annex M, the ADSL interface trains in ITU G.992.3 mode (applicable to SRX210 devices).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>itu-dmt-bis—Configure the ADSL interface to train in ITU G.992.3 mode. The ADSL interface trains in ITU G.992.5 mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>adsl2plus—Configure the ADSL interface to train in ITU G.992.5 mode. You can configure this mode only when it is supported on the DSLAM.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Annex A and Annex B, select the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>itu-dmt—Configure the ADSL interface to train in ITU G.992.1 mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>adsl2plus—Configure the ADSL interface to train in ITU G.992.5 mode. You can configure this mode only when it is supported on the DSLAM.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>itu-dmt-bis—Configure the ADSL interface to train in ITU G.992.3 mode. The ADSL interface trains in ITU G.992.5 mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Annex A only, select the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ansi-dmt—Configure the ADSL interface to train in the ANSI T1.413 Issue II mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Annex B only, select the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>itu-annexb-ur2—Configure the ADSL line to train in the G.992.1 Deutsche Telekom UR-2 mode.</td>
<td></td>
</tr>
</tbody>
</table>
Adding an ATM-over-ADSL Network Interface with a Configuration Editor

To configure ATM-over-ADSL network interfaces for the J Series device with a configuration editor:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 36 on page 140.
3. If you are finished configuring the J Series device, commit the configuration.
4. Go on to one of the following procedures:
   - To enable authentication on the interface, see “Configuring CHAP on DSL Interfaces (Optional)” on page 155.
   - To configure PPP over Ethernet (PPPoE) encapsulation on an Ethernet interface or on an ATM-over-ADSL interface, see “Configuring Point-to-Point Protocol over Ethernet” on page 289.
5. To check the configuration, see “Verifying DSL Interface Configuration” on page 156.

Table 36: Adding an ATM-over-ADSL Network Interface

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Interfaces</strong> level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select <strong>Configure &gt; CLI Tools &gt; Point and Click CLI</strong>.</td>
<td>From the [edit] hierarchy level, enter edit interfaces at-2/0/0.</td>
</tr>
<tr>
<td></td>
<td>2. Next to Interfaces, click <strong>Edit</strong>.</td>
<td>edit interfaces at-2/0/0.</td>
</tr>
<tr>
<td>Create the new interface—for example, at-2/0/0.</td>
<td>1. Next to Interface, click <strong>Add new entry</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. In the Interface name box, type at-2/0/0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>OK</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Physical Properties
Table 36: Adding an ATM-over-ADSL Network Interface (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure ATM virtual path identifier (VPI) options for the interface—for example, at-2/0/0.</td>
<td></td>
<td>1. To configure the VPI value, enter set atm-options vpi 25</td>
</tr>
<tr>
<td>▪ ATM VPI—A number between 0 and 255—for example, 25.</td>
<td></td>
<td>2. To configure OAM liveness values on a VPI, enter set atm-options vpi 25 oam-liveness up-count 200 down-count 200</td>
</tr>
<tr>
<td>▪ Operation, Maintenance, and Administration (OAM) F5 loopback cell thresholds (&quot;liveness&quot;) on ATM virtual circuits. The range is between 1 and 255, and the default is 5 cells.</td>
<td></td>
<td>3. To configure the OAM period, enter set atm-options vpi 25 oam-period 100</td>
</tr>
<tr>
<td></td>
<td>▪ Down count—Number of consecutive OAM loopback cells an ATM virtual circuit must lose to be identified as unavailable—for example, 200.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ Up count—Number of consecutive OAM loopback cells an ATM virtual interface must receive to be identified as operational—for example, 200.</td>
<td></td>
</tr>
<tr>
<td>▪ OAM period—Interval, in seconds, at which OAM cells are transmitted on ATM virtual circuits—for example, 100. The range is between 1 and 900 seconds.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Configure CBR for the Interface—for example, at-1/0/0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ CBR — Range from 33000 through 1199920</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ CDVT — Range from 1 through 9999</td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> CDVT is not supported on J Series devices.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Configure VBR for the Interface—for example, at-1/0/0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ MBS — Range from 33000 through 1199920</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ CDVT — Range from 1 through 9999</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ PCR — Range from 33000 through 1199920</td>
<td></td>
</tr>
<tr>
<td></td>
<td>▪ SCR — Range from 33000 through 1199920</td>
<td></td>
</tr>
</tbody>
</table>
Table 36: Adding an ATM-over-ADSL Network Interface (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>In the Interface name box, select <strong>at-2/0/0</strong>.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Next to Atm options, click <strong>Configure</strong>.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Next to Vpi, click <strong>Add new entry</strong>.</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>In the Vpi number box, type <strong>25</strong>.</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Click <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>In the Actions box, click <strong>Edit</strong>.</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Next to Oam liveness, click <strong>Configure</strong>.</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>In the Down count box, type <strong>200</strong>.</td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>In the Up count box, type <strong>200</strong>.</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>Click <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td>Next to Oam period, click <strong>Configure</strong>.</td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>From the Oam period choices list, select <strong>Oam period</strong>.</td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td>In the Oam period box, type <strong>100</strong>.</td>
<td></td>
</tr>
<tr>
<td>14.</td>
<td>Click <strong>OK</strong> until you return to the Interface page.</td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>Next to Shaping, click <strong>Configure</strong>.</td>
<td></td>
</tr>
<tr>
<td>16.</td>
<td>In the Queue length box, type <strong>200</strong>.</td>
<td></td>
</tr>
<tr>
<td>17.</td>
<td>From the Useless Shaping Choice list, select <strong>Cbr</strong>.</td>
<td></td>
</tr>
<tr>
<td>18.</td>
<td>In the Cbr value box, type <strong>33000</strong>.</td>
<td></td>
</tr>
<tr>
<td>19.</td>
<td>In the Cdvt box, type <strong>200</strong>, Click <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td>20.</td>
<td>From the Useless Shaping Choice list, select <strong>Vbr</strong>.</td>
<td></td>
</tr>
<tr>
<td>21.</td>
<td>In the Burst box, type <strong>33000</strong>.</td>
<td></td>
</tr>
<tr>
<td>22.</td>
<td>In the Cdvt box, type <strong>200</strong>.</td>
<td></td>
</tr>
<tr>
<td>23.</td>
<td>In the Peak box, type <strong>142</strong>.</td>
<td></td>
</tr>
</tbody>
</table>
Table 36: Adding an ATM-over-ADSL Network Interface (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter set dsl-options operating-mode auto</td>
</tr>
</tbody>
</table>

Configure the type of DSL operating mode for the ATM-over-ADSL interface—for example auto.

Annex A and Annex B support the following operating modes:

- **auto**—Configures the ADSL interface to autonegotiate settings with the DSLAM located at the central office. For Annex A, the ADSL interface trains in either ANSI T1.413 Issue II mode or ITU G.992.1 mode. For Annex B, the ADSL interface trains in ITU G.992.1 mode.
- **itu-dmt**—Configures the ADSL interface to train in ITU G.992.1 mode.

Annex A supports the following operating modes:

- **adsl2plus**—Configures the ADSL interface to train in ITU G.992.5 mode. You can configure this mode only when it is supported on the DSLAM.
- **itu-dmt-bis**—Configures the ADSL interface to train in ITU G.992.3 mode. You can configure this mode only when it is supported on the DSLAM.
- **ansi-dmt**—Configures the ADSL interface to train in the ANSI T1.413 Issue II mode.

Annex B supports the following operating modes:

- **etsi**—Configures the ADSL line to train in the ETSI TS 101 388 V1.3.1 mode.
- **itu-annexb-ur2**—Configures the ADSL line to train in the G.992.1 Deutsche Telekom UR-2 mode.
- **itu-annexb-non-ur2**—Configures the ADSL line to train in the G.992.1 Non-UR-2 mode.

Configure the encapsulation type—for example, **ethernet-over-atm**.

- **atm-pvc**—ATM permanent virtual circuits is the default encapsulation for ATM-over-ADSL interfaces. For PPP over ATM (PPPoA) over ADSL interfaces, use this type of encapsulation.
- **ethernet-over-atm**—Ethernet over ATM encapsulation. For PPP over Ethernet (PPPoE) over ATM-over-ADSL interfaces that carry IPv4 traffic, use this type of encapsulation.

---

24. In the Sustained box, type 33000.
25. Click **OK**.
<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Logical Properties</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Scroll down the page to Unit, and click <strong>Add new entry</strong>.</td>
<td></td>
<td>Enter set unit 3</td>
</tr>
<tr>
<td>2. In the Interface unit number box, type 3.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Enter other values in the fields required by your network.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Add the logical interface. Set a value from 0 and 16385—for example, 3. Add other values if required by your network.

Configure encapsulation for the ATM-for-ADSL logical unit—for example, **atm-nlpid**.

The following encapsulations are supported on the ATM-over-ADSL interfaces that use **inet** (IP) protocols only:

- **atm-vc-mux**—Use ATM virtual circuit multiplex encapsulation.
- **atm-nlpid**—Use ATM network layer protocol identifier (NLPID) encapsulation.
- **atm-cisco-nlpid**—Use Cisco NLPID encapsulation.
- **ether-over-atm-llc**—For interfaces that carry IPv4 traffic, use Ethernet over LLC encapsulation. You cannot configure multipoint interfaces if you use this type of encapsulation.

The following encapsulations are supported on the ATM-over-ADSL for PPP-over-ATM (PPPoA) interfaces only. (For a sample PPPoA configuration, see “Verifying Interface Configuration” on page 113.)

- **atm-ppp-llc**—AAL5 logical link control (LLC) encapsulation.
- **atm-ppp-vc-mux**—Use AAL5 multiplex encapsulation.

Other encapsulation types supported on the ATM-over-ADSL interfaces:

- **ppp-over-ether-over-atm-llc**—Use PPP over Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead you configure the interface address on the PPP interface.
- **atm-snap**—Use ATM subnetwork attachment point (SNAP) encapsulation.
Table 36: Adding an ATM-over-ADSL Network Interface (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Operation, Maintenance, and Administration (OAM) options for ATM virtual circuits.</td>
<td>1. Next to Oam liveness, click <strong>Configure</strong>.</td>
<td>1. To configure OAM liveness values for an ATM virtual circuit, enter</td>
</tr>
<tr>
<td>■ OAM F5 loopback cell thresholds (“liveness”) on ATM virtual circuits. The range is between 1 and 255, and the default is 5 cells.</td>
<td>2. In the Down count box, type 200.</td>
<td>set unit 3 oam-liveness up-count 200 down-count 200</td>
</tr>
<tr>
<td>■ Down count—Number of consecutive OAM loopback cells an ATM virtual circuit must lose to be identified as unavailable—for example, 200.</td>
<td>3. In the Up count box, type 200.</td>
<td>2. To configure the OAM period, enter set unit 3 oam-period 100</td>
</tr>
<tr>
<td>■ Up count—Number of consecutive OAM loopback cells an ATM virtual interface must receive to be identified as operational—for example, 200.</td>
<td>4. Click <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td>■ OAM period—Interval, in seconds, at which OAM cells are transmitted on ATM virtual circuits—for example, 100. The range is between 1 and 900 seconds.</td>
<td>5. Next to Oam period, click <strong>Configure</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. From the Oam period choices list, select <strong>Oam period</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. In the Oam period box, type 100.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td>Add the Family protocol type—for example, inet.</td>
<td>1. In the Inet box, select <strong>Yes</strong> and click <strong>Configure</strong>.</td>
<td>Enter set unit 3 family inet</td>
</tr>
<tr>
<td></td>
<td>2. Enter the values in the fields required by your network.</td>
<td>Commands vary depending on the protocol type.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td>Configure ATM virtual channel identifier (VCI) options for the interface.</td>
<td>1. From the Vci Type list, select <strong>vci</strong>.</td>
<td>1. To configure the VCI value, enter</td>
</tr>
<tr>
<td>■ ATM VCI type—vci.</td>
<td>2. In the Vci box, type 35.</td>
<td>set unit 3 vci 35</td>
</tr>
<tr>
<td>■ ATM VCI value—A number between 0 and 4089—for example, 35—with VCIs 0 through 31 reserved.</td>
<td>3. Click <strong>OK</strong> until you return to the Interfaces page.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring ATM-over-SHDSL Interfaces

J Series devices with G.SHDSL interfaces can use an Asynchronous Transfer Mode (ATM) interface to send network traffic through a point-to-point connection to a DSL access multiplexer (DSLAM).

**NOTE:** You can configure J Series devices with a G.SHDSL interface for connections through SHDSL only, not for direct ATM connections.
J Series devices with a 2-port G.SHDSL interface installed support the following modes. You can configure only one mode on each interface.

- 2-port two-wire mode (Annex A or Annex B)—Supports autodetection of the line rate or fixed line rates and provides network speeds from 192 Kbps to 2.3 Mbps in 64-Kbps increments. Two-wire mode provides two separate, slower SHDSL interfaces.

- 1-port four-wire mode (Annex A or Annex B)—Supports fixed line rates only and provides network speeds from 384 Kbps to 4.6 Mbps in 128-Kbps increments, doubling the bandwidth. Four-wire mode provides a single, faster SHDSL interface.

To configure Point-to-Point Protocol (PPP), see the Junos Network Interfaces Configuration Guide.

You configure the underlying G.SHDSL interface as an ATM interface, with an interface name of at<pim/>0/<port>. (See “Network Interface Naming” on page 9.) Multiple encapsulation types are supported on both the physical and logical ATM-over-SHDSL interface.

This section contains the following topics:

- Configuring an ATM-over-SHDSL Interface with Quick Configuration on page 146
- Adding an ATM-over-SHDSL Interface with a Configuration Editor on page 150

Configuring an ATM-over-SHDSL Interface with Quick Configuration

The ATM-over-SHDSL Quick Configuration pages allow you to configure ATM-over-SHDSL interfaces and SHDSL options.

To configure an ATM-over-SHDSL interface with Quick Configuration:

1. In the J-Web interface, select Configure > Interfaces.
   A list of the network interfaces installed on the device is displayed. (See “Network Interface Naming” on page 9.)

2. Select an at<pim/>0/<port> interface from the list.
   The ATM-over-SHDSL Interface Quick Configuration page is displayed, as shown in Figure 25 on page 147.
3. Enter information into the ATM-over-SHDSL Quick Configuration page, as described in Table 37 on page 147.

4. From the ATM-over-SHDSL Quick Configuration main page, click one of the following buttons:
   - To apply the configuration and stay in the ATM-over-SHDSL interface Quick Configuration main page, click **Apply**.
   - To apply the configuration and return to the Interfaces Quick Configuration page, click **OK**.
   - To cancel your entries and return to the Interfaces Quick Configuration page, click **Cancel**.

5. To verify the ATM-over-SHDSL interface properties, see “Verifying DSL Interface Configuration” on page 156.

Table 37: ATM-over-SHDSL Interface Quick Configuration Pages Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Logical Interfaces</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 37: ATM-over-SHDSL Interface Quick Configuration Pages Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Interface Name</td>
<td>Lists the logical interfaces for the ATM-over-SHDSL physical interface.</td>
<td>If you have not added an ATM interface, click Add and enter the information required in the Interfaces Quick Configuration fields. If you have already configured a logical interface, select the interface name from the Logical Interface Name list. To delete a logical interface, select the interface and click Delete.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Adding or Editing a Logical Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add logical interfaces</td>
<td>Defines one or more logical units that you connect to this physical ADSL interface. Type a text description of the logical interface to clearly identify it in monitoring displays. From the list, select one of the following types of encapsulations.</td>
<td>Click Add.</td>
</tr>
<tr>
<td>Logical Interface Description</td>
<td>(Optional) Describes the logical interface.</td>
<td></td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Specifies the type of encapsulation on the SHDSL logical interface.</td>
<td></td>
</tr>
</tbody>
</table>

For ATM-over-SHDSL interfaces that use inet (IPv4) protocols only, select one of the following:
- **Cisco-compatible ATM NLPID**—Use Cisco NLPID encapsulation.
- **ATM NLPID**—Use ATM network layer protocol identifier (NLPID) encapsulation.
- **ATM PPP over AA5/LLC**—Use AAL5 logical link control (LLC) encapsulation.
- **ATM PPP over raw AAL5**—Use AAL5 multiplex encapsulation.
- **ATM LLC/SNAP**—For interfaces that carry IPv4 traffic, use ATM over logical link control (LLC) encapsulation. You cannot configure multipoint interfaces if you use this type of encapsulation.
- **ATM VC multiplexing**—Use ATM virtual circuit multiplex encapsulation.

For other encapsulation types on the ATM-over-SHDSL interfaces, select one of the following:
- **Ethernet over ATM (LLC/SNAP)**—Use ATM subnetwork attachment point (SNAP) encapsulation.
- **PPPoE over ATM (LLC/SNAP)**—Use PPP over Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead you configure the interface address on the PPP interface.
### Table 37: ATM-over-SHDSL Interface Quick Configuration Pages Summary *(continued)*

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCI</td>
<td>Configures the ATM virtual circuit identifier (VCI) for the interface.</td>
<td>In the VCI box, type the number for the VCI.</td>
</tr>
<tr>
<td>Add IPv4 address prefixes and</td>
<td>Specifies one or more IPv4 addresses and destination addresses.</td>
<td>Click Add.</td>
</tr>
<tr>
<td>destinations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv4 Address Prefix</td>
<td>Specifies an IPv4 address for the interface.</td>
<td>Type an IPv4 address and prefix. For example: 10.10.10.10/24</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Specifies the destination address.</td>
<td>1. Type an IPv4 address for the destination. 2. Click OK</td>
</tr>
</tbody>
</table>

#### Configuring Physical Properties

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Interface Description</td>
<td>Describes the physical interface description information. (Optional)</td>
<td>Type a description of the interface.</td>
</tr>
<tr>
<td>MTU (bytes)</td>
<td>Specifies the maximum transmission unit (MTU) size, in bytes, of a packet on the ATM-over-SHDSL interface.</td>
<td>Type a value for the byte size—for example, 1500.</td>
</tr>
</tbody>
</table>
| Encapsulation                      | Selects the type of encapsulation for traffic on the physical interface. | Select one of the following types of encapsulation:  
  - **ATM permanent virtual circuits**—Use this type of encapsulation for PPP over ATM (PPPoA) over SHDSL interfaces. This is the default encapsulation for ATM-over-SHDSL interfaces.  
  - **Ethernet over ATM encapsulation**—Use this type of encapsulation for PPP over Ethernet (PPPoE) over ATM-over-SHDSL interfaces that carry IPv4 traffic. |
| VPI                                | Configures the ATM virtual path identifier (VPI) for the interface.      | In the VPI field, type a number between 0 and 255—for example, 25. |

#### Configuring SHDSL Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
</table>
| PIC Mode                           | Specifies the mode on the ATM-over-SHDSL interface.                      | Select either of the following:  
  - **1-port-atm**—1-port four-wire mode  
  - **2-port-atm**—2-port two-wire mode |
| Annex                              | Specifies the type of annex for the interface.                           | Select one of the following:  
  - **Annex A**—Used in North American network implementations.  
  - **Annex B**—Used in European network implementations. |
| Line Rate                          | Specifies the available line rates, in kilobits per second, to use on an G.SHDSL interface. | Select the appropriate value.  
  For 2-port-atm mode only, you can select **auto**, which automatically selects a line rate. |
Table 37: ATM-over-SHDSL Interface Quick Configuration Pages Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback</td>
<td>Specifies the type of loopback testing for the interface.</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>local</strong>—Used for testing the SHDSL equipment with local network devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>payload</strong>—Used to command the remote configuration to send back the received payload.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>remote</strong>—Used to test SHDSL with a remote network configuration.</td>
</tr>
<tr>
<td>Current SNR Margin</td>
<td>Specifies the signal-to-noise ratio (SNR) margin or disables SNR.</td>
<td>To disable Current SNR Margin, select <strong>Disable</strong>.</td>
</tr>
<tr>
<td>Disable Value</td>
<td></td>
<td>To configure a specific value, type a number from 0 to 10—for example, 5.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The range is 0 dB to 10 dB with a default value of 0.</td>
</tr>
<tr>
<td>SNEXT SNR Margin</td>
<td>Sets a value, from –10 dB to 10 dB, for the self-near-crosstalk (SNEXT) SNR margin, or disables SNEXT.</td>
<td>To disable SNEXT SNR Margin, select <strong>Disable</strong>.</td>
</tr>
<tr>
<td>Disable Value</td>
<td></td>
<td>To configure a specific value, type a number from –10 to 10—for example, 5.</td>
</tr>
</tbody>
</table>

Adding an ATM-over-SHDSL Interface with a Configuration Editor

To configure ATM-over-SHDSL network interfaces for the J Series device with a configuration editor:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 38 on page 151.
3. If you are finished configuring the J Series device, commit the configuration.
4. Go on to one of the following procedures:
   - To enable authentication on the interface, see “Configuring CHAP on DSL Interfaces (Optional)” on page 155.
   - To configure PPP over Ethernet (PPPoE) encapsulation on an Ethernet interface or on an ATM-over-SHDSL interface, see “Configuring Point-to-Point Protocol over Ethernet” on page 289.
5. To check the configuration, see “Verifying DSL Interface Configuration” on page 156.
### Table 38: Adding an ATM-over-SHDSL Network Interface

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Navigate to the **Chassis** level in the configuration hierarchy. | 1. In the J-Web interface, select **Configure > CLI Tools > Point and Click CLI**  
2. Next to Chassis, click **Configure**. | From the [edit] hierarchy level, enter  
set chassis fpc 6 pic 0 shdsl pic-mode 1-port-atm |
| Set the ATM-over-SHDSL mode on the G.SHDSL interface, if required. By default, G.SHDSL interfaces are enabled in two-wire Annex B mode. To configure the four-wire mode on the G.SHDSL interface, follow the tasks in this table. | 1. Next to Fpc, click **Add new entry**.  
2. In the Slot box, type 6.  
3. Next to Pic, click **Add new entry**.  
4. In the Slot box, type 0.  
5. Next to Shdsl, click **Configure**.  
6. From the Pic mode menu, select **1-port-atm**.  
7. Click **OK** until you return to the main Configuration page. | |
| Navigate to the **Interfaces** level in the configuration hierarchy. | On the main Configuration page next to Interfaces, click **Edit** | From the [edit] hierarchy level, enter  
edit interfaces at-2/0/0 |
| Create the new interface—for example, at-2/0/0. | 1. Next to Interface, click **Add new entry**.  
2. In the Interface name box, type at-2/0/0.  
3. Click **OK**. | |

### Configuring Physical Properties
### Table 38: Adding an ATM-over-SHDSL Network Interface (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure ATM virtual path identifier (VPI) options for the interface—for example, at-2/0/0.</td>
<td>1. In the Interface name box, select <strong>at-2/0/0</strong>.</td>
<td>1. To configure the VPI value, enter <code>set atm-options vpi 25</code></td>
</tr>
<tr>
<td>■ ATM VPI—A number between 0 and 255—for example, 25.</td>
<td>2. Next to Atm options, click <strong>Configure</strong>.</td>
<td>2. To configure OAM liveness values on a VPI, enter <code>set atm-options vpi 25 oam-liveness up-count 200 down-count 200</code></td>
</tr>
<tr>
<td>■ Operation, Maintenance, and Administration (OAM) F5 loopback cell thresholds (“liveness”) on ATM virtual circuits. The range is between 1 and 255, and the default is 5 cells.</td>
<td>3. Next to Vpi, click <strong>Add new entry</strong>.</td>
<td>3. To configure the OAM period, enter <code>set atm-options vpi 25 oam-period 100</code></td>
</tr>
<tr>
<td>■ Down count—Number of consecutive OAM loopback cells an ATM virtual circuit must lose to be identified as unavailable—for example, 200.</td>
<td>4. In the Vpi number box, type 25.</td>
<td></td>
</tr>
<tr>
<td>■ Up count—Number of consecutive OAM loopback cells an ATM virtual interface must receive to be identified as operational—for example, 200.</td>
<td>5. Click <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td>■ OAM period—Interval, in seconds, at which OAM cells are transmitted on ATM virtual circuits—for example, 100. The range is between 1 and 900 seconds.</td>
<td>6. In the Actions box, click <strong>Edit</strong>.</td>
<td></td>
</tr>
<tr>
<td>■ Next to Oam liveness, click <strong>Configure</strong>.</td>
<td>7. Next to Oam liveness, click <strong>Configure</strong>.</td>
<td></td>
</tr>
<tr>
<td>■ In the Up count box, type 200.</td>
<td>8. In the Down count box, type 200.</td>
<td></td>
</tr>
<tr>
<td>■ In the Up count box, type 200.</td>
<td>9. Click <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td>■ Click <strong>OK</strong>.</td>
<td>10. Click <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td>■ Next to Oam period, click <strong>Configure</strong>.</td>
<td>11. Next to Oam period, click <strong>Configure</strong>.</td>
<td></td>
</tr>
<tr>
<td>■ From the Oam period choices list, select <strong>Oam period</strong>.</td>
<td>12. From the Oam period choices list, select <strong>Oam period</strong>.</td>
<td></td>
</tr>
<tr>
<td>■ In the Oam period box, type 100.</td>
<td>13. In the Oam period box, type 100.</td>
<td></td>
</tr>
<tr>
<td>■ Click <strong>OK</strong> until you return to the Interface page.</td>
<td>14. Click <strong>OK</strong> until you return to the Interface page.</td>
<td></td>
</tr>
</tbody>
</table>

Configure the encapsulation type—for example, ethernet-over-atm. | From the Encapsulation list, select **ethernet-over-atm**. | Enter `set encapsulation ethernet-over-atm` |
| ■ atm-pvc—ATM permanent virtual circuits is the default encapsulation for ATM-over-SHDSL interfaces. For PPP over ATM (PPPoA) over SHDSL interfaces, use this type of encapsulation. |  | |
| ■ ethernet-over-atm—Ethernet over ATM encapsulation. For PPP over Ethernet (PPPoE) over ATM-over-SHDSL interfaces that carry IPv4 traffic, use this type of encapsulation. |  | |

Set the annex type. |  | Enter `set shdsl-options annex annex-a` |
| ■ Annex A—Used in North American network implementations. | 1. Next to Shdsl options, click **Configure**. | |
| ■ Annex B—Used in European network implementations. | 2. From the Annex list, select **Annex-a**. | |
Table 38: Adding an ATM-over-SHDSL Network Interface (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the SHDSL line rate for the ATM-over-SHDSL interface—for example, automatic selection of the line rate.</td>
<td>From the Line Rate list, select auto.</td>
<td>Enter set shdsl-options line-rate auto</td>
</tr>
<tr>
<td>The following values are available:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ auto—Automatically selects a line rate. This option is available only in two-wire mode and is the default value.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ 192 Kbps or higher—Speed of transmission of data on the SHDSL connection.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>In the four-wire mode, the default line rate is 4608 Kbps.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the loopback option for testing the SHDSL connection integrity—for example, local loopback.</td>
<td>From the Loopback list, select local.</td>
<td>Enter set shdsl-options loopback local</td>
</tr>
<tr>
<td>The following values are available:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ local—Used for testing the SHDSL equipment with local network devices.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ payload—Used to command the remote configuration to send back the received payload.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ remote—Used to test SHDSL with a remote network configuration.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the signal-to-noise ratio (SNR) margin—for example, 5 dB for either or both of the following thresholds:</td>
<td>1. Next to Snr margin, select Yes, then click Configure. 2. From the Current list, select Enter Specific Value. 3. In the Value box, type 5. 4. From the Snext list, select Enter Specific Value. 5. In the Value box, type 5. 6. Click OK until you return to the Interface page.</td>
<td>1. Enter set shdsl-options snr-margin current 5 2. Enter set shdsl-options snr-margin snext 5</td>
</tr>
<tr>
<td>■ current—Line trains at higher than current noise margin plus SNR threshold. The range is 0 to 10 dB. The default value is 0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ snext—Line trains at higher than self-near-end crosstalk (SNEXT) threshold. The default value is disabled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setting the SNR creates a more stable SHDSL connection by making the line train at a SNR margin higher than the threshold. If any external noise below the threshold is applied to the line, the line remains stable. You can also disable the SNR margin thresholds.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Configuring Logical Properties**

Add the logical interface.

Set a value from 0 and 16385—for example, 3.

Add other values if required by your network.

1. Scroll down the page to Unit, and click Add new entry.
2. In the Interface unit number box, type 3.
3. Enter other values in the fields required by your network.
Table 38: Adding an ATM-over-SHDSL Network Interface (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure encapsulation for the ATM-for-SHDSL logical unit—for example, atm-nlpid.</td>
<td>From the Encapsulation list, select atm-nlpid.</td>
<td>Enter set unit 3 encapsulation atm-nlpid</td>
</tr>
</tbody>
</table>

The following encapsulations are supported on the ATM-over-SHDSL interfaces that use inet (IP) protocols only:

- atm-vc-mux—Use ATM virtual circuit multiplex encapsulation.
- atm-nlpid—Use ATM network layer protocol identifier (NLPID) encapsulation.
- atm-cisco-nlpid—Use Cisco NLPID encapsulation.
- ether-over-atm-llc—For interfaces that carry IPv4 traffic, use Ethernet over LLC encapsulation. You cannot configure multipoint interfaces if you use this type of encapsulation.

The following encapsulations are supported on the ATM-over-SHDSL for PPP-over-ATM (PPPoA) interfaces only. (For a sample PPPoA configuration, see “Verifying Interface Configuration” on page 113.)

- atm-ppp-llc—AAL5 logical link control (LLC) encapsulation.
- atm-ppp-vc-mux—Use AAL5 multiplex encapsulation.

Other encapsulation types supported on the ATM-over-SHDSL interfaces:

- ppp-over-ether-over-atm-llc—Use PPP over Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead you configure the interface address on the PPP interface.
- atm-snap—Use ATM subnetwork attachment point (SNAP) encapsulation.

Configure Operation, Maintenance, and Administration (OAM) options for ATM virtual circuits:

- OAM F5 loopback cell thresholds (“liveness”) on ATM virtual circuits. The range is between 1 and 255, and the default is 5 cells.
  1. Down count—Number of consecutive OAM loopback cells an ATM virtual circuit must lose to be identified as unavailable—for example, 200.
  2. Up count—Number of consecutive OAM loopback cells an ATM virtual interface must receive to be identified as operational—for example, 200.
- OAM period—Interval, in seconds, at which OAM cells are transmitted on ATM virtual circuits—for example, 100. The range is between 1 and 900 seconds.
Table 38: Adding an ATM-over-SHDSL Network Interface (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add the Family protocol type—for example, inet.</td>
<td>1. In the Inet box, select Yes and click Configure.</td>
<td>Enter set unit 3 family inet</td>
</tr>
<tr>
<td></td>
<td>2. Enter the values in the fields required by your network.</td>
<td>Commands vary depending on the protocol type.</td>
</tr>
<tr>
<td></td>
<td>3. Click OK.</td>
<td></td>
</tr>
<tr>
<td>Configure ATM virtual channel identifier (VCI) options for the interface.</td>
<td>1. From the Vci type list, select vci.</td>
<td>1. To configure the VCI value, enter set unit 3 vci 35</td>
</tr>
<tr>
<td>■ ATM VCl type—vci.</td>
<td>2. In the Vci box, type 35.</td>
<td></td>
</tr>
<tr>
<td>■ ATM VCI value—A number between 0 and 4089—for example, 35—with VCl 0 through 31 reserved.</td>
<td>3. Click OK until you return to the Interfaces page.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring CHAP on DSL Interfaces (Optional)

For interfaces with PPPoA encapsulation, you can optionally configure interfaces to support the PPP Challenge Handshake Authentication Protocol (CHAP). When you enable CHAP on an interface, the interface can authenticate its peer and be authenticated by its peer.

If you set the passive option to handle incoming CHAP packets only, the interface does not challenge its peer. However, if the interface is challenged, it responds to the challenge. If you do not set the passive option, the interface always challenges its peer.

For more information about CHAP, see the Junos Network Interfaces Configuration Guide.

To configure CHAP on the ATM-over-ADSL or ATM-over-SHDSL interface:
1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 39 on page 156.
3. If you are finished configuring the J Series device, commit the configuration.
4. To check the configuration, see “Verifying DSL Interface Configuration” on page 156.
Table 39: Configuring CHAP

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Access level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit access</td>
</tr>
<tr>
<td></td>
<td>2. Next to Access, click Configure or Edit.</td>
<td></td>
</tr>
<tr>
<td>Define a CHAP access profile—for example, A-ppp-client—with a client</td>
<td>1. Next to Profile, click Add new entry.</td>
<td>Enter</td>
</tr>
<tr>
<td>named client 1 and the secret (password) my-secret.</td>
<td>2. In the Profile name box, type A-ppp-client.</td>
<td>set profile A-ppp-client client1</td>
</tr>
<tr>
<td></td>
<td>3. Next to Client, click Add new entry.</td>
<td>chap-secret my-secret</td>
</tr>
<tr>
<td></td>
<td>4. In the Name box, type client1.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. In the Chap secret box, type my-secret.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Click OK until you return to the main Configuration page.</td>
<td></td>
</tr>
<tr>
<td>Navigate to the appropriate ATM interface level in the configuration</td>
<td>1. On the main Configuration page next to Interfaces, click Configure or Edit.</td>
<td>From the [edit] hierarchy level, enter</td>
</tr>
<tr>
<td>hierarchy—for example, at-3/0/0 unit 0.</td>
<td>2. In the Interface name box, click at-3/0/0.</td>
<td>edit interfaces at-3/0/0 unit 0</td>
</tr>
<tr>
<td></td>
<td>3. Under Interface unit number box, click 0.</td>
<td></td>
</tr>
<tr>
<td>Configure CHAP on the ATM-over-ADSL or ATM-over-SHDSL interface</td>
<td>1. Next to Ppp options, click Configure.</td>
<td>Enter</td>
</tr>
<tr>
<td>and specify a unique profile name containing a client list and access</td>
<td>2. Next to Chap, click Configure.</td>
<td>set ppp-options chap access-profile A-ppp-client</td>
</tr>
<tr>
<td>parameters—for example, A-ppp-client.</td>
<td>3. In the Access profile box, type A-ppp-client.</td>
<td></td>
</tr>
<tr>
<td>Specify a unique hostname to be used in CHAP challenge and response</td>
<td>In the Local name box, type A-3/0/0.0.</td>
<td>Enter</td>
</tr>
<tr>
<td>packets—for example, A-3/0/0.0.</td>
<td></td>
<td>set ppp-options chap local-name A-3/0/0.0.</td>
</tr>
<tr>
<td>Set the passive option to handle incoming CHAP packets only.</td>
<td>1. In the Passive box, click Yes.</td>
<td>Enter</td>
</tr>
<tr>
<td></td>
<td>2. Click OK.</td>
<td>set ppp-options chap passive</td>
</tr>
</tbody>
</table>

Verifying DSL Interface Configuration

To verify ATM-over-ADSL or ATM-over-SHDSL, perform these tasks:

- Verifying ADSL Interface Properties on page 157
- Displaying a PPPoA Configuration for an ATM-over-ADSL Interface on page 160
- Verifying an ATM-over-SHDSL Configuration on page 160
Verifying ADSL Interface Properties

**Purpose**  
Verify that the interface properties are correct.

**Action**  
From the CLI, enter the `show interfaces interface-name extensive` command.

**Sample Output**

```plaintext
user@host> show interfaces at-1/0/0 extensive
Physical interface: at-1/0/0, Enabled, Physical link is Up
Interface index: 141, SNMP ifIndex: 49, Generation: 142
Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, ADSL mode,
Speed: ADSL, Loopback: None
Device flags : Present Running
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:05:85:c3:17:f4
Last flapped : 2008-06-26 23:11:09 PDT (01:41:30 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
Input errors:
Errors: 0, Drops: 0, Invalid VCs: 0, Framing errors: 0, Policed discards: 0,
L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
Resource errors: 0
Output errors:
Carrier transitions: 3, Errors: 0, Drops: 0, Aged packets: 0, MTU errors: 0,
Resource errors: 0
ADSL alarms : None
ADSL defects : None
ADSL media:     Seconds Count State
LOF            1      1 OK
LOS            1      1 OK
LOM            0      0 OK
LOP            0      0 OK
LOCDI          0      0 OK
LOCDNI         0      0 OK
ADSL status:
Modem status : Showtime (Adsl2plus)
DSL mode : Auto Annex A
Last fail code: None
Subfunction : 0x00
Seconds in showtime: 6093
ADSL Chipset Information:  ATU-R  ATU-C
Vendor Country : 0x0F  0xb5
Vendor ID : STMI IFTN
Vendor Specific: 0x0000 0x70de
ADSL Statistics:
Attenuation (dB) : 0.0 0.0
Capacity used(%) : 100 92
Noise margin(dB) : 7.5 9.0
Output power (dBm) : 10.0 12.5

Interleave Fast Interleave Fast

Bit rate (kbps) : 0 24465 0 1016
```
CRC               :                    0          0           0         0
FEC               :                    0          0           0         0
HEC               :                    0          0           0         0
Received cells    :                    0         49
Transmitted cells :                    0          0

ATM status:
  HCS state:     Hunt
  LOC      :       OK

ATM Statistics:
  Uncorrectable HCS errors: 0, Correctable HCS errors: 0,
  Tx cell FIFO overruns: 0,
  Rx cell FIFO overruns: 0,
  Rx cell FIFO underruns: 0,
  Input cell count: 49, Output cell count: 0,
  Output idle cell count: 0,
  Output VC queue drops: 0,
  Input no buffers: 0,
  Input length errors: 0,
  Input timeouts: 0,
  Input invalid VCs: 0,
  Input bad CRCs: 0,
  Input OAM cell no buffers: 0

Packet Forwarding Engine configuration:
  Destination slot: 1
  Direction : Output

<table>
<thead>
<tr>
<th>Cos transmit queue</th>
<th>Bandwidth</th>
<th>Buffer</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>7600000</td>
<td>95</td>
</tr>
<tr>
<td>3 network-control</td>
<td>5</td>
<td>400000</td>
<td>5</td>
</tr>
</tbody>
</table>

But for ADSL MiniPim TI chipset does not send ADSL Chipset Information. Also Adsl minipim does not send any alarms. So we can’t show alarm stats for minipim. So following information will not be displayed in Minipim case.

ADSL alarms   : None
ADSL defects  : None

ADSL media:

<table>
<thead>
<tr>
<th></th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOF</td>
<td>1</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>LOS</td>
<td>1</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>LOM</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>LOP</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>LOCDI</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>LOCDNI</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
</tbody>
</table>

ADSL Chipset Information:

<table>
<thead>
<tr>
<th>ATU-R</th>
<th>ATU-C</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0f</td>
<td>0xb5</td>
</tr>
</tbody>
</table>

Vendor Country : STMI IFTN
Vendor ID      : 0x0000 0x70de
Vendor Specific: 0x0000 0x70de

Meaning

The output shows a summary of interface information. Verify the following information:

- The physical interface is Enabled. If the interface is shown as Disabled, do either of the following:
  - In the CLI configuration editor, delete the disable statement at the [edit interfaces interface-name] level of the configuration hierarchy.
In the J-Web configuration editor, clear the Disable check box on the Interfaces > interface-name page.

The physical link is Up. A link state of Down indicates a problem with the interface module, interface port, or physical connection (link-layer errors).

The Last Flapped time is an expected value. The Last Flapped time indicates the last time the physical interface became unavailable and then available again. Unexpected flapping indicates likely link-layer errors.

The traffic statistics reflect expected input and output rates. Verify that the number of inbound and outbound bytes and packets matches expected throughput for the physical interface. To clear the statistics and see only new changes, use the clear interfaces statistics interface-name command.

No ADSL alarms and defects appear that can render the interface unable to pass packets. When a defect persists for a certain amount of time, it is promoted to an alarm. The following are ADSL-specific alarms:

- **LOCDI**—Loss of cell delineation for interleaved channel
- **LOCDNI**—Loss of cell delineation for non-interleaved channel
- **LOF**—Loss of frame
- **LOM**—Loss of multiframe
- **LOP**—Loss of power
- **LOS**—Loss of signal
- **FAR_LOF**—Loss of frame in ADSL transceiver unit-central office (ATU-C)
- **FAR_LOS**—Loss of signal in ATU-C
- **FAR_LOCDI**—Loss of cell delineation for interleaved channel in ATU-C
- **FAR_LOCDNI**—Loss of cell delineation for non-interleaved channel in ATU-C

Examine the operational statistics for an ADSL interface. Statistics in the ATU-R (ADSL transceiver unit–remote) column are for the near end. Statistics in the ATU-C (ADSL transceiver unit–central office) column are for the far end.

- **Attenuation (dB)**—Reduction in signal strength measured in decibels.
- **Capacity used (%)**—Amount of ADSL usage in %.
- **Noise Margin (dB)**—Maximum extraneous signal allowed without causing the output to deviate from an acceptable level.
- **Output Power (dBm)**—Amount of power used by the ADSL interface.
- **Bit Rate (kbps)**—Data transfer speed on the ADSL interface.

**Related Topics** For a complete description of show interfaces extensive output, see the Junos Interfaces Command Reference.
**Displaying a PPPoA Configuration for an ATM-over-ADSL Interface**

**Purpose** Verify the PPPoA configuration for an ATM-over-ADSL interface.

**Action** From the J-Web interface, select Configure > CLI Tools > CLI Viewer. Alternatively, from configuration mode in the CLI, enter the `show interfaces interface-name` and the `show access` commands from the top level.

```
[edit]
user@host# show interfaces at-1/0/0
at-1/0/0 {
  encapsulation atm-pvc;
  atm-options {
    vpi 0;
  }
  dsl-options {
    operating-mode auto;
  }
  unit 0 {
    encapsulation atm-ppp-llc;
    vci 0.100;
    ppp-options {
      chap {
        access-profile A-ppp-client;
        local-name A-at-1/0/0.0;
        passive;
      }
    }
    family inet {
      negotiate address;
    }
  }
}
user@host# show access
profile A-ppp-client {
  client A-ppp-server chap-secret "$9$G4ikPuO1SyKP5clKv7Nik.PT3"; ## SECRET-DATA
}
```

**Meaning** Verify that the output shows the intended configuration of PPPoA.

**Related Topics** For more information about the format of a configuration file, see the J-Web Interface User Guide or the Junos CLI User Guide.

**Verifying an ATM-over-SHDSL Configuration**

**Purpose** Verify that the interface properties are correct.

**Action** From the CLI, enter the `show interfaces interface-name extensive` command.
### Sample Output

```bash
user@host> show interfaces at-6/0/0 extensive
```

Physical interface: at-6/0/0, Enabled, Physical link is Up

Interface index: 141, SNMP ifIndex: 23, Generation: 48

Link-level type: ATM-PVC, MTU: 4482, Clocking: Internal, ADSL mode, Speed: ADSL,

Loopback: None

Device flags : Present Running

Link flags : None

CoS queues : 8 supported

Hold-times : Up 0 ms, Down 0 ms

Current address: 00:05:85:c7:44:3c

Last flapped : 2005-05-16 05:54:41 PDT (00:41:42 ago)

Statistics last cleared: Never

Traffic statistics:

- Input bytes: 4520, 0 bps
- Output bytes: 39250, 0 bps
- Input packets: 71, 0 pps
- Output packets: 1309, 0 pps

Input errors:

- Errors: 0, Drops: 0, Invalid VCs: 0, Framing errors: 0, Policed discards: 0,
- L3 incompletes: 0, L2 channel errors: 1, L2 mismatch timeouts: 0, Resource errors: 0

Output errors:

- Carrier transitions: 3, Errors: 0, Drops: 0, Aged packets: 0, MTU errors: 0,
- Resource errors: 0

Queue counters:

<table>
<thead>
<tr>
<th>Queue counters</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>4</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>2340</td>
<td>2340</td>
<td>0</td>
</tr>
</tbody>
</table>

SHDSL alarms : None

SHDSL defects : None

SHDSL media:

- LOSD: 239206, 2 OK
- LOSW: 239208, 1 OK
- ES: 3, 1 OK
- SES: 0, 0 OK
- UAS: 3, 1 OK

SHDSL status:

- Line termination : STU-R
- Annex : Annex B
- Line Mode : 2-wire
- Modem Status : Data
- Last fail code : 0
- Framer mode : ATM
- Dying Gasp : Enabled

SHDSL Statistics:

- Transmit power (dB) : 8.5
- Receiver gain (dB) : 21.420
- SNR sampling (dB) : 39.3690

Verifying an ATM-over-SHDSL Configuration
Bit rate (kbps) : 2304
Bit error rate : 0
CRC errors : 0
SEGA errors : 1
LOSW errors : 0
Received cells : 1155429
Transmitted cells : 1891375
HEC errors : 0
Cell drop : 0

Meaning  The output shows a summary of interface information. Verify the following information:

- The physical interface is Enabled. If the interface is shown as Disabled, do either of the following:
  - In the CLI configuration editor, delete the disable statement at the [edit interfaces interface-name] level of the configuration hierarchy.
  - In the J-Web configuration editor, clear the Disable check box on the Interfaces > interface-name page.

- The physical link is Up. A link state of Down indicates a problem with the interface module, interface port, or physical connection (link-layer errors).

- The Last Flapped time is an expected value. The Last Flapped time indicates the last time the physical interface became unavailable and then available again. Unexpected flapping indicates likely link-layer errors.

- The traffic statistics reflect expected input and output rates. Verify that the number of inbound and outbound bytes and packets matches expected throughput for the physical interface. To clear the statistics and see only new changes, use the clear interfaces statistics interface-name command.

- No SHDSL alarms and defects appear that can render the interface unable to pass packets. When a defect persists for a certain amount of time, it is promoted to an alarm.
  - LOS—Loss of signal. No signal was detected on the line.
  - LOSW—Loss of sync word. A message ID was sent.
  - Power status—A power failure has occurred.
  - LOSD—Loss of signal was detected at the remote application interface.
  - ES—Errored seconds. One or more cyclic redundancy check (CRC) anomalies were detected.
  - SES—Severely errored seconds. At least 50 CRC anomalies were detected.
  - UAS—Unavailable seconds. An interval has occurred during which one or more LOSW defects were detected.
Examine the SHDSL interface status:

- **Line termination**—SHDSL transceiver unit–remote (STU–R). (Only customer premises equipment is supported.)
- **Annex**—Either Annex A or Annex B. Annex A is supported in North America, and Annex B is supported in Europe.
- **Line Mode**—SHDSL mode configured on the G.SHDSL interface pair, either 2-wire or 4-wire.
- **Modem Status**—Data. Sending or receiving data.
- **Last fail code**—Code for the last interface failure.
- **Framer mode**—Framer mode of the underlying interface: ATM.
- **Dying Gasp**—Ability of a J Series device that has lost power to send a message informing the attached DSL access multiplexer (DSLAM) that it is about to go offline.
- **Chipset version**—Version number of the chipset on the interface
- **Firmware version**—Version number of the firmware on the interface.

Examine the operational statistics for a SHDSL interface.

- **Loop Attenuation (dB)**—Reduction in signal strength measured in decibels.
- **Transmit power (dB)**—Amount of SHDSL usage in %.
- **Receiver gain (dB)**—Maximum extraneous signal allowed without causing the output to deviate from an acceptable level.
- **SNR sampling (dB)**—Signal-to-noise ratio at a receiver point, in decibels.
- **Bit Rate (kbps)**—Data transfer speed on the SHDSL interface.
- **CRC errors**—Number of cyclic redundancy check errors.
- **SEGA errors**—Number of segment anomaly errors. A regenerator operating on a segment received corrupted data.
- **LOSW errors**—Number of loss of signal defect errors. Three or more consecutively received frames contained one or more errors in the framing bits.
- **Received cells**—Number of cells received through the interface.
- **Transmitted cells**—Number of cells sent through the interface.
- **HEC errors**—Number of header error checksum errors.
- **Cell drop**—Number of dropped cells on the interface.

**Related Topics** For a complete description of show interfaces extensive output, see the Junos Interfaces Command Reference.
Configuring MLPPP over ADSL Interfaces

J Series and SRX Series devices with an ADSL interface support link fragmentation and interleaving (LFI) through a Multilink Point-to-Point Protocol (MLPPP).

**NOTE:** Currently, JUNOS Software supports bundling of only one xDSL link under bundle interface.

To configure MLPPP, see the Junos Network Interfaces Configuration Guide.

To support MLPPP encapsulation and the family mlppp on the ADSL interface on a J Series or SRX Series device, an existing JUNOS CLI is enabled. To configure MLPPP encapsulation and the family mlppp, use the following commands:

```
set interfaces at-5/0/0 unit 0 encapsulation atm-mlppp-llc
set interfaces at-5/0/0 unit 0 family mlppp bundle lsq-0/0/0.1
```

**Figure 26: MLPPP over ADSL Interface**

To establish an ADSL link between network devices, you must use some intermediate connections. First, use an RJ-11 cable to connect the customer premises equipment (CPE) (for example, a J Series or SRX Series device) to a DSLAM patch panel to form an ADSL link. Then use OC3 or DS3 to connect the DSLAM to M Series or E Series devices to form an ATM backbone. Figure 26 on page 164 shows a typical example of MLPPP over ADSL end-to-end connectivity.
Chapter 5

Configuring G.SHDSL Interfaces

For information about which devices support the features documented in this chapter, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.

This chapter includes the following topics:

- Before You Begin on page 165
- Configuring the G.SHDSL Interface with the CLI Configuration Editor on page 165
- Verifying G.SHDSL Interface Properties on page 168
- Configuring the G.SHDSL Interface on SRX Series Devices on page 176

Before You Begin

Before you begin configuring G.SHDSL interfaces on SRX Series devices, complete the following tasks:

- Establish basic connectivity. See the Getting Started Guide for your device.
- If you do not already have a basic understanding of physical and logical interfaces and Juniper Networks interface conventions, read “Interfaces Overview” on page 3.
- Configure network interfaces as necessary. See “Configuring Ethernet, DS1, DS3, and Serial Interfaces” on page 81.

Configuring the G.SHDSL Interface with the CLI Configuration Editor

Use the CLI configuration editor to configure the G.SHDSL interface.

**NOTE:** J-Web support for configuring the G.SHDSL Interface is not available.

**NOTE:** The G.SHDSL configuration details mentioned in this topic are applicable to SRX Series devices. For information about configuring G.SHDSL configuration on J Series devices, see “Configuring ATM-over-SHDSL Interfaces” on page 145.

To configure the G.SHDSL interfaces for SRX210 and SRX240 devices:
1. Navigate to the top of the interfaces configuration hierarchy in the CLI configuration editor.
2. Perform the configuration tasks described in Table 40 on page 166.
3. Commit the configuration after you have completed configuring the device.

Table 40: Configuring the G.SHDSL Interface Using the CLI Configuration Editor

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor Commands</th>
<th>Description</th>
</tr>
</thead>
</table>
| Navigate to the Chassis level in the configuration hierarchy. | From the [edit] hierarchy level, enter set chassis fpc fpc-slot-number pic pic-slot-number shdsl pic-mode wire mode | Specifies the wire mode on the G.SHDSL interface. Select one of the following options:  
  - 1-port-atm — Use this option to configure the 8-wire (1-port, 8-wire) wire mode.  
  - 2-port-atm — Use this option to configure the 4-wire (2-port, 4-wire) wire mode.  
  - 4-port-atm — Use this option to configure the 2-wire (4-port, 2-wire) wire mode.  
  
  **NOTE:** The default wire mode is 4-wire (2-port, 4-wire). |
| Navigate to the Interfaces level in the configuration hierarchy. | From the [edit] hierarchy level, enter edit interfaces interface | Provides a hierarchy level to configure the interface. |
| Set the annex type. | From the [edit] hierarchy level, enter set interfaces interface shdsl-options annex annex-type | Sets the annex type. The following options are available:  
  - Annex A  
  - Annex B  
  - Annex F  
  - Annex G  
  
  **NOTE:** The default annex type is Annex B.
Table 40: Configuring the G.SHDSL Interface Using the CLI Configuration Editor (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor Commands</th>
<th>Description</th>
</tr>
</thead>
</table>
| Configure the line rates. | From the [edit] hierarchy level, enter  
set interfaces interface shdsl-options line-rate line rate value | Configures the SHDSL line rate. Line rate is speed of transmission of data on the SHDSL connection. The following values are available:  
- **auto** — Automatically selects a line rate.  
- **value** — Select the values between 192 kbps and 22784 kbps.  
**NOTE:** The default line rate is Auto. |
| Configure the encapsulation type. | From the [edit] hierarchy level, enter  
set interfaces interface encapsulation encapsulation type | Sets the encapsulation type. The following values are available:  
- **atm-pvc** — ATM permanent virtual circuits is the default encapsulation for ATM-over-SHDSL interfaces. For PPP over ATM (PPPoA) over SHDSL interfaces, use this type of encapsulation. Use this type of encapsulation if you are using ATM DSLAM.  
- **ethernet-over-atm** — Ethernet over ATM encapsulation. For PPP over Ethernet (PPPoE) over ATM-over-SHDSL interfaces that carry IPv4 traffic, use this type of encapsulation. Use this type of encapsulation if you are using IP DSLAM. |

**Configuring Logical Properties**

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor Commands</th>
<th>Description</th>
</tr>
</thead>
</table>
| Add the logical interface. | From the [edit] hierarchy level, enter  
set interfaces interface unit unit value | Defines one or more logical units that you connect to this physical G.SHDSL interface. Set a value from 0 through 7. |

Example:

- set interfaces at-1/0/0 shdsl-options line-rate auto
- set interfaces at-1/0/0 encapsulation ethernet-over-atm
Table 40: Configuring the G.SHDSL Interface Using the CLI Configuration Editor (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor Commands</th>
<th>Description</th>
</tr>
</thead>
</table>
| Configure encapsulation. | From the [edit] hierarchy level, enter set interfaces interface unit unit value encapsulation | Sets the encapsulation type. The following values are available:  
  - `atm-cisco-nlpid` — Use Cisco NLPID encapsulation.  
  - `atm-mlppp-llc` — Use ATM MLPPP over AAL5/LLC encapsulation.  
  - `atm-nlpid` — Use ATM network layer protocol identifier (NLPID) encapsulation.  
  - `atm-ppp-llc` — AAL5 logical link control (LLC) encapsulation.  
  - `atm-ppp-vc-mux` — Use AAL5 multiplex encapsulation.  
  - `atm-vc-mux` — Use ATM virtual circuit multiplex encapsulation.  
  - `atm-snap` — Use ATM subnetwork attachment point (SNAP) encapsulation.  
  - `ether-over-atm-llc` — For interfaces that carry IPv4 traffic, use Ethernet over LLC encapsulation. You cannot configure multipoint interfaces if you use this type of encapsulation.  
  - `ppp-over-ether-over-atm-llc` — Use PPP over Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead you configure the interface address on the PPP interface. |

**NOTE:** For more information on configuring the physical and logical properties for the G.SHDSL interface, see “Configuring ATM-over-SHDSL Interfaces” on page 145.

**Related Topics**  
- Configuring ATM-over-SHDSL Interfaces on page 145  
- Verifying G.SHDSL Interface Properties on page 168

**Verifying G.SHDSL Interface Properties**

**Purpose**  
Verify that the G.SHDSL interface properties are configured properly

**Action**  
From the CLI configuration editor, enter the `show interfaces interface-name extensive` command.
Sample Output  4-wire mode (for interface at-1/0/0)

user@host# run show interfaces at-1/0/0 extensive
Physical interface: at-1/0/0, Enabled, Physical link is Up

Interface index: 146, SNMP ifIndex: 139, Generation: 329
Link-level type: ATM-PVC, MTU: 1496, Clocking: Internal, Speed: SHDSL(4-wire)

Speed: SHDSL(4-wire), Loopback: None
Device flags : Present Running
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:24:dc:01:cf:a0
Last flapped : 2009-09-24 00:19:03 PDT (00:00:54 ago)
Statistics last cleared: 2009-09-24 00:18:24 PDT (00:01:33 ago)
Traffic statistics:
Input bytes : 125 0 bps
Output bytes : 96 0 bps
Input packets: 2 0 pps
Output packets: 1 0 pps
Input errors:

Errors: 0, Drops: 0, Invalid VCs: 0, Framing errors: 0, Policed discards: 0,
L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
Resource errors: 0

Output errors:
Carrier transitions: 1, Errors: 0, Drops: 0, Aged packets: 0, MTU errors: 0,
Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
0 best-effort 1 1 0
1 expedited-fo 0 0 0
2 assured-forw 0 0 0
3 network-cont 0 0 0

SHDSL alarms : None
SHDSL defects : None
SHDSL media: Seconds Count State
LINE1_LOSD 32 0 OK
LINE1_LOSW 37 0 OK
LINE2_LOSD 32 0 OK
LINE2_LOSW 37 0 OK
ES 37
SES 37
UAS 48
SHDSL status:
Line termination : STU-R
Annex : Annex B
Line mode : 4-wire
Modem status : Data
Bit rate (kbps) : 4608
Last fail mode : No failure (0x00)
Framer mode : ATM
Dying gasp : Enabled
Framers sync status : In sync
Chipset version : 00

SHDSL statistics:
Loop attenuation (dB) : 0.0
Transmit power (dBm) : 0.0
Receiver gain (dB) : -inf
SNR sampling (dB) : inf
CRC errors : 0
SEGA errors : 0
LOSW errors : 0
Received cells : 0
Transmitted cells : 0
HEC errors : 0
Cell drop : 0

Packet Forwarding Engine configuration:
Destination slot: 1

CoS information:
Direction : Output
CoS transmit queue
Bandwidth Buffer Priority
Limit % bps % usec
0 best-effort 95 4377600 95 0 low
none
3 network-control 5 230400 5 0 low
none

Logical interface at-1/0/0.0 (Index 76) (SNMP ifIndex 133) (Generation 402)
Flags: Point-To-Multipoint SNMP-Traps OxO Encapsulation: Ether-over-ATM-LLC
Traffic statistics:
Input bytes : 125
Output bytes : 116
Input packets: 2
Output packets: 1
Local statistics:
Input bytes : 125
Output bytes : 116
Input packets: 2
Output packets: 1
Transit statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
Security: Zone: Null
Flow Statistics:
Flow Input statistics:
Self packets : 0
ICMP packets : 0
VPN packets : 0
Multicast packets : 0
Bytes permitted by policy : 0
Connections established : 0
Flow Output statistics:
Multicast packets : 0
Bytes permitted by policy : 0
Flow error statistics (Packets dropped due to):
Address spoofing: 0
Authentication failed: 0
Incoming NAT errors: 0
Invalid zone received packet: 0
Multiple user authentications: 0
Multiple incoming NAT: 0
No parent for a gate: 0
No one interested in self packets: 0

No minor session: 0
No more sessions: 0
No NAT gate: 0
No route present: 0
No SA for incoming SPI: 0
No tunnel found: 0
No session for a gate: 0
No zone or NULL zone binding: 0
Policy denied: 0
Security association not active: 0
TCP sequence number out of window: 0
Syn-attack protection: 0
User authentication errors: 0

Protocol inet, MTU: 1468, Generation: 322, Route table: 0
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
  Destination: 17.1.1/24, Local: 17.1.1.1, Broadcast: 17.1.1.255, Generation: 496

VCI 1.70
  Flags: Active, Multicast
  Total down time: 0 sec, Last down: Never
  ATM per-VC transmit statistics:
    Tail queue packet drops: 0
  Traffic statistics:
    Input bytes : 0
    Output bytes : 0
    Input packets: 0
    Output packets: 0

Logical interface at-1/0/0.32767 (Index 77) (SNMP ifIndex 141) (Generation 403)

  Flags: Point-To-Multipoint No-Multicast SNMP-Traps 0x0 Encapsulation: ATM-VCMUX

  Traffic statistics:
    Input bytes : 0
    Output bytes : 0
    Input packets: 0
    Output packets: 0
  Local statistics:
    Input bytes : 0
    Output bytes : 0
    Input packets: 0
    Output packets: 0
  Security: Zone: Null
  Flow Statistics:
    Flow Input statistics:
    Self packets : 0
    ICMP packets : 0
    VPN packets : 0
    Multicast packets : 0
    Bytes permitted by policy : 0
    Connections established : 0
  Flow Output statistics:
    Multicast packets : 0
    Bytes permitted by policy : 0
Flow error statistics (Packets dropped due to):
Address spoofing: 0
Authentication failed: 0
Incoming NAT errors: 0
Invalid zone received packet: 0
Multiple user authentications: 0
Multiple incoming NAT: 0
No parent for a gate: 0
No one interested in self packets: 0
No minor session: 0
No more sessions: 0
No NAT gate: 0
No route present: 0
No SA for incoming SPI: 0
No tunnel found: 0
No session for a gate: 0
No zone or NULL zone binding: 0
Policy denied: 0
Security association not active: 0
TCP sequence number out of window: 0
Syn-attack protection: 0
User authentication errors: 0
VCI 1.4
Flags: Active
Total down time: 0 sec, Last down: Never
ATM per-VC transmit statistics:
Tail queue packet drops: 0
Traffic statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0

Sample Output 4-wire mode (for interface at-1/0/1)

Physical interface: at-1/0/1, Enabled, Physical link is Up

Interface index: 147, SNMP ifIndex: 140, Generation: 330
Link-level type: Ethernet-over-ATM, MTU: 1496, Clocking: Internal, Speed: SHDSL(4-wire)
Speed: SHDSL(4-wire), Loopback: None
Device flags: Present Running
Link flags: None
CoS queues: 8 supported, 8 maximum usable queues
Hold-times: Up 0 ms, Down 0 ms
Current address: 00:24:dc:01:cf:a1
Last flapped: 2009-09-24 00:19:02 PDT (00:00:58 ago)
Statistics last cleared: 2009-09-24 00:18:24 PDT (00:01:36 ago)
Traffic statistics:
Input bytes: 0 0 bps
Output bytes: 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
Input errors:
Errors: 0, Drops: 0, Invalid VCs: 0, Framing errors: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, Resource errors: 0
Output errors:
- Carrier transitions: 0, Errors: 0, Drops: 0, Aged packets: 0, MTU errors: 0,
- Resource errors: 0

Egress queues: 8 supported, 4 in use

Queue counters:

<table>
<thead>
<tr>
<th>Queue Status</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forward</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-control</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

SHDSL alarms: None
SHDSL defects: None

SHDSL media:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINE1_LOSD</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>LINE1_LOSW</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>LINE2_LOSD</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>LINE2_LOSW</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>ES</td>
<td>36</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SES</td>
<td>36</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UAS</td>
<td>47</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SHDSL status:
- Line termination: STU-R
- Annex: Annex B
- Line mode: 4-wire
- Modem status: Data
- Bit rate (kbps): 4608
- Last fail mode: No failure (0x00)
- Framer mode: ATM
- Dying gasp: Enabled
- Framer sync status: In sync
- Chipset version: 00

SHDSL statistics:
- Loop attenuation (dB): 0.0
- Transmit power (dBm): 0.0
- Receiver gain (dB): -inf
- SNR sampling (dB): inf
- CRC errors: 0
- SEGA errors: 0
- LOSW errors: 0
- Received cells: 0
- Transmitted cells: 0
- HEC errors: 0
- Cell drop: 0

Packet Forwarding Engine configuration:
- Destination slot: 1

CoS information:
- Direction: Output

<table>
<thead>
<tr>
<th>Class of Service (CoS)</th>
<th>Limit</th>
<th>Bandwidth</th>
<th>Buffer Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>95%</td>
<td>4377600</td>
<td>0, low</td>
</tr>
<tr>
<td>3 network-control</td>
<td>5%</td>
<td>230400</td>
<td>0, low</td>
</tr>
</tbody>
</table>

Logical interface at-1/0/1.0 (Index 78) (SNMP ifIndex 145) (Generation 404)
- Flags: Point-To-Multipoint SNMP-Traps 0x0 Encapsulation: Ether-over-ATM-LLC

Traffic statistics:
### Local statistics:
- Input bytes: 0
- Output bytes: 0
- Input packets: 0
- Output packets: 0

### Transit statistics:
- Input bytes: 0 (0 bps)
- Output bytes: 0 (0 bps)
- Input packets: 0 (0 pps)
- Output packets: 0 (0 pps)

### Security:
- Zone: Null

### Flow Statistics:
**Flow Input statistics:**
- Self packets: 0
- ICMP packets: 0
- VPN packets: 0
- Multicast packets: 0
- Bytes permitted by policy: 0

**Flow Output statistics:**
- Multicast packets: 0
- Bytes permitted by policy: 0

**Flow error statistics (Packets dropped due to):**
- Address spoofing: 0
- Authentication failed: 0
- Incoming NAT errors: 0
- Invalid zone received packet: 0
- Multiple user authentications: 0
- Multiple incoming NAT: 0
- No parent for a gate: 0
- No one interested in self packets: 0
- No minor session: 0
- No more sessions: 0
- No NAT gate: 0
- No route present: 0
- No SA for incoming SPI: 0
- No tunnel found: 0
- No session for a gate: 0
- No zone or NULL zone binding: 0
- Policy denied: 0
- Security association not active: 0
- TCP sequence number out of window: 0
- Syn-attack protection: 0
- User authentication errors: 0

### ATM per-VC transmit statistics:
- Tail queue packet drops: 0

### Traffic statistics:
- Input bytes: 0

---

### Protocol inet, MTU: 1468, Generation: 323, Route table: 0
- Addresses, Flags: Is-Preferred Is-Primary
- Destination: 18.1.1/24, Local: 18.1.1.1, Broadcast: 18.1.1.255, Generation: 498

### VCI 1.71
- Flags: Active, Multicast
- Total down time: 0 sec, Last down: Never
- ATM per-VC transmit statistics:
  - Tail queue packet drops: 0
- Traffic statistics:
  - Input bytes: 0
Logical interface at-1/0/1.32767 (Index 79) (SNMP ifIndex 146) (Generation 405)

Flags: Point-To-Multipoint No-Multicast SNMP-Traps 0x0 Encapsulation: ATM-VCMUX

Traffic statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0

Local statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0

Security: Zone: Null

Flow Statistics:

Flow Input statistics:
Self packets: 0
ICMP packets: 0
VPN packets: 0
Multicast packets: 0
Bytes permitted by policy: 0
Connections established: 0

Flow Output statistics:
Multicast packets: 0
Bytes permitted by policy: 0

Flow error statistics (Packets dropped due to):
Address spoofing: 0
Authentication failed: 0
Incoming NAT errors: 0
Invalid zone received packet: 0
Multiple user authentications: 0
Multiple incoming NAT: 0
No parent for a gate: 0
No one interested in self packets: 0
No minor session: 0
No more sessions: 0
No NAT gate: 0
No route present: 0
No SA for incoming SPI: 0
No tunnel found: 0
No session for a gate: 0
No zone or NULL zone binding: 0
Policy denied: 0
Security association not active: 0
TCP sequence number out of window: 0
Syn-attack protection: 0
User authentication errors: 0

VCI 1.4
Flags: Active
Total down time: 0 sec, Last down: Never
ATM per-VC transmit statistics:
Tail queue packet drops: 0
Traffic statistics:
- Input bytes : 0
- Output bytes : 0
- Input packets: 0
- Output packets: 0

**Meaning** The output shows a summary of information about the G.SHDSL interface in this example.

**Related Topics** For a complete description of `show interfaces extensive` output, see the *JUNOS Interfaces Command Reference Guide*.

## Configuring the G.SHDSL Interface on SRX Series Devices

This topic provides information on the minimum steps required to configure a G.SHDSL interface on SRX Series devices. The configuration example uses an SRX210 Services Gateway, the information is also applicable to the SRX240 device.

- Topology Diagrams of the G.SHDSL Mini-PIM on page 176
- Example: Configuring the G.SHDSL Interface on the SRX210 Services Gateway on page 177

### Topology Diagrams of the G.SHDSL Mini-PIM

The following topology diagrams show various G.SHDSL Mini-PIM connections:

Figure 27 on page 176 shows the topology for the G.SHDSL Mini-PIM operating in the 2X4-wire mode.

**Figure 27: G.SHDSL Mini-PIM Operating in the 2X4-Wire Mode**

![Topology diagram](image)

Figure 28 on page 177 shows the topology for the G.SHDSL Mini-PIM operating in the 4X2-wire mode.
Example: Configuring the G.SHDSL Interface on the SRX210 Services Gateway

The following assumptions are made in this example:

- The G.SHDSL Mini-PIM is installed in the first slot of the SRX210 device chassis; therefore the FPC used here is fpc 1.
- The SRX210 device is connected to a DSLAM (IP DSLAM and ATM DSLAM).

The steps to configure the G.SHDSL interface when the device is connected to an IP DSLAM and ATM DSLAM are given separately (see Table 42 on page 178 and Table 43 on page 179).

Table 41 on page 178 provides the basic configuration steps for the G.SHDSL interface on an SRX210 device.
**Table 41: Basic Configuration of the G.SHDSL Interface**

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the operating wire mode (2-wire, 4-wire or 8-wire)</td>
<td>From the [chassis] hierarchy level, enter:</td>
</tr>
<tr>
<td></td>
<td>■ set chassis fpc 1 pic 0 shdsl pic-mode 1-port-atm</td>
</tr>
<tr>
<td></td>
<td>■ set chassis fpc 1 pic 0 shdsl pic-mode 2-port-atm</td>
</tr>
<tr>
<td><strong>NOTE:</strong> When the wire mode is set to 8-wire, one physical interface (IFD) is created. Similarly for 2-wire mode and 4-wire modes, four IFDs and two IFDs are created respectively.</td>
<td>(1x8-wire configuration)</td>
</tr>
<tr>
<td></td>
<td>■ set chassis fpc 1 pic 0 shdsl pic-mode 4-port-atm</td>
</tr>
<tr>
<td></td>
<td>(2x4-wire configuration)</td>
</tr>
<tr>
<td><strong>NOTE:</strong> The 2x4-wire configuration is the default configuration and behavior.</td>
<td>(4x2-wire configuration)</td>
</tr>
<tr>
<td>Configure the line rates.</td>
<td>From the [edit] hierarchy level, enter:</td>
</tr>
<tr>
<td></td>
<td>set interfaces at-1/0/0 shdsl-options line-rate 4096</td>
</tr>
<tr>
<td>Set the annex type.</td>
<td>From the [edit] hierarchy level, enter:</td>
</tr>
<tr>
<td></td>
<td>set interfaces at-1/0/0 shdsl-options annex annex-a</td>
</tr>
</tbody>
</table>

Table 42 on page 178 provides the configuration steps for configuring the G.SHDSL interface on an SRX210 device when it is connected to an IP DSLAM.

**Table 42: G.SHDSL Interface Configuration Steps (IP DSLAM)**

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the type of encapsulation on the G.SHDSL interface.</td>
<td>set interface at-1/0/0 encapsulation ethernet-over-atm</td>
</tr>
<tr>
<td>Configure the ATM virtual path identifier (VPI) options for the interface.</td>
<td>set interface at-1/0/0 atm-options vpi 0</td>
</tr>
<tr>
<td>Specify the type of encapsulation on the G.SHDSL logical interface.</td>
<td>set interface at-1/0/0 unit 0 encapsulation ether-over-atm-llc</td>
</tr>
<tr>
<td>Configure the ATM virtual channel identifier (VCI) options for the logical interface.</td>
<td>set interface at-1/0/0 unit 0 vci 0.60</td>
</tr>
<tr>
<td>Configure the interface address for logical interface.</td>
<td>set interface at-1/0/0 unit 0 family inet address 1.1.1.1/24</td>
</tr>
</tbody>
</table>

Table 43 on page 179 provides the configuration steps for configuring the G.SHDSL interface on an SRX210 device when the device is connected to an ATM DSLAM.
### Table 43: G.SHDSL Interface Configuration Steps (ATM DSLAM)

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the type of encapsulation on the G.SHDSL interface.</td>
<td>set interface at-1/0/0 encapsulation atm-pvc</td>
</tr>
<tr>
<td>Configure the ATM virtual path identifier (VPI) options for the interface.</td>
<td>interface at-1/0/0 atm-options vpi 0</td>
</tr>
<tr>
<td>Specify the type of encapsulation on the G.SHDSL logical interface.</td>
<td>interface at-1/0/0 unit 0 encapsulation atm-snap</td>
</tr>
<tr>
<td>Configure the ATM virtual channel identifier (VCI) options for the logical interface.</td>
<td>set interface at-1/0/0 unit 0 vci 0.65</td>
</tr>
<tr>
<td>Configure the interface address for logical interface.</td>
<td>set interface at-1/0/0 unit 0 family inet address 2.1.1.1/24</td>
</tr>
</tbody>
</table>

Table 44 on page 179 provides the configuration steps for configuring PPPoE over ATM on the G.SHDSL interface on an SRX210 device when it is connected to an IP DSLAM.

### Table 44: Steps for Configuring PPPoE over ATM for the G.SHDSL Interface

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the ATM virtual path identifier (VPI) options for the interface.</td>
<td>interface at-1/0/0 atm-options vpi 0</td>
</tr>
<tr>
<td>Specify the type of encapsulation on the G.SHDSL logical interface.</td>
<td>set interfaces at-1/0/0 unit 0 encapsulation ppp-over-ether-over-atm-llc</td>
</tr>
<tr>
<td>Configure the ATM virtual channel identifier (VCI) options for the logical interface.</td>
<td>set interfaces at-1/0/0 unit 0 vci 0.35</td>
</tr>
<tr>
<td>Configure a PPPoE interface with the PAP access profile.</td>
<td>set interfaces pp0 unit 0 ppp-options pap access-profile pap_prof</td>
</tr>
<tr>
<td>Configure a local-name for the PAP interface.</td>
<td>set interfaces pp0 unit 0 ppp-options pap local-name srx-210</td>
</tr>
<tr>
<td>Configure a local-password for the PAP interface.</td>
<td>set interfaces pp0 unit 0 ppp-options pap local-password &quot;59$0Lw15eN-woJDsr-v12GU69cp1RSre&quot;</td>
</tr>
<tr>
<td>Set the passive option to handle incoming PAP packets only.</td>
<td>set interfaces pp0 unit 0 ppp-options pap passive</td>
</tr>
<tr>
<td>Specify the logical interface as the underlying interface for the PPPoE session.</td>
<td>set interfaces pp0 unit 0 pppoe-options underlying-interface at-1/0/0.0</td>
</tr>
<tr>
<td>Specify the number of seconds (from 1 through 4294967295) to wait before reconnecting after a PPPoE session is terminated.</td>
<td>set interfaces pp0 unit 0 pppoe-options auto-reconnect 120</td>
</tr>
<tr>
<td>Specify the logical interface as the client for the PPPoE interface.</td>
<td>set interfaces pp0 unit 0 pppoe-options client</td>
</tr>
</tbody>
</table>
**Table 44: Steps for Configuring PPPoE over ATM for the G.SHDSL Interface (continued)**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>set interfaces pp0 unit 0 family inet negotiate-address</td>
<td>Obtain an IP address by negotiation with the remote end.</td>
</tr>
</tbody>
</table>

Table 45 on page 180 provides the configuration steps for configuring PPP-over-ATM (PPPoA) on the G.SHDSL interface on an SRX210 device when the device is connected to an IP DSLAM.

**Table 45: Steps for Configuring PPPoA for the G.SHDSL Interface**

<table>
<thead>
<tr>
<th>Commands</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>set interfaces at-1/0/0 encapsulation atm-pvc</td>
<td>Specify the type of encapsulation on the G.SHDSL interface.</td>
</tr>
<tr>
<td>set interfaces at-1/0/0 atm-options vpi 1</td>
<td>Configure the ATM virtual path identifier (VPI) options for the interface.</td>
</tr>
<tr>
<td>set interfaces at-1/0/0 unit 0 encapsulation atm-ppp-llc</td>
<td>Specify the type of encapsulation on the G.SHDSL logical interface.</td>
</tr>
<tr>
<td>(For PPP over ATM adaptation layer 5 (AAL5) logical link control (LLC))</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>set interfaces at-1/0/0 unit 0 encapsulation atm-ppp-vc-mux</td>
<td>(For PPP over ATM AAL5 multiplex)</td>
</tr>
<tr>
<td>set interfaces at-1/0/0 unit 0 vci 1.122</td>
<td>Configure the ATM virtual channel identifier (VCI) options for the logical interface.</td>
</tr>
<tr>
<td>set interfaces at-1/0/0 unit 0 ppp-options chap access-profile juniper</td>
<td>Configure a PPPoA interface with the CHAP access profile.</td>
</tr>
<tr>
<td>set interfaces at-1/0/0 unit 0 ppp-options chap local-name srx-210</td>
<td>Configure a local-name for the CHAP interface.</td>
</tr>
<tr>
<td>set interfaces at-1/0/0 unit 0 family inet negotiate-address</td>
<td>Obtain an IP address by negotiation with the remote end.</td>
</tr>
</tbody>
</table>
Chapter 6  
Configuring DOCSIS Mini-PIM Interfaces

This chapter includes following topics:

- Before You Begin on page 181
- Configuring the DOCSIS Interfaces (CLI procedure) on page 181
- Configuring the DOCSIS Logical Interfaces (J-Web procedure) on page 183
- Configuring the DOCSIS Physical Interfaces (J-Web procedure) on page 184
- Verifying DOCSIS Interfaces Properties on page 184

Before You Begin

Before you begin configuring Data over Cable Service Interface Specifications (DOCSIS) interfaces, complete the following tasks:

- Establish basic connectivity. See the Getting Started Guide for your device.
- If you do not already have a basic understanding of physical and logical interfaces and Juniper Networks interfaces conventions, read “Interfaces Overview” on page 3.
- Configure network interfaces as necessary. See “Configuring Ethernet, DS1, DS3, and Serial Interfaces” on page 81.

Configuring the DOCSIS Interfaces (CLI procedure)

To use the CLI configuration editor to configure the DOCSIS network interface for SRX210 and SRX240 devices:

1. Navigate to the top of the interface configuration hierarchy in the CLI configuration editor.
2. Perform the configuration tasks described in Table 46 on page 182.
3. When you are done, commit the configuration.
4. To check the configuration, see “Verifying DOCSIS Interfaces Properties” on page 184.
Table 46: Configuring the DOCSIS Mini-PIM Interfaces Using the CLI

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Interfaces</strong> level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter &lt;br&gt;edit interfaces cm-1/0/0</td>
<td>Provides a hierarchy level to configure the interface.</td>
</tr>
</tbody>
</table>

### Configuring Physical Properties

Configure the traceoptions.

From the [edit] hierarchy level, enter <br>set interfaces interface-name traceoptions

Example:

```
set interfaces cm-2/0/0 traceoptions
```

Select the flag option

```
set interface interface-name traceoptions flag flag-options
```

Example:

```
set interface cm-2/0/0 traceoptions flag
```

The following options are supported:
- **Flag**—Sets tracing parameters
  - **flag**—Sets tracing parameters

**NOTE:** MTU is limited to 1518 bytes on this interface.

### Configuring Logical Properties

Add the logical interface.

From the [edit] hierarchy level, enter <br>set interfaces interface-name unit unit value

Example:

```
set interfaces cm-2/0/0 unit 0
```

Add the Family protocol type—for example, **inet**.

```
set interfaces interface-name unit unit value family inet
```

Example:

```
set interfaces cm-2/0/0 unit 0 family inet
```

Commands vary depending on the protocol type.
### Table 46: Configuring the DOCSIS Mini-PIM Interfaces Using the CLI (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
<th>Description</th>
</tr>
</thead>
</table>
| Configure the Dynamic Host Configuration Protocol (DHCP) client. | set interfaces cm-2/0/0 unit 0 family inet dhcp | The following option is supported:  
  - client-identifier—The DHCP server identifies a client by a client-identifier value. |

### Configuring the DOCSIS Logical Interfaces (J-Web procedure)

To configure the logical interface of DOCSIS Mini-PIM using J-Web:

1. Select **Interfaces > Configure**.
2. Under Interface, select **cm-4/0/0** and then click **Add > Logical Interface**. A pop-up window appears.
3. From the Zone list, select **None**.
4. To add a family protocol type to the Mini-PIM interfaces, select the following check boxes as applicable:
   - **INET**: Supports IP protocol traffic, including OSPF, BGP, and ICMP.
   - **MPLS**: Supports MPLS.
5. Click **OK**.

To edit the logical interfaces of the DOCSIS Mini-PIM using J-Web:

1. Under Interface, select the logical interface added to the DOCSIS Mini-PIM and then click **Edit**. A pop-up window appears.
2. From the Zone list, select **None**.
3. To add a family protocol type to the Mini-PIM interfaces, select the following check boxes as applicable:
   - **INET**: Supports IP protocol traffic including, Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Internet Control Message Protocol (ICMP).
   - **MPLS**: Supports Multiprotocol Label Switching (MPLS).
4. Click **OK**.

**NOTE:** You cannot add or edit Interface Name, Description, and Unit for a logical interface.

To delete the logical interface of the DOCSIS Mini-PIM using J-Web:

1. Select **Interfaces > Configure**.
2. Under Interface, select **cm-4/0/0.0** and then click **Delete**. A pop-up window appears.
3. Click **Yes**.

### Configuring the DOCSIS Physical Interfaces (J-Web procedure)

To edit the physical interface of the DOCSIS Mini-PIM using J-Web:

1. Select **Interfaces > Configure**.
2. Under Interface, select **cm-4/0/0** and then click **Edit**. A pop-up window appears.
3. In the **Description** box, enter a description to be updated for the configured Mini-PIM interface.
4. In the **MTU** box, enter an integer value between 256 and 9192 bytes.
5. Click **OK**.

To disable the physical interface of the DOCSIS Mini-PIM using J-Web:

1. Select **Interfaces > Configure**.
2. Under Interface, select **cm-4/0/0** and then click **Disable**. A pop-up window appears.
3. Click **Yes**.

### Verifying DOCSIS Interfaces Properties

**Purpose**
Verify that the DOCSIS interface properties are configured properly.

**Action**
From the CLI configuration editor, enter the `show interfaces interface-name extensive` command.

**Sample Output**
```
show interfaces cm-1/0/0 extensive

Physical interface: cm-1/0/0, Enabled, Physical link is Up

   Interface index: 154, SNMP ifIndex: 522, Generation: 157

   Link-level type: Ethernet, MTU: 1518, Speed: 40mbps

   Link flags     : None
   Hold-times     : Up 0 ms, Down 0 ms

   State   : OPERATIONAL, Mode: 2.0, Upstream speed: 5120000 0 0 0

   Downstream scanning: CM_MEDIA_STATE_DONE, Ranging: CM_MEDIA_STATE_DONE


   Downstream buffers used           : 0
   Downstream buffers free           : 0
```
Upstream buffers free : 0
Upstream buffers used : 0
Request opportunity burst : 0 MSlots
Physical burst : 0 MSlots
Tuner frequency : 555 0 0 0 MHz
Standard short grant : 0 Slots
Standard long grant : 0 Slots
Baseline privacy state: authorized, Encryption algorithm: ?????, Key length: 0

<table>
<thead>
<tr>
<th>MAC statistics:</th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total octets</td>
<td>1935</td>
<td>2036</td>
</tr>
<tr>
<td>Total packets</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

CoS queues : 8 supported, 8 maximum usable queues
Current address: 00:24:dc:0d:76:19, Hardware address: 00:24:dc:0d:76:19
Last flapped : 2009-11-10 19:55:40 UTC (00:16:29 ago)
Statistics last cleared: Never

Traffic statistics:
Input bytes : 710 0 bps
Output bytes : 866 0 bps
Input packets: 2 0 pps
Output packets: 4 0 pps

Packet Forwarding Engine configuration:
Destination slot: 1
Direction : Output

<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>%</td>
<td>bps</td>
</tr>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>38000000</td>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 network-control</td>
<td>5</td>
<td>2000000</td>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Logical interface cm-1/0/0.0 (Index 69) (SNMP ifIndex 523) (Generation 134)

Flags: Point-To-Point SNMP-Traps Encapsulation: ENET2

Traffic statistics:
- Input bytes: 710
- Output bytes: 806
- Input packets: 2
- Output packets: 4

Local statistics:
- Input bytes: 710
- Output bytes: 806
- Input packets: 2
- Output packets: 4

Transit statistics:
- Input bytes: 0
- Output bytes: 0
- Input packets: 0
- Output packets: 0

Security: Zone: Null

Flow Statistics:

Flow Input statistics:
- Self packets: 0
- ICMP packets: 0
- VPN packets: 0
- Multicast packets: 0
- Bytes permitted by policy: 0
- Connections established: 0

Flow Output statistics:
- Multicast packets: 0
- Bytes permitted by policy: 0
Flow error statistics (Packets dropped due to):

- Address spoofing: 0
- Authentication failed: 0
- Incoming NAT errors: 0
- Invalid zone received packet: 0
- Multiple user authentications: 0
- Multiple incoming NAT: 0
- No parent for a gate: 0
- No one interested in self packets: 0
- No minor session: 0
- No more sessions: 0
- No NAT gate: 0
- No route present: 0
- No SA for incoming SPI: 0
- No tunnel found: 0
- No session for a gate: 0
- No zone or NULL zone binding: 0
- Policy denied: 0
- Security association not active: 0
- TCP sequence number out of window: 0
- Syn-attack protection: 0
- User authentication errors: 0

Protocol inet, MTU: 1504, Generation: 147, Route table: 0

Flags: None

Addresses, Flags: Is-Preferred Is-Primary

Destination: 20.20.20/24, Local: 20.20.20.5, Broadcast: 20.20.20.255, Generation: 144

**Meaning** The output shows a summary of information about the DOCSIS interface in this example.
Chapter 7

Configuring VDSL2 Interface

This chapter includes following sections:

- Before You Begin on page 189
- Configuring the VDSL2 Interface with the CLI Configuration Editor on page 189
- Example: Configuring the VDSL2 Interface on SRX Series Services Gateways (CLI) on page 191
- Example: Configuring the ADSL Interface on SRX Series Services Gateway (CLI) on page 208

Before You Begin

Before you begin configuring VDSL2 interfaces, complete the following tasks:

- Establish basic connectivity. See the Getting Started Guide for your device.
- If you do not already have a basic understanding of physical and logical interfaces and Juniper Networks interface conventions, read “Interfaces Overview” on page 3.
- Configure network interfaces as necessary. See “Configuring Ethernet, DS1, DS3, and Serial Interfaces” on page 81.

Configuring the VDSL2 Interface with the CLI Configuration Editor

NOTE: J-Web support for configuring the VDSL2 Interface is not available in JUNOS Software Release 10.1.

To use the CLI configuration editor to configure the VDSL2 network interfaces for SRX210 and SRX240 devices:

1. Navigate to the top of the interfaces configuration hierarchy in the CLI configuration editor.
2. Perform the configuration tasks described in Table 47 on page 190.
3. Commit the configuration once you have completed configuring the device.
NOTE: The VDSL2 Mini-PIM has backward compatibility with ADSL/ADSL2/ADSL2+. The VDSL2 interface is represented by the `pt` interface when configured to function as VDSL2, and the ADSL interface is represented by the `at` interface when configured to function as ADSL.

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Interfaces</strong> level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter</td>
<td>Provides a hierarchy level to configure the interface.</td>
</tr>
<tr>
<td></td>
<td><code>edit interfaces pt-1/0/0</code></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Physical Properties

Configure the type of VDSL2 profiles.

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>From the [edit] hierarchy level, enter</td>
<td>The following profiles are supported:</td>
</tr>
<tr>
<td></td>
<td><code>set interfaces interface name vdsl-options vdsl-profile profile-name</code></td>
<td>■ <code>8a</code></td>
</tr>
<tr>
<td></td>
<td>Example</td>
<td>■ <code>8b</code></td>
</tr>
<tr>
<td></td>
<td><code>set interfaces pt-1/0/0 vdsl-options vdsl-profile auto</code></td>
<td>■ <code>8c</code></td>
</tr>
<tr>
<td></td>
<td>Example</td>
<td>■ <code>8d</code></td>
</tr>
<tr>
<td></td>
<td><code>set interfaces pt-1/0/0 vdsl-options vdsl-profile auto</code></td>
<td>■ <code>12a</code></td>
</tr>
<tr>
<td></td>
<td>Example</td>
<td>■ <code>12b</code></td>
</tr>
<tr>
<td></td>
<td><code>set interfaces pt-1/0/0 vdsl-options vdsl-profile auto</code></td>
<td>■ <code>17a</code></td>
</tr>
<tr>
<td></td>
<td>Example</td>
<td>■ auto (default)</td>
</tr>
</tbody>
</table>

### Configuring Logical Properties

Add the logical interface.

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>From the [edit] hierarchy level, enter</td>
<td>Defines one or more logical units that you connect to this physical VDSL interface.</td>
</tr>
<tr>
<td></td>
<td><code>set interfaces interface name unit unit value</code></td>
<td>Set a value from 0 through 16385. Add other values if required by your network.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>set interfaces pt-1/0/0 unit 0</code></td>
<td></td>
</tr>
</tbody>
</table>

Select the encapsulation for the logical interface.

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>set interfaces interface name unit unit value encapsulation encapsulation-type</code></td>
<td>Specifies the type of encapsulation on the VDSL logical interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>■ <code>ppp-over-ether</code>—Use this type of encapsulation for PPPoE over VDSL interfaces that carry IPv4 traffic.</td>
</tr>
<tr>
<td></td>
<td><code>set interfaces pt-1/0/0 unit 0 encapsulation ppp-over-ether</code></td>
<td>NOTE: The encapsulation type Point-to-Point Protocol over Ethernet (PPPoE) is supported for the VDSL2 interface. You can also set no encapsulation for the VDSL2 interface.</td>
</tr>
</tbody>
</table>

---

**Table 47: Configuring the VDSL2 Interface Using the CLI Configuration Editor**

**NOTE:** The encapsulation type Point-to-Point Protocol over Ethernet (PPPoE) is supported for the VDSL2 interface. You can also set no encapsulation for the VDSL2 interface.
Example: Configuring the VDSL2 Interface on SRX Series Services Gateways (CLI)

This topic provides information on the minimum steps required to configure a VDSL2 interface on SRX Series devices. The configuration example uses an SRX210 device; the information is also applicable to the SRX240 device.

This topic includes the following sections:

- Requirements on page 191
- Overview on page 191
- Before You Begin on page 192
- VDSL2 Interface Configuration on page 193

Requirements

Before you configure the VDSL2 interface, be sure you have completed the following tasks:

- Install JUNOS Software Release 10.1 or later for the SRX Series devices.
- Set up and perform initial configuration on the SRX Series device.
- Install the VDSL2 Mini-PIM on the SRX210 device chassis.
- Connect the SRX210 device to a DSLAM.

Overview

The SRX210 and SRX240 devices support the VDSL2 Mini-Physical Interface Module (Mini-PIM) (Annex A). The VDSL2 Mini-PIM carries the Ethernet backplane. When the Mini-PIM is plugged into the chassis, the Mini-PIM connects to one of the ports of the baseboard switch. The VDSL2 Mini-PIM on the SRX Series devices provides ADSL backward compatibility.
Figure 30 on page 192 shows a typical SRX Series Services Gateway VDSL2 Mini-PIM network connection.

**Before You Begin**

Note the following before you start configuration:

- On the VDSL2 Mini-PIMs, by default the pt-1/0/0 interface is created when there is no configuration already created for either pt-1/0/0 or at-1/0/0 interface. You can switch to ADSL mode by just configuring at-1/0/0. If the configurations are already created for pt-1/0/0 or at-1/0/0, then you need to deactivate pt-1/0/0 before you create at-1/0/0 or deactivate at-1/0/0 to create pt-1/0/0.

Use the following commands to deactivate pt-1/0/0 or at-1/0/0:

- deactivate interface pt-1/0/0
- deactivate interface at-1/0/0

- Before you begin a new configuration, make sure that you have deleted the previous configurations on pt-1/0/0 and pp0.

Use following command to delete the old configuration:

- delete interface pt-1/0/0
- delete interface pp0
VDSL2 Interface Configuration

This section provides information about the following configurations:

- VDSL2 Mini-PIM Default Configuration and Verification on page 193
- Configuring the VDSL2 Interface for End-to-End Data Path on page 196
- Configuring PPPoE on the pt-x/x/x Interface with a Static IP Address on page 199
- Configuring PPPoE on the pt-x/x/x Interface with a Static IP Address (CHAP Authentication) on page 200
- Configuring PPPoE on the pt-x/x/x Interface with Unnumbered IP (PAP Authentication) on page 202
- Configuring PPPoE on the pt-x/x/x Interface with Unnumbered IP (CHAP Authentication) on page 203
- Configuring PPPoE on the pt-x/x/x Interface with Negotiated IP (PAP Authentication) on page 205
- Configuring PPPoE on the pt-x/x/x Interface with Negotiated IP (CHAP Authentication) on page 206

VDSL2 Mini-PIM Default Configuration and Verification

2. Verify the FPC status by entering the `show chassis fpc` command. The output should display FPC status as online.

```
user@host# run show chassis fpc
Temp CPU Utilization (%) Memory Utilization (%)
Slot State (C) Total Interrupt DRAM (MB) Heap Buffer
0 Online --------------------------- CPU less FPC ---------------------------
1 Online --------------------------- CPU less FPC ---------------------------
```

NOTE: The VDSL2 Mini-PIM is installed in the first slot of the SRX210 device chassis; therefore the FPC used here is fpc 1. For SRX240 devices, the FPC used will be fpc 1, fpc 2, fpc 3, or fpc 4.

3. Enter `run show interface pt-1/0/0` and verify the following information in the command output:

- Status of interface pt-1/0/0 is displayed as `physical link is up`.
- Modem status is displayed as `Showtime (Profile-17a)`.
- Time in seconds during which the interface stayed up is displayed as `Seconds in Showtime`.
- VDSL profile is displayed as `Auto Annex A`.

Example: Configuring the VDSL2 Interface on SRX Series Services Gateways (CLI)
Physical interface: pt-1/0/0, Enabled, Physical link is Up
Interface index: 146, SNMP ifIndex: 524, Generation: 149
Type: PTM, Link-level type: Ethernet, MTU: 1496, VDSL mode, Speed: 45440kbps
Speed: VDSL2
Device flags : Present Running
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:b1:7e:85:84:ff
Statistics last cleared: 2009-10-19 00:29:37 PDT (00:00:02 ago)
Traffic statistics:
  Input bytes : 22438962 97070256 bps
  Output bytes : 10866024 43334088 bps
  Input packets: 15141 8187 pps
  Output packets: 7332 3655 pps
Input errors:
  Errors: 0, Drops: 0, Policed discards: 0, L3 incompletes: 0,
  L2 channel errors: 0, L2 mismatch timeouts: 0, Resource errors: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, Aged packets: 0, MTU
  errors: 0,
  Resource errors: 0
Egress queues: 8 supported, 4 in use
Queue counters: Queued packets Transmitted packets Dropped packets
  0 best-effort 6759 6760 0
  1 expedited-fo 0 0 0
  2 assured-forw 0 0 0
  3 network-cont 0 0 0
VDSL alarms : None
VDSL defects : None
VDSL media: Seconds Count State
  LOF 0 0 OK
  LOS 0 0 OK
  LOM 0 0 OK
  LOP 0 0 OK
  LOCIDI 0 0 OK
  LOCNDI 0 0 OK
VDSL status:
  Modem status : Showtime (Profile-17a)
  VDSL profile : Profile-17a Annex A
  Last fail code: None
  Subfunction : 0x00
  Seconds in showtime : 45171
VDSL Chipset Information: VTU-R VTU-C
  Vendor Country : 0xb5 0xb5
  Vendor ID : BDCM BDCM
  Vendor Specific: 0x9385 0x9385
VDSL Statistics: VTU-R VTU-C
  Attenuation (dB) : 0.0 0.0
  Capacity used (%) : 0 0
  Noise margin (dB) : 20.0 20.0
  Output power (dBm) : 6.0 12.0

<table>
<thead>
<tr>
<th>Interleave</th>
<th>Fast</th>
<th>Interleave</th>
<th>Fast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit rate (kbps) : 100004</td>
<td>0</td>
<td>45440</td>
<td>0</td>
</tr>
<tr>
<td>CRC : 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FEC : 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>HEC : 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Packet Forwarding Engine configuration:
  Destination slot: 0 (0x00)
CoS information:
Direction : Output
CoS transmit queue Bandwidth Buffer Priority Limit

<table>
<thead>
<tr>
<th>Limit</th>
<th>%</th>
<th>bps</th>
<th>%</th>
<th>usec</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>best-effort</td>
<td>95</td>
<td>43168000</td>
<td>95</td>
<td>0</td>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>network-control</td>
<td>5</td>
<td>2272000</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Logical interface pt-1/0/0.0 (Index 71) (SNMP ifIndex 525) (Generation 136)
Flags: SNMP-Traps Encapsulation: ENET2
Traffic statistics:
Input bytes : 23789064
Output bytes : 10866024
Input packets: 16052
Output packets: 7332
Local statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Transit statistics:
Input bytes : 23789064  97070256 bps
Output bytes : 10866024  43334088 bps
Input packets: 16052  8187 pps
Output packets: 7332  3655 pps
Security: Zone: Null
Flow Statistics :
Flow Input statistics :
Self packets : 0
ICMP packets : 0
VPN packets : 0
Multicast packets : 0
Bytes permitted by policy : 0
Connections established : 0
Flow Output statistics:
Multicast packets : 0
Bytes permitted by policy : 0
Flow error statistics (Packets dropped due to):
Address spoofing: 0
Authentication failed: 0
Incoming NAT errors: 0
Invalid zone received packet: 0
Multiple user authentications: 0
Multiple incoming NAT: 0
No parent for a gate: 0
No one interested in self packets: 0
No minor session: 0
No more sessions: 0
No NAT gate: 0
No route present: 0
No SA for incoming SPI: 0
No tunnel found: 0
No session for a gate: 0
No zone or NULL zone binding 0
Policy denied: 0
Security association not active: 0
TCP sequence number out of window: 0
Syn-attack protection: 0
User authentication errors: 0

Example: Configuring the VDSL2 Interface on SRX Series Services Gateways (CLI)  ■  195
Configuring the VDSL2 Interface for End-to-End Data Path

The following steps provide the basic configuration details for the VDSL2 interface on an SRX210 device for end-to-end data path.

1. Configure the VDSL2 interface with the VDSL profile and the Layer-3 configuration.

```
user@host# set interfaces pt-1/0/0 vdsl-options vdsl-profile 17a
[edit]
user@host# set interfaces pt-1/0/0 unit 0 family inet address 11.11.11.1/24
[edit]
user@host# commit
commit complete
```

2. Verify interface status by using the `show interface terse` command and test end-to-end data path connectivity by sending the ping packets to the remote end IP address.

```
user@host# run show interfaces pt-1/0/0 terse
Interface Admin Link Proto Local Remote
pt-1/0/0 up up
pt-1/0/0.0 up up inet 11.11.1.1/24
[edit]
user@host# run ping 11.11.11.2 count 1000 rapid
PING 11.11.11.2 (11.11.11.2): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
- 11.11.11.2 ping statistics ---
1000 packets transmitted, 1000 packets received, 0% packet loss
round-trip min/avg/max/stddev = 16.109/17.711/28.591/2.026 ms
```

3. Verify the VDSL2 interface configuration and check the traffic statistics.

```
user@host# run show interfaces pt-1/0/0 extensive
Physical interface: pt-1/0/0, Enabled, Physical link is Up
Interface index: 146, SNMP ifIndex: 524, Generation: 197
Type: PTM, Link-level type: Ethernet, MTU: 1496, VDSL mode, Speed: 45440kbps
Speed: VDSL2
Device flags : Present Running
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:b1:7e:85:84:ff
Last flapped : 2009-10-28 00:36:29 PDT (00:12:03 ago)
Statistics last cleared: 2009-10-28 00:47:56 PDT (00:00:36 ago)
Traffic statistics:
Input bytes : 84000 0 bps
Output bytes : 138000 0 bps
Input packets: 1000 0 pps
```
Output packets: 1000 0 pps

Input errors:
Errors: 0, Drops: 0, Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0, Resource errors: 0

Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, Aged packets: 0, MTU errors: 0, Resource errors: 0

Egress queues: 8 supported, 4 in use

Queue counters:

<table>
<thead>
<tr>
<th>Queue Type</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>1 expedited-fo</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 network-cont</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

VDXL alarms: None
VDXL defects: None

VDXL media:

<table>
<thead>
<tr>
<th></th>
<th>Seconds</th>
<th>Count</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOF</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>LOS</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>LOM</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>LOP</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>LOCDI</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>LOCDNI</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
</tbody>
</table>

VDXL status:
Modem status: Showtime (Profile-17a)
VDXL profile: Profile-17a Annex A
Last fail code: None
Subfunction: 0x00
Seconds in showtime: 723

VDXL Chipset Information:

<table>
<thead>
<tr>
<th>Vendor Country</th>
<th></th>
<th>Vendor ID</th>
<th></th>
<th>Vendor Specific</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0xb5</td>
<td></td>
<td>BDCM</td>
<td></td>
<td>0x9385</td>
<td></td>
</tr>
</tbody>
</table>

VDXL Statistics:

| Attenuation (dB) | 0.0 | 0.0 |
| Capacity used (%)| 0   | 0   |
| Noise margin (dB)| 16.0| 20.0|
| Output power (dBm)| 5.0 | 13.0|

Interleave Fast Interleave

<table>
<thead>
<tr>
<th>Bit rate (kbps)</th>
<th>10004</th>
<th>0</th>
<th>45440</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRC</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FEC</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>HEC</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Packet Forwarding Engine configuration:
Destination slot: 0 (0x00)

CoS information:
Direction: Output

<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>43168000</td>
</tr>
</tbody>
</table>
Logical interface pt-1/0/0.0 (Index 72) (SNMP ifIndex 521) (Generation 158)

Flags: SNMP-Traps Encapsulation: ENET2

Traffic statistics:
Input bytes : 84000
Output bytes : 98000
Input packets: 1000
Output packets: 1000

Local statistics:
Input bytes : 84000
Output bytes : 98000
Input packets: 1000
Output packets: 1000

Transit statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps

Security: Zone: Null
Flow Statistics:
Flow Input statistics:
Self packets : 0
ICMP packets : 0
VPN packets : 0
Multicast packets : 0
Bytes permitted by policy : 0
Connections established : 0

Flow Output statistics:
Multicast packets : 0
Bytes permitted by policy : 0

Flow error statistics (Packets dropped due to):
Address spoofing: 0
Authentication failed: 0
Incoming NAT errors: 0
Invalid zone received packet: 0
Multiple user authentications: 0
Multiple incoming NAT: 0
No parent for a gate: 0
No one interested in self packets: 0
No minor session: 0
No more sessions: 0
No NAT gate: 0
No route present: 0
No SA for incoming SPI: 0
No tunnel found: 0
No session for a gate: 0
No zone or NULL zone binding: 0
Policy denied: 0
Security association not active: 0
TCP sequence number out of window: 0
Syn-attack protection: 0
User authentication errors: 0

Protocol inet, MTU: 1482, Generation: 169, Route table: 0
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
    Destination: 11.11.11/24, Local: 11.11.11.1, Broadcast: 11.11.11.255, Generation: 189
Configuring PPPoE on the pt-x/x/x Interface with a Static IP Address

1. Configure the VDSL2 interface on the SRX210 device.

```
user@host# set interfaces pt-1/0/0 vdsl-options vdsl-profile 17a
[edit]
user@host# set interfaces pt-1/0/0 unit 0 encapsulation ppp-over-ether
[edit]
user@host# set interfaces pp0 unit 0 ppp-options pap access-profile pap_prof
[edit]
user@host# set interfaces pp0 unit 0 ppp-options pap local-name locky
[edit]
user@host# set interfaces pp0 unit 0 ppp-options pap local-password india
[edit]
user@host# set interfaces pp0 unit 0 ppp-options pap passive
[edit]
user@host# set interfaces pp0 unit 0 pppoe-options underlying-interface pt-1/0/0.0
[edit]
user@host# set interfaces pp0 unit 0 pppoe-options auto-reconnect 120
[edit]
user@host# set interfaces pp0 unit 0 pppoe-options client
[edit]
user@host# set interfaces pp0 unit 0 family inet address 10.1.1.6/24
[edit]
user@host# set access profile pap_prof authentication-order password
[edit]
user@host# set access profile pap_prof client cuttack pap-password india
[edit]
user@host# commit
commit complete
```

2. Verify the interface output.

```
user@host# run show interfaces pp0
Physical interface: pp0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 510
  Type: PPPoE, Link-level type: PPPoE, MTU: 1532
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link type      : Full-Duplex
  Link flags     : None
  Input packets  : 0
  Output packets : 0

Logical interface pp0.0 (Index 71) (SNMP ifIndex 522)
  Flags: Hardware-Down Point-To-Point SNMP-Traps 0x0 Encapsulation: PPPoE
  PPPoE:
    State: SessionDown, Session ID: None,
    Configured AC name: None, Service name: None,
    Auto-reconnect timeout: 120 seconds, Idle timeout: Never,
    Underlying interface: pt-1/0/0.0 (Index 69)
    Input packets : 57
    Output packets: 56
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 22 (00:00:40 ago), Output: 25 (00:00:04 ago)
  LCP state: Down
```
3. Verify the end-to-end data path on the interface.

```
user@host# run show interfaces pt-1/0/0 terse
Interface               Admin Link Proto    Local                 Remote
pt-1/0/0                up    up
pt-1/0/0.0              up    up

[edit]
user@host# run show interfaces pp0 terse
Interface               Admin Link Proto    Local                 Remote
pp0                     up    up
pp0.0                   up    up   inet     10.1.1.6/24

[edit]
user@host# run ping 10.1.1.1 count 100 rapid
PING 10.1.1.1 (10.1.1.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
- 10.1.1.1 ping statistics ---
100 packets transmitted, 100 packets received, 0% packet loss
time=15.649 ms
```

### Configuring PPPoE on the pt-x/x/x Interface with a Static IP Address (CHAP Authentication)

1. Configure the VDSL interface on the SRX210 device.

```
user@host# set interfaces pt-1/0/0 vdsl-options vdsl-profile 17a
[edit]
user@host# set interfaces pt-1/0/0 unit 0 encapsulation ppp-over-ether
[edit]
user@host# set interfaces pp0 unit 0 ppp-options chap default-chap-secret india
[edit]
user@host# set interfaces pp0 unit 0 ppp-options chap local-name locky
[edit]
user@host# set interfaces pp0 unit 0 ppp-options chap passive
[edit]
user@host# set interfaces pp0 unit 0 pppoe-options underlying-interface pt-1/0/0.0
[edit]
user@host# set interfaces pp0 unit 0 pppoe-options auto-reconnect 120
[edit]
user@host# set interfaces pp0 unit 0 pppoe-options client
[edit]
user@host# set interfaces pp0 unit 0 family inet address 10.1.1.6/24
[edit]
user@host# commit
commit complete
```
2. Verify the interface status.

```bash
user@host# run show interfaces pp0
Physical interface: pp0, Enabled, Physical link is Up
Interface index: 128, SNMP ifIndex: 510
Type: PPPoE, Link-level type: PPPoE, MTU: 1532
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps
Link type : Full-Duplex
Link flags : None
Input packets : 0
Output packets: 0

Logical interface pp0.0 (Index 70) (SNMP ifIndex 522)
Flags: Point-To-Point SNMP-Traps 0x0 Encapsulation: PPPoE
PPPoE:
  State: SessionUp, Session ID: 31,
  Session AC name: cuttack, Remote MAC address: 00:03:6c:c8:8c:55,
  Configured AC name: None, Service name: None,
  Auto-reconnect timeout: 120 seconds, Idle timeout: Never,
  Underlying interface: pt-1/0/0.0 (Index 69)
Input packets : 12
Output packets: 10
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive: Input: 1 (00:00:08 ago), Output: 0 (never)
LCP state: Opened
NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured,
  mpls: Not-configured
  CHAP state: Success
  PAP state: Closed
Security: Zone: Null
Protocol inet, MTU: 1492
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
  Destination: 10.1.1/24, Local: 10.1.1.6
```

3. Verify the interface and check end-to-end data path connectivity.

```bash
user@host# run show interfaces pt-1/0/0 terse
Interface               Admin Link Proto    Local                 Remote
pt-1/0/0                up    up
pt-1/0/0.0              up    up   inet     10.1.1.6/24

[edit]
user@host# run show interfaces pp0 terse
Interface               Admin Link Proto    Local                 Remote
pp0                     up    up
pp0.0                   up    up   inet     10.1.1.6/24

[edit]
user@host# run ping 10.1.1.1 count 100 rapid
PING 10.1.1.1 (10.1.1.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 10.1.1.1 ping statistics ---
100 packets transmitted, 100 packets received, 0% packet loss
round-trip min/avg/max/stddev = 14.608/15.466/25.939/1.779 ms
```
Configuring PPPoE on the pt-x/x/x Interface with Unnumbered IP (PAP Authentication)

1. Configure the VDSL2 interface on the SRX210 device:

   user@host# set interfaces pt-1/0/0 vdsl-options vdsl-profile 17a
   [edit]
   user@host# set interfaces pt-1/0/0 unit 0 encapsulation ppp-over-ether
   [edit]
   user@host# set interfaces lo0 unit 0 family inet address 10.1.1.24/32
   [edit]
   user@host# set interfaces pp0 unit 0 ppp-options pap access-profile pap_prof
   [edit]
   user@host# set interfaces pp0 unit 0 ppp-options pap local-name locky
   [edit]
   user@host# set interfaces pp0 unit 0 ppp-options pap local-password india
   [edit]
   user@host# set interfaces pp0 unit 0 ppp-options pap passive
   [edit]
   user@host# set interfaces pp0 unit 0 pppoe-options underlying-interface pt-1/0/0.0
   [edit]
   user@host# set interfaces pp0 unit 0 pppoe-options auto-reconnect 120
   [edit]
   user@host# set interfaces pp0 unit 0 pppoe-options client
   [edit]
   user@host# set interfaces pp0 unit 0 family inet unnumbered-address lo0.0
   [edit]
   user@host# set interfaces pp0 unit 0 family inet unnumbered-address destination 10.1.1.1
   [edit]
   user@host# set access profile pap_prof authentication-order password
   [edit]
   user@host# set access profile pap_prof client cuttack pap-password india
   [edit]
   user@host# commit
   commit complete

2. Verify the interface status.

   user@host# run show interfaces pp0
   Physical interface: pp0, Enabled, Physical link is Up
   Interface index: 128, SNMP ifIndex: 510
   Type: PPPoE, Link-level type: PPPoE, MTU: 1532
   Device flags : Present Running
   Interface flags: Point-To-Point SNMP-Traps
   Link type : Full-Duplex
   Link flags : None
   Input packets : 0
   Output packets: 0

   Logical interface pp0.0 (Index 72) (SNMP ifIndex 522)
   Flags: Point-To-Point SNMP-Traps 0x0 Encapsulation: PPPoE
   PPPoE:
   State: SessionUp, Session ID: 33,
   Session AC name: cuttack, Remote MAC address: 00:03:6c:c8:8c:55,
   Configured AC name: None, Service name: None,
   Auto-reconnect timeout: 120 seconds, Idle timeout: Never,
Underlying interface: pt-1/0/0.0 (Index 69)
Input packets : 22
Output packets: 20
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive: Input: 1 (00:00:08 ago), Output: 0 (never)
LCP state: Opened
CHAP state: Closed
PAP state: Success
Security: Zone: Null
Protocol inet, MTU: 1492
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
  Destination: 10.1.1.1, Local: 10.1.1.24

3. Verify the end-to-end data path testing.

```
user@host# run show interfaces pt-1/0/0 terse
Interface               Admin Link Proto    Local                 Remote
pt-1/0/0                up    up
pt-1/0/0.0              up    up

[edit]
user@host# run show interfaces pp0 terse
Interface               Admin Link Proto    Local                 Remote
pp0                     up    up   inet     10.1.1.24           -->
pp0.0                   up    up    inet 10.1.1.24          -->
10.1.1.1

[edit]
user@host# run ping 10.1.1.1 count 100 rapid
PING 10.1.1.1 (10.1.1.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 10.1.1.1 ping statistics ---
100 packets transmitted, 100 packets received, 0% packet loss
round-trip min/avg/max/stddev = 14.584/15.503/21.204/1.528 ms
```

Configuring PPPoE on the pt-x/x/x Interface with Unnumbered IP (CHAP Authentication)

1. Configure the VDSL2 interface on the SRX210 device:

```
user@host# set interfaces pt-1/0/0 vdsl-options vdsl-profile 17a
[edit]
user@host# set interfaces pt-1/0/0 unit 0 encapsulation ppp-over-ether
[edit]
user@host# set interfaces lo0 unit 0 family inet address 10.1.1.24/32
[edit]
user@host# set interfaces pp0 unit 0 ppp-options chap default-chap-secret india
[edit]
user@host# set interfaces pp0 unit 0 ppp-options chap local-name locky
[edit]
user@host# set interfaces pp0 unit 0 ppp-options chap passive
[edit]
user@host# set interfaces pp0 unit 0 pppoe-options underlying-interface pt-1/0/0.0
[edit]
```
user@host# set interfaces pp0 unit 0 pppoe-options auto-reconnect 120
[edit]
user@host# set interfaces pp0 unit 0 pppoe-options client
[edit]
user@host# set interfaces pp0 unit 0 family inet unnumbered-address lo0.0
[edit]
user@host# set interfaces pp0 unit 0 family inet unnumbered-address destination 10.1.1.1
[edit]
user@host# commit
commit complete

2. Verify the interface status.

user@host# run show interfaces pp0
Physical interface: pp0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 510
  Type: PPPoE, Link-level type: PPPoE, MTU: 1532
  Device flags: Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link type: Full-Duplex
  Link flags: None
    Input packets: 0
    Output packets: 0

Logical interface pp0.0 (Index 70) (SNMP ifIndex 522)
  Flags: Point-To-Point SNMP-Traps 0x0 Encapsulation: PPPoE
  PPPoE:
    State: SessionUp, Session ID: 35,
    Session AC name: cuttack, Remote MAC address: 00:03:6c:c8:8c:55,
    Configured AC name: None, Service name: None,
    Auto-reconnect timeout: 120 seconds, Idle timeout: Never,
    Underlying interface: pt-1/0/0.0 (Index 69)
    Input packets: 25
    Output packets: 22
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 2 (00:00:10 ago), Output: 2 (00:00:02 ago)
  LCP state: Opened
  NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured,
  mpls: Not-configured
  CHAP state: Success
  PAP state: Closed
  Security: Zone: Null
  Protocol inet, MTU: 1492
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 10.1.1.1, Local: 10.1.1.24

3. Verify the end-to-end data path testing on the PPPoE interface.

user@host# run show interfaces pt-1/0/0 terse
Interface               Admin Link Proto    Local                 Remote
pt-1/0/0                up    up
pt-1/0/0.0              up    up   inet     10.1.1.24           -->
10.1.1.1

Example: Configuring the VDSL2 Interface on SRX Series Services Gateways (CLI)
[edit]
user@host# run ping 10.1.1.1 count 100 rapid
PING 10.1.1.1 (10.1.1.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
-- 10.1.1.1 ping statistics ---
100 packets transmitted, 100 packets received, 0% packet loss
round-trip min/avg/max/stddev = 14.585/16.025/22.354/2.019 ms

Configuring PPPoE on the pt-x/x/x Interface with Negotiated IP (PAP Authentication)

1. Configure the VDSL2 interface on the SRX210 device.

    user@host# set interfaces pt-1/0/0 vdsl-options vdsl-profile 17a
    [edit]
    user@host# set interfaces pt-1/0/0 unit 0 encapsulation ppp-over-ether
    [edit]
    user@host# set interfaces pp0 unit 0 ppp-options pap access-profile my_prf
    [edit]
    user@host# set interfaces pp0 unit 0 ppp-options pap local-name purple
    [edit]
    user@host# set interfaces pp0 unit 0 ppp-options pap local-password
    Embe1mpls
    [edit]
    user@host# set interfaces pp0 unit 0 ppp-options pap passive
    [edit]
    user@host# set interfaces pp0 unit 0 pppoe-options underlying-interface
    pt-1/0/0.0
    [edit]
    user@host# set interfaces pp0 unit 0 pppoe-options auto-reconnect 120
    [edit]
    user@host# set interfaces pp0 unit 0 pppoe-options client
    [edit]
    user@host# set interfaces pp0 unit 0 family inet negotiate-address
    [edit]
    user@host# set access profile my_prf authentication-order password
    [edit]
    user@host# set access-profile my_prf
    [edit]
    user@host# commit
    commit complete

2. Verify the PPPoE interface status.

    user@host# run show interfaces pp0
    Physical interface: pp0, Enabled, Physical link is Up
    Interface index: 128, SNMP ifIndex: 510
    Type: PPPoE, Link-level type: PPPoE, MTU: 1532
    Device flags   : Present Running
    Interface flags: Point-To-Point SNMP-Traps
    Link type      : Full-Duplex
    Link flags     : None
    Input packets  : 0
    Output packets : 0

    Logical interface pp0.0 (Index 72) (SNMP ifIndex 522)
    Flags: Point-To-Point SNMP-Traps 0x0 Encapsulation: PPPoE
PPPoE:
State: SessionUp, Session ID: 4,
Session AC name: belur, Remote MAC address: 00:90:1a:43:18:d1,
Configured AC name: None, Service name: None,
Auto-reconnect timeout: 120 seconds, Idle timeout: Never,
Underlying interface: pt-1/0/0.0 (Index 69)
Input packets : 18
Output packets: 18
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive: Input: 0 (never), Output: 11 (00:00:01 ago)
LCP state: Opened
NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured,
mpls: Not-configured
CHAP state: Closed
PAP state: Success
Security: Zone: Null
Protocol inet, MTU: 1474
Flags: Negotiate-Address
Addresses, Flags: Kernel Is-Preferred Is-Primary

3. Verify the end-to-end data path connectivity.

user@host# run show interfaces pt-1/0/0 terse
Interface               Admin Link Proto    Local                 Remote
pt-1/0/0                up    up
pt-1/0/0.0              up    up

[edit]
user@host# run show interfaces pp0 terse
Interface               Admin Link Proto    Local                 Remote
pp0                     up    up             inet     12.12.12.11         -->
pp0.0                   up    up             inet     12.12.12.1
12.12.12.1

[edit]
user@host# run ping 12.12.12.1 count 100 rapid
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 12.12.12.1 ping statistics ---
100 packets transmitted, 100 packets received, 0% packet loss
round-trip min/avg/max/stddev = 16.223/17.692/24.359/2.292 ms

Configuring PPPoE on the pt-x/x/x Interface with Negotiated IP (CHAP Authentication)

1. Configure the VDSL2 interface on the SRX210 device.

user@host# set interfaces pt-1/0/0 vdsl-options vdsl-profile 17a
[edit]
user@host# set interfaces pt-1/0/0 unit 0 encapsulation ppp-over-ether
[edit]
user@host# set interfaces pp0 unit 0 ppp-options chap default-chap-secret
Embe1mpls
[edit]
user@host# set interfaces pp0 unit 0 ppp-options chap local-name purple
[edit]
user@host# set interfaces pp0 unit 0 ppp-options chap passive
[edit]
Example: Configuring the VDSL2 Interface on SRX Series Services Gateways (CLI)
Example: Configuring the ADSL Interface on SRX Series Services Gateway (CLI)

This topic includes the following sections:

- Requirements on page 208
- Overview on page 208
- ADSL Interface Configuration on page 208

Requirements

Before you configure the ADSL2 interface, be sure you have completed the following tasks:

- Install JUNOS Software Release 10.1 or later for the SRX Series devices.
- Set up and perform initial configuration on the SRX Series device.
- Install the VDSL2 Mini-PIM on the SRX210 device chassis.
- SRX210 device is connected to a DSLAM that supports VDSL2 to ADSL fallback.

Overview

The SRX210 and SRX240 devices support the VDSL2 Mini-Physical Interface Module (Mini-PIM) (Annex A). The VDSL2 Mini-PIM carries the Ethernet backplane. When the Mini-PIM is plugged into the chassis, the Mini-PIM connects to one of the ports of the baseboard switch. The VDSL2 Mini-PIM on the SRX Series devices provides ADSL backward compatibility. The VDSL2 uses EFM or PTM mode as first mile and is represented as pt-x/x/x. In case of ADSL fallback mode, the VDSL2 Mini-PIM operates on the ATM encapsulation interface as first mile and is represented as at-x/x/x.

ADSL Interface Configuration

This section provides information about the following configurations:

- Configuring the ADSL Interface for End-to-End Data Path on page 209
- Configuring PPPoA on the at-x/x/x Interface with Negotiated IP (CHAP Authentication) on page 211
- Configuring PPPoA on the at-x/x/x Interface with Negotiated IP (PAP Authentication) on page 212
- Configuring PPPoA on the at-x/x/x Interface with Static IP (CHAP Authentication) on page 214
Configuring the ADSL Interface for End-to-End Data Path

The following steps provide the basic configuration details for the ADSL interface on an SRX210 device for end-to-end data path for "second mile" ATM.

1. Configure the ADSL interface:

   ```
   user@host# delete interfaces at-1/0/0
   [edit]
   user@host# set interfaces at-1/0/0 encapsulation atm-pvc
   [edit]
   user@host# set interfaces at-1/0/0 atm-options vpi 2
   [edit]
   user@host# set interfaces at-1/0/0 dsl-options operating-mode itu-dmt
   [edit]
   user@host# set interfaces at-1/0/0 unit 0 encapsulation atm-snap
   [edit]
   user@host# set interfaces at-1/0/0 unit 0 vci 2.119
   [edit]
   user@host# set interfaces at-1/0/0 unit 0 family inet address 10.10.1.24
   [edit]
   user@host# commit
   commit complete
   [edit]
   user@host#
   ```

2. Verify interface status by using the `show interfaces at-1/0/0 terse` command and test end-to-end data path connectivity by sending the ping packets to remote end IP address.

   ```
   user@host# run show interfaces at-1/0/0 terse
   Interface       Admin Link Proto  Local     Remote
   at-1/0/0        up    up
   at-1/0/0.0      up    up   inet     10.10.1.24
   at-1/0/0.32767  up    up
   [edit]
   user@host# run ping 10.10.1.2 count 1000 rapid
   PING 10.10.1.2 (10.10.1.2): 56 data bytes
   !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   --- 10.10.1.2 ping statistics ---
   1000 packets transmitted, 1000 packets received, 0% packet loss
   round-trip min/avg/max/stddev = 7.141/9.356/58.347/3.940 ms
   ```
3. Verify the ADSL interface and traffic statistics.

```
user@host# run show interfaces at-1/0/0

Physical interface: at-1/0/0, Enabled, Physical link is Up
  Interface index: 146, SNMP ifIndex: 504
  Link-level type: ATM-PVC, MTU: 1496, Clocking: Internal, ADSL mode,
  Speed: ADSL
  Speed: 832kbps, Loopback: None
  Device flags : Present Running
  Link flags : None
  CoS queues : 8 supported, 8 maximum usable queues
  Current address: 00:b1:7e:85:84:ff
  Last flapped : 2009-10-28 02:14:45 PDT (00:09:54 ago)
  Input rate : 0 bps (0 pps)
  Output rate : 0 bps (0 pps)
  ADSL alarms : None
  ADSL defects : None
  ADSL status:  
    Modem status : Showtime (Itu-dmt)
    DSL mode : Itu-dmt Annex A
    Last fail code: None
    Subfunction : 0x00
    Seconds in showtime : 596

Logical interface at-1/0/0.0 (Index 69) (SNMP ifIndex 523)
  Flags: Point-To-Point SNMP-Traps 0x0 Encapsulation: ATM-SNAP
  Input packets : 1000
  Output packets: 1000
  Security: Zone: Null
  Protocol inet, MTU: 1456
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 10.10.10/24, Local: 10.10.10.1, Broadcast:
    VCI 2.119
      Flags: Active
      Total down time: 0 sec, Last down: Never
      Input packets : 1000
      Output packets: 1000

Logical interface at-1/0/0.32767 (Index 70) (SNMP ifIndex 525)
  Flags: Point-To-Multipoint No-Multicast SNMP-Traps 0x0
  Encapsulation: ATM-VCMUX
  Input packets : 0
  Output packets: 0
  Security: Zone: Null
  VCI 2.4
    Flags: Active
    Total down time: 0 sec, Last down: Never
    Input packets : 0
    Output packets: 0
```
Configuring PPPoA on the at-x/x/x Interface with Negotiated IP (CHAP Authentication)

1. Configure the Point-to-Point Protocol over ATM (PPPoA) on ADSL PHY for "second mile" ATM.

   ```
   user@host# set interfaces at-1/0/0 encapsulation atm-pvc
   [edit]
   user@host# set interfaces at-1/0/0 atm-options vpi 2
   [edit]
   user@host# set interfaces at-1/0/0 unit 0 encapsulation atm-ppp-llc
   [edit]
   user@host# set interfaces at-1/0/0 unit 0 vci 2.119
   [edit]
   user@host# set interfaces at-1/0/0 unit 0 ppp-options chap access-profile jnpr
   [edit]
   user@host# set interfaces at-1/0/0 unit 0 ppp-options chap local-name locky
   [edit]
   user@host# set interfaces at-1/0/0 unit 0 family inet negotiate-address
   [edit]
   user@host# set access profile jnpr client sringeri chap-secret india
   [edit]
   user@host# commit
   commit complete
   [edit]
   user@host#
   ```

2. Verify the interface output:

   ```
   user@host# run show interfaces at-1/0/0
   Physical interface: at-1/0/0, Enabled, Physical link is Up
   Interface index: 146, SNMP ifIndex: 504
   Link-level type: ATM-PVC, MTU: 1496, Clocking: Internal, ADSL mode, Speed: ADSL
   Speed: 832kbps, Loopback: None
   Device flags : Present Running
   Link flags : None
   CoS queues : 8 supported, 8 maximum usable queues
   Current address: 00:b1:7e:85:84:ff
   Last flapped : 2009-10-28 02:39:14 PDT (00:01:37 ago)
   Input rate : 0 bps (0 pps)
   Output rate : 80 bps (0 pps)
   ADSL alarms : None
   ADSL defects : None
   ADSL status:
   Modem status : Showtime (Itu-dmt)
   DSL mode : Auto Annex A
   Last fail code: None
   Subfunction : 0x00
   Seconds in showtime : 97
   Logical interface at-1/0/0.0 (Index 71) (SNMP ifIndex 523)
   Flags: Point-To-Point SNMP-Traps 0x0 Encapsulation: ATM-PPP-LLC
   Input packets : 26
   Output packets: 29
   Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
   Keepalive: Input: 10 (00:00:02 ago), Output: 8 (00:00:06 ago)
   ```
LCP state: Opened
NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured,
  mpls: Not-configured
CHAP state: Success
PAP state: Closed
Security: Zone: Null
Protocol inet, MTU: 1486
  Flags: Negotiate-Address
  Addresses, Flags: Kernel Is-Preferred Is-Primary
    Destination: 100.100.100.6, Local: 100.100.100.1
VCI 2.119
  Flags: Active
    Total down time: 0 sec, Last down: Never
    Input packets : 26
    Output packets: 29

Logical interface at-1/0/0.32767 (Index 70) (SNMP ifIndex 525)
  Flags: Point-To-Multipoint No-Multicast SNMP-Traps 0x0 Encapsulation:
    ATM-VCMUX
  Input packets : 0
  Output packets: 0
  Security: Zone: Null
  VCI 2.4
  Flags: Active
    Total down time: 0 sec, Last down: Never
    Input packets : 0
    Output packets: 0

3. Verify the end-to-end data path connectivity:

```bash
user@host# run show interfaces at-1/0/0 terse
Interface               Admin Link Proto    Local                 Remote
at-1/0/0                up    up
at-1/0/0.0              up    up   inet     100.100.100.1       -->
  100.100.100.6
at-1/0/0.32767          up    up

[edit]
user@host# run ping 100.100.100.6 count 100 rapid
PING 100.100.100.6 (100.100.100.6): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 100.100.100.6 ping statistics ---
100 packets transmitted, 100 packets received, 0% packet loss
round-trip min/avg/max/stddev = 7.231/9.167/58.852/5.716 ms
```

**Configuring PPPoA on the at-x/x/x Interface with Negotiated IP (PAP Authentication)**

1. Configure the PPPoA on ADSL PHY for "second mile" ATM.

```bash
user@host# set interfaces at-1/0/0 encapsulation atm-pvc
[edit]
user@host# set interfaces at-1/0/0 atm-options vpi 2
[edit]
user@host# set interfaces at-1/0/0 dsl-options operating-mode auto
[edit]
user@host# set interfaces at-1/0/0 unit 0 encapsulation atm-ppp-llc
[edit]
```
user@host# set interfaces at-1/0/0 unit 0 vci 2.119
[edit]
user@host# set interfaces at-1/0/0 unit 0 ppp-options pap access-profile jnpr
[edit]
user@host# set interfaces at-1/0/0 unit 0 ppp-options pap local-name locky
[edit]
user@host# set interfaces at-1/0/0 unit 0 ppp-options pap local-password india
[edit]
user@host# set interfaces at-1/0/0 unit 0 family inet negotiate-address
[edit]
user@host# set access profile jnpr client sringeri pap-password india
[edit]
user@host# commit
commit complete

2. Verify the Interface status.

user@host# run show interfaces at-1/0/0
Physical interface: at-1/0/0, Enabled, Physical link is Up
Interface index: 146, SNMP ifIndex: 504
Link-level type: ATM-PVC, MTU: 1496, Clocking: Internal, ADSL mode,
Speed: ADSL
  Speed: 832kbps, Loopback: None
Device flags : Present Running
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Current address: 00:b1:7e:85:84:ff
Last flapped : 2009-10-28 02:39:14 PDT (00:09:29 ago)
Input rate : 0 bps (0 pps)
Output rate : 80 bps (0 pps)
ADSL alarms : None
ADSL defects : None
ADSL status:
  Modem status : Showtime (Itu-dmt)
  DSL mode : Auto Annex A
  Last fail code: None
  Subfunction : 0x00
  Seconds in showtime : 571

Logical interface at-1/0/0.0 (Index 69) (SNMP ifIndex 523)
  Flags: Point-To-Point SNMP-Traps 0x0 Encapsulation: ATM-PPP-LLC
  Input packets : 2
  Output packets: 2
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 8 (00:00:00:01 ago), Output: 9 (00:00:00:03 ago)
  LCP state: Opened
  NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured,
  mpls: Not-configured
  CHAP state: Closed
  PAP state: Success
  Security: Zone: Null
  Protocol inet, MTU: 1486
    Flags: Negotiate-Address
    Addresses, Flags: Kernel Is-Preferred Is-Primary
      Destination: 100.100.100.6, Local: 100.100.100.1
  VCI 2.119
    Flags: Active
    Total down time: 0 sec, Last down: Never
    Input packets : 2

Example: Configuring the ADSL Interface on SRX Series Services Gateway (CLI)
Output packets: 2

Logical interface at-1/0/0.32767 (Index 70) (SNMP ifIndex 525)
  Flags: Point-To-Multipoint No-Multicast SNMP-Traps 0x0 Encapsulation:
  ATM-VCMUX
  Input packets : 0
  Output packets: 0
  Security: Zone: Null
  VCI 2.4
  Flags: Active
  Total down time: 0 sec, Last down: Never
  Input packets : 0
  Output packets: 0

3. Verify the interface and check end-to-end data path connectivity.

```
user@host# run show interfaces at-1/0/0 terse
Interface         Admin Link Proto    Local               Remote
at-1/0/0           up    up               
at-1/0/0.0          up    up inet 100.100.100.1       --> 100.100.100.6
at-1/0/0.32767     up    up               
```

```
[edit]
user@host# run ping 100.100.100.6 count 100 rapid
PING 100.100.100.6 (100.100.100.6): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
2. Verify the interface status.

```bash
user@host# run show interfaces at-1/0/0
Physical interface: at-1/0/0, Enabled, Physical link is Up
Interface index: 146, SNMP ifIndex: 504
Link-level type: ATM-PVC, MTU: 1496, Clocking: Internal, ADSL mode,
Speed: ADSL
Speed: 832kbps, Loopback: None
Device flags : Present Running
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Current address: 00:b1:7e:85:84:ff
Last flapped : 2009-10-28 22:18:50 PDT (00:05:17 ago)
Input rate : 0 bps (0 pps)
Output rate : 0 bps (0 pps)
ADSL alarms : None
ADSL defects : None
ADSL status:
Modem status : Showtime (Itu-dmt)
DSL mode : Auto Annex A
Last fail code: None
Subfunction : 0x00
Seconds in showtime : 316
Logical interface at-1/0/0.0 (Index 71) (SNMP ifIndex 523)
Flags: Point-To-Point SNMP-Traps 0x0 Encapsulation: ATM-PPP-LLC
Input packets : 46
Output packets: 88
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive: Input: 18 (00:00:04 ago), Output: 17 (00:00:08 ago)
LCP state: Opened
NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured,
mpls: Not-configured
CHAP state: Success
PAP state: Closed
Security: Zone: HOST
Allowed host-inbound traffic : any-service bfd bgp dvmrp igmp ldp msdp
nhrp ospf pim rip router-discovery rsvp sap vrrp
Protocol inet, MTU: 1486
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
Destination: 100.100.100/24, Local: 100.100.100.1, Broadcast:
100.100.100.255
VCI 2.119
Flags: Active
Total down time: 0 sec, Last down: Never
Input packets : 46
Output packets: 88
Logical interface at-1/0/0.32767 (Index 72) (SNMP ifIndex 525)
Flags: Point-To-Multipoint No-Multicast SNMP-Traps 0x0 Encapsulation: ATM-VCMUX
Input packets : 0
Output packets: 0
Security: Zone: HOST
Allowed host-inbound traffic : any-service bfd bgp dvmrp igmp ldp msdp
nhrp ospf pim rip router-discovery rsvp sap vrrp
VCI 2.4
Flags: Active
Total down time: 0 sec, Last down: Never
```
3. Verify the end-to-end data path testing.

```
user@host# run show interfaces at-1/0/0 terse
Interface Admin Link Proto     Local               Remote
at-1/0/0     up    up
at-1/0/0.0   up    up   inet     100.100.100.1/24
at-1/0/0.32767 up    up

[edit]
user@host# run ping 100.100.100.6 count 100 rapid
PING 100.100.100.6 (10.100.100.6): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 100.100.100.6 ping statistics ---
100 packets transmitted, 100 packets received, 0% packet loss
round-trip min/avg/max/stddev = 7.787/9.300/15.081/2.023 ms
```

### Configuring PPPoA on the at-x/x/x Interface with Static IP (PAP Authentication)

1. Configure the PPPoA on ADSL PHY for "second mile" ATM.

```
user@host# set interfaces at-1/0/0 encapsulation atm-pvc
[edit]
user@host# set interfaces at-1/0/0 atm-options vpi 2
[edit]
user@host# set interfaces at-1/0/0 unit 0 encapsulation atm-ppp-llc
[edit]
user@host# set interfaces at-1/0/0 unit 0 vci 2.119
[edit]
user@host# set interfaces at-1/0/0 unit 0 ppp-options pap access-profile jnpr
[edit]
user@host# set interfaces at-1/0/0 unit 0 ppp-options pap local-name locky
[edit]
user@host# set interfaces at-1/0/0 unit 0 ppp-options pap local-password india
[edit]
user@host# set interfaces at-1/0/0 unit 0 family inet address 100.100.100.10/24
[edit]
user@host# set access profile jnpr client sringeri pap-password india
[edit]
user@host# commit
commit complete
```

2. Verify the interface status.

```
user@host# run show interfaces at-1/0/0
Physical interface: at-1/0/0, Enabled, Physical link is Up
  Interface index: 146, SNMP ifIndex: 504
  Link-level type: ATM-PVC, MTU: 1496, Clocking: Internal, ADSL mode,
  Speed: ADSL
  Speed: 832kbps, Loopback: None
```
Device flags : Present Running
Link flags : None
CoS queues : 8 supported, 8 maximum usable queues
Current address: 00:b1:7e:85:84:ff
Last flapped : 2009-10-28 22:18:50 PDT (00:10:26 ago)
Input rate : 0 bps (0 pps)
Output rate : 80 bps (0 pps)
ADSL alarms : None
ADSL defects : None
ADSL status:
  Modem status : Showtime (Itu-dmt)
  DSL mode : Auto Annex A
  Last fail code: None
  Subfunction : 0x00
  Seconds in showtime : 624
Logical interface at-1/0/0.0 (Index 73) (SNMP ifIndex 523)
  Flags: Point-To-Point SNMP-Traps 0x0 Encapsulation: ATM-PPP-LLC
  Input packets : 28
  Output packets: 29
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 2 (00:00:01 ago), Output: 1 (00:00:09 ago)
  LCP state: Opened
  CHAP state: Closed
  PAP state: Success
  Security: Zone: HOST
  Allowed host-inbound traffic : any-service bfd bgp dvmrp igmp ldp msdp nh rp ospf pgm pim rip router-discovery rsvp sap vrrp
  Protocol inet, MTU: 1486
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 100.100.100/24, Local: 100.100.100.10, Broadcast: 100.100.100.255
  VCI 2.119
  Flags: Active
  Total down time: 0 sec, Last down: Never
  Input packets : 28
  Output packets: 29
Logical interface at-1/0/0.32767 (Index 72) (SNMP ifIndex 525)
  Flags: Point-To-Multipoint No-Multicast SNMP-Traps 0x0 Encapsulation: ATM-VCMUX
  Input packets : 0
  Output packets: 0
  Security: Zone: HOST
  Allowed host-inbound traffic : any-service bfd bgp dvmrp igmp ldp msdp nh rp ospf pgm pim rip router-discovery rsvp sap vrrp
  VCI 2.4
  Flags: Active
  Total down time: 0 sec, Last down: Never
  Input packets : 0
  Output packets: 0

3. Verify the end-to-end data path testing.

user@host# run show interfaces at-1/0/0 terse
Interface         Admin Link Proto Local           Remote
at-1/0/0          up   up   inet     100.100.100.10/24

Example: Configuring the ADSL Interface on SRX Series Services Gateway (CLI)
Configuring PPPoA on the at-x/x/x Interface with Unnumbered IP (PAP Authentication)

1. Configure the PPPoA on ADSL PHY for "second mile" ATM.

```
user@host# set interfaces at-1/0/0 encapsulation atm-pvc
[edit]
user@host# set interfaces at-1/0/0 atm-options vpi 2
[edit]
user@host# set interfaces at-1/0/0 dsl-options operating-mode auto
[edit]
user@host# set interfaces at-1/0/0 unit 0 encapsulation atm-ppp-llc
[edit]
user@host# set interfaces at-1/0/0 unit 0 vci 2.119
[edit]
user@host# set interfaces at-1/0/0 unit 0 ppp-options pap access-profile jnpr
[edit]
user@host# set interfaces at-1/0/0 unit 0 ppp-options pap local-name locky
[edit]
user@host# set interfaces at-1/0/0 unit 0 ppp-options pap local-password india
[edit]
user@host# set interfaces at-1/0/0 unit 0 family inet unnumbered-address lo0.0
[edit]
user@host# set interfaces at-1/0/0 unit 0 family inet unnumbered-address destination 100.100.100.6
[edit]
user@host# set interfaces lo0 unit 0 family inet address 100.100.100.20/32
[edit]
user@host# set access profile jnpr client sringeri pap-password india
[edit]
user@host# commit
commit complete
```

2. Verify the interface status.

```
user@host# run show interfaces at-1/0/0
Physical interface: at-1/0/0, Enabled, Physical link is Up
  Interface index: 146, SNMP ifIndex: 504
  Link-level type: ATM-PVC, MTU: 1496, Clocking: Internal, ADSL mode,
  Speed: ADSL
  Speed: 832kbps, Loopback: None
  Device flags : Present Running
  Link flags : None
```
CoS queues: 8 supported, 8 maximum usable queues
Current address: 00:b1:7e:85:84:ff
Last flapped: 2009-10-28 22:18:50 PDT (00:19:19 ago)
Input rate: 0 bps (0 pps)
Output rate: 0 bps (0 pps)
ADSL alarms: None
ADSL defects: None
ADSL status:
Modem status: Showtime (Itu-dmt)
DSL mode: Auto Annex A
Last fail code: None
Subfunction: 0x00
Seconds in showtime: 1158

Logical interface at-1/0/0.0 (Index 73) (SNMP ifIndex 523)
Flags: Point-To-Point SNMP-Traps 0x0 Encapsulation: ATM-PPP-LLC
Input packets: 441
Output packets: 342
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive: Input: 53 (00:00:06 ago), Output: 55 (00:00:05 ago)
LCP state: Opened
CHAP state: Closed
PAP state: Success
Security: Zone: HOST
Allowed host-inbound traffic: any-service bfd bgp dvmrp igmp ldp msdp
   nhp ospf pgm pim rip router-discovery rsvp sap vrrp
Protocol inet, MTU: 1486
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
Destination: 100.100.100/24, Local: 100.100.100.20, Broadcast: 100.100.100.255
VCI 2.119
Flags: Active
Total down time: 0 sec, Last down: Never
Input packets: 441
Output packets: 342

Logical interface at-1/0/0.32767 (Index 72) (SNMP ifIndex 525)
Flags: Point-To-Multipoint No-Multicast SNMP-Traps 0x0 Encapsulation: ATM-VCMUX
Input packets: 0
Output packets: 0
Security: Zone: HOST
Allowed host-inbound traffic: any-service bfd bgp dvmrp igmp ldp msdp
   nhp ospf pgm pim rip router-discovery rsvp sap vrrp
VCI 2.4
Flags: Active
Total down time: 0 sec, Last down: Never
Input packets: 0
Output packets: 0

3. Verify the end-to-end data path connectivity.

Example: Configuring the ADSL Interface on SRX Series Services Gateway (CLI)
Configuring PPPoA on the at-x/x/x Interface with Unnumbered IP (CHAP Authentication)

1. Configure the PPPoA on ADSL PHY for "second mile" ATM.

   user@host# set interfaces at-1/0/0 encapsulation atm-pvc
   [edit]
   user@host# set interfaces at-1/0/0 atm-options vpi 2
   [edit]
   user@host# set interfaces at-1/0/0 unit 0 encapsulation atm-ppp-llc
   [edit]
   user@host# set interfaces at-1/0/0 unit 0 vci 2.119
   [edit]
   user@host# set interfaces at-1/0/0 unit 0 ppp-options chap access-profile jnpr
   [edit]
   user@host# set interfaces at-1/0/0 unit 0 ppp-options chap local-name locky
   [edit]
   user@host# set interfaces at-1/0/0 unit 0 family inet unnumbered-address lo0.0
   [edit]
   user@host# set interfaces at-1/0/0 unit 0 family inet unnumbered-address destination 100.100.100.6
   [edit]
   user@host# set interfaces lo0 unit 0 family inet address 100.100.100.10/32
   [edit]
   user@host# set access profile jnpr client sringeri chap-secret india
   [edit]
   user@host# commit
   commit complete

2. Verify the interface status.

   user@host# run show interfaces at-1/0/0
   Physical interface: at-1/0/0, Enabled, Physical link is Up
   Interface index: 146, SNMP ifIndex: 504
   Link-level type: ATM-PVC, MTU: 1496, Clocking: Internal, ADSL mode,
   Speed: ADSL
   Speed: 832kbps, Loopback: None
   Device flags : Present Running
   Link flags : None
   CoS queues : 8 supported, 8 maximum usable queues
   Current address: 00:b1:7e:85:84:ff
   Last flapped : 2009-10-28 22:18:50 PDT (00:37:35 ago)
   Input rate : 0 bps (0 pps)
Output rate : 0 bps (0 pps)
ADSL alarms : None
ADSL defects : None
ADSL status:
  Modem status : Showtime (Itu-dmt)
  DSL mode : Auto Annex A
  Last fail code: None
  Subfunction : 0x00
  Seconds in showtime : 2253

Logical interface at-1/0/0.0 (Index 71) (SNMP ifIndex 523)
  Flags: Point-To-Point SNMP-Traps 0x0 Encapsulation: ATM-PPP-LLC
  Input packets : 36
  Output packets: 35
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 12 (00:00:07 ago), Output: 13 (00:00:05 ago)
  LCP state: Opened
  CHAP state: Success
  PAP state: Closed
  Security: Zone: HOST
  Allowed host-inbound traffic : any-service bfd bgp dvmrp igmp ldp msdp nhp ospf pim rip router-discovery rsvp sap vrrp
  Protocol inet, MTU: 1486
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 100.100.100.6, Local: 100.100.100.10
  VCI 2.119
  Flags: Active
  Total down time: 0 sec, Last down: Never
    Input packets : 36
    Output packets: 35

Logical interface at-1/0/0.32767 (Index 72) (SNMP ifIndex 525)
  Flags: Point-To-Multipoint No-Multicast SNMP-Traps 0x0 Encapsulation: ATM-VCMUX
  Input packets : 0
  Output packets: 0
  Security: Zone: HOST
  Allowed host-inbound traffic : any-service bfd bgp dvmrp igmp ldp msdp nhp ospf pim rip router-discovery rsvp sap vrrp
  VCI 2.4
  Flags: Active
  Total down time: 0 sec, Last down: Never
    Input packets : 0
    Output packets: 0

3. Verify the end-to-end data path connectivity.

user@host# run show interfaces at-1/0/0 terse
Interface               Admin Link Proto    Local                 Remote
at-1/0/0                up    up
at-1/0/0.0              up    up   inet     100.100.100.10      -->
                        100.100.100.6
at-1/0/0.32767          up    up

[edit]
user@host# run ping 100.100.100.6 count 100 rapid
PING 100.100.100.6 (100.100.100.6): 56 data bytes
--- 100.100.100.6 ping statistics ---
100 packets transmitted, 100 packets received, 0% packet loss
round-trip min/avg/max/stddev = 7.881/9.046/15.136/1.697 ms

Configuring PPPoE over ATM on the at-x/x/x Interface with Negotiated IP (PAP Authentication)

1. Configure the Point-to-Point Protocol over Ethernet over Asynchronous Transfer Mode (PPPoE over ATM) on ADSL PHY for "second mile" Ethernet.

   user@host# set interfaces at-1/0/0 encapsulation ethernet-over-atm
   [edit]
   user@host# set interfaces at-1/0/0 atm-options vpi 2
   [edit]
   user@host# set interfaces at-1/0/0 unit 0 vci 2.119
   [edit]
   user@host# set interfaces at-1/0/0 unit 0 encapsulation ppp-over-ether-over-atm-llc
   [edit]
   user@host# set interfaces pp0 unit 0 ppp-options pap access-profile my_prf
   [edit]
   user@host# set interfaces pp0 unit 0 ppp-options pap local-name purple
   [edit]
   user@host# set interfaces pp0 unit 0 ppp-options pap local-password Embe1mpls
   [edit]
   user@host# set interfaces pp0 unit 0 ppp-options pap passive
   [edit]
   user@host# set interfaces pp0 unit 0 pppoe-options underlying-interface at-1/0/0.0
   [edit]
   user@host# set interfaces pp0 unit 0 pppoe-options auto-reconnect 120
   [edit]
   user@host# set interfaces pp0 unit 0 pppoe-options client
   [edit]
   user@host# set interfaces pp0 unit 0 family inet negotiate-address
   [edit]
   user@host# set access profile my_prf authentication-order password
   [edit]
   user@host# set access-profile my_prf
   [edit]
   user@host# commit
   commit complete

2. Verify the interface status.

   user@host# run show interfaces pp0
   Physical interface: pp0, Enabled, Physical link is Up
   Interface index: 128, SNMP ifIndex: 510
   Type: PPPoE, Link-level type: PPPoE, MTU: 1532
   Device flags : Present Running
   Interface flags: Point-To-Point SNMP-Traps
   Link type : Full-Duplex
   Link flags : None
   Input packets : 0
   Output packets: 0
Logical interface pp0.0 (Index 72) (SNMP ifIndex 526)
  Flags: Point-To-Point SNMP-Traps 0x0 Encapsulation: PPPoE
  PPPoE:
    State: SessionUp, Session ID: 63,
    Session AC name: belur, Remote MAC address: 00:90:1a:41:03:c5,
    Configured AC name: None, Service name: None,
    Auto-reconnect timeout: 120 seconds, Idle timeout: Never,
    Underlying interface: at-1/0/0.0 (Index 71)
  Input packets : 464
  Output packets: 241
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 1 (00:39:31 ago), Output: 225 (00:00:08 ago)
  LCP state: Opened
  NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured,
  mpls:
    Not-configured
  CHAP state: Closed
  PAP state: Success
  Security: Zone: Null
  Protocol inet, MTU: 1456
  Flags: Negotiate-Address
  Addresses, Flags: Kernel Is-Preferred Is-Primary

3. Verify the end-to-end data path connectivity.

```
user@host# run show interfaces at-1/0/0 terse
Interface          Admin Link Proto    Local                 Remote
at-1/0/0            up    up
at-1/0/0.0          up    up
at-1/0/0.32767      up    up

[edit]
user@host# run show interfaces pp0 terse
Interface          Admin Link Proto    Local                 Remote
pp0                up    up
pp0.0              up    up inet 12.12.12.15 --> 12.12.12.1

[edit]
user@host# run ping 12.12.12.1 count 100 rapid

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 12.12.12.1 ping statistics ---
100 packets transmitted, 100 packets received, 0% packet loss
round-trip min/avg/max/stddev = 9.369/10.590/16.716/1.660 ms
```

Configuring PPPoE over ATM on the at-x/x/x Interface with Negotiated IP (CHAP Authentication)

1. Configure the Point-to-Point Protocol over Ethernet over Asynchronous Transfer Mode (PPPoE over ATM) on ADSL PHY for "second mile" Ethernet.

```
user@host# set interfaces at-1/0/0 encapsulation ethernet-over-atm
[edit]
user@host# set interfaces at-1/0/0 atm-options vpi 2
[edit]
user@host# set interfaces at-1/0/0 unit 0 vci 2.119
```
2. Verify the interface status.

```
user@host# run show interfaces pp0
Physical interface: pp0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 510
  Type: PPPoE, Link-level type: PPPoE, MTU: 1532
  Device flags : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link type : Full-Duplex
  Link flags : None
    Input packets : 0
    Output packets: 0

Logical interface pp0.0 (Index 70) (SNMP ifIndex 526)
  Flags: Point-To-Point SNMP-Traps 0x0 Encapsulation: PPPoE
  PPPoE:
    State: SessionUp, Session ID: 64,
    Session AC name: belur, Remote MAC address: 00:90:1a:41:03:c5,
    Configured AC name: None, Service name: None,
    Auto-reconnect timeout: 120 seconds, Idle timeout: Never,
    Underlying interface: at-1/0/0.0 (Index 71)
    Input packets : 14
    Output packets: 13
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 0 (never), Output: 7 (00:00:08 ago)
  LCP state: Opened
  NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured,
  mpls: Not-configured
  CHAP state: Success
  Security: Zone: Null
  Protocol inet, MTU: 1456
  Flags: Negotiate-Address
  Addresses, Flags: Kernel Is-Preferred Is-Primary
```

3. Verify the end-to-end data path connectivity.
user@host# run show interfaces at-1/0/0 terse
Interface           Admin Link Proto    Local   Remote
at-1/0/0             up      up
at-1/0/0.0           up      up
at-1/0/0.32767       up      up

[edit]
user@host# run show interfaces pp0 terse
Interface           Admin Link Proto    Local   Remote
pp0                 up      up
pp0.0               up      up   inet  12.12.12.16 -->
12.12.12.1

[edit]
user@host# run ping 12.12.1 count 1000 rapid

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 12.12.1 ping statistics ---
1000 packets transmitted, 1000 packets received, 0% packet loss
round-trip min/avg/max/stddev = 8.748/10.461/21.386/1.915 ms

[edit]
user@host#
Chapter 8

Configuring 2-Port 10 Gigabit Ethernet XPIM

Before You Begin on page 227
- Configuring the 2-Port 10 Gigabit Ethernet XPIM Interface (CLI Procedure) on page 227
- Configuring the 2-Port 10 Gigabit Ethernet XPIM Interface (J-Web Procedure) on page 230
- Verifying the 2-Port 10 Gigabit Ethernet XPIM Configuration on page 233

Before You Begin

Before you begin configuring the 2-Port 10 Gigabit Ethernet XPIM, complete the following tasks:
- Establish basic connectivity. See the Getting Started Guide for your device.
- If you do not already have a basic understanding of physical and logical interfaces and Juniper Networks interface conventions, read “2-Port 10 Gigabit Ethernet XPIM Overview” on page 47.
- Configure network interfaces as necessary. See “Configuring Ethernet, DS1, DS3, and Serial Interfaces” on page x.

Configuring the 2-Port 10 Gigabit Ethernet XPIM Interface (CLI Procedure)

To perform basic configuration for the 2-Port 10 Gigabit Ethernet XPIM and configure network interfaces for the services gateway with the CLI:
1. Navigate to the top of the interface configuration hierarchy in the CLI configuration editor.
2. Perform the configuration tasks described in Table 48 on page 228.
3. Once you have completed configuring the device, commit the configuration.
4. To check the configuration, see “Verifying the 2-Port 10 Gigabit Ethernet XPIM Configuration” on page 233.
NOTE: The following format is used to represent the 2-Port 10 Gigabit Ethernet XPIM:

\[ \text{type-fpc/pic/port} \]

- **type** — Media type (xe)
- **fpc** — Number of the Flexible PIC Concentrator (FPC) card on which the physical interface is located (6 or 2)
- **pic** — Number of the PIC on which the physical interface is located (0)
- **port** — Specific port on a PIC (0 or 1)

Example: xe-6/0/0 or xe-2/0/0

---

**Table 48: Configuring the 2-Port 10 Gigabit Ethernet XPIM Using the CLI**

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the operating mode.</td>
<td>From the [edit] hierarchy level, enter&lt;br&gt;set interfaces xe-x/x/x media-type&lt;br&gt;Example: set interfaces xe-6/0/0 media-type copper&lt;br&gt;set interfaces xe-6/0/0 media-type fiber</td>
<td>Specifies the operating modes for the 2-Port 10 Gigabit Ethernet XPIM.&lt;br&gt;The following operating modes are available:&lt;br&gt;• Copper&lt;br&gt;• Fiber&lt;br&gt;The 2-Port 10 Gigabit Ethernet XPIM can be configured to operate in two-copper mode, two-fiber mode, or mixed mode (one copper and one fiber).</td>
</tr>
<tr>
<td>Set the operating speed for XPIM.</td>
<td>From the [edit] hierarchy level, enter&lt;br&gt;set interfaces xe-x/x/x speed&lt;br&gt;Example: set interfaces xe-6/0/0 speed 100m&lt;br&gt;set interfaces xe-6/0/0 speed 10g&lt;br&gt;set interfaces xe-6/0/0 speed 1g&lt;br&gt;set interfaces xe-6/0/0 speed 10m</td>
<td>Specifies the operating speed for the 2-Port 10 Gigabit Ethernet XPIM.&lt;br&gt;The following link speeds are supported:&lt;br&gt;• 100m — Sets the link speed to 100 Mbps.&lt;br&gt;• 10g — Sets the link speed to 10 Gbps.&lt;br&gt;• 10m — Sets the link speed to 10 Mbps.&lt;br&gt;• 1g — Sets the link speed to 1 Gbps.</td>
</tr>
</tbody>
</table>
### Table 48: Configuring the 2-Port 10 Gigabit Ethernet XPIM Using the CLI (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add the logical interface.</td>
<td>From the [edit] hierarchy level, enter</td>
<td>Defines one or more logical units that you can connect to the 2-Port 10 Gigabit Ethernet XPIM.</td>
</tr>
<tr>
<td></td>
<td>set interfaces xe-x/y/x unit unit number family inet</td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>set interfaces xe-6/0/1 unit 0 family inet</td>
<td></td>
</tr>
<tr>
<td>Assign MTU values.</td>
<td>From the [edit] hierarchy level, enter</td>
<td>Specifies the maximum transmission unit size for the 2-Port 10 Gigabit Ethernet XPIM.</td>
</tr>
<tr>
<td></td>
<td>set interfaces xe-x/y/x unit 0 family inet mtu mtu values</td>
<td>Enter a value from 256 through 9216. The default MTU for Gigabit Ethernet interfaces is 1514.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set interfaces xe-6/0/0 unit 0 family inet mtu 1514</td>
<td></td>
</tr>
<tr>
<td>Set link options.</td>
<td>From the [edit] hierarchy level, enter</td>
<td>Sets the link settings for the 2-Port 10 Gigabit Ethernet XPIM with the following options:</td>
</tr>
<tr>
<td></td>
<td>set interfaces xe-x/y/x gigether-options</td>
<td>■ 802.3ad — Specifies an aggregated Ethernet bundle.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>■ auto-negotiation — Enables auto-negotiation of flow control, link mode, and speed.</td>
</tr>
<tr>
<td></td>
<td>set interfaces xe-6/0/0 gigether-options</td>
<td>■ loopback — Enables loopback.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ no auto-negotiation — Disables auto-negotiation of flow control, link mode, and speed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ no loopback — Disables loopback.</td>
</tr>
<tr>
<td>Enable and disabling the interface.</td>
<td>From the [edit] hierarchy level, enter</td>
<td>Enables or disables the 2-Port 10 Gigabit Ethernet XPIM.</td>
</tr>
<tr>
<td></td>
<td>set interfaces xe-x/y/x disable/enable</td>
<td>By default, the interfaces on the ports on the uplink module installed in services gateways are</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>enabled. You can disable the interfaces using a CLI command.</td>
</tr>
<tr>
<td></td>
<td>■ set interfaces xe-6/0/0 disable</td>
<td>If an interface on the uplink module is disabled, you can enable the interface using a CLI command.</td>
</tr>
<tr>
<td></td>
<td>■ set interfaces xe-6/0/0 Enable</td>
<td></td>
</tr>
</tbody>
</table>
Configuring the 2-Port 10 Gigabit Ethernet XPIM Interface (J-Web Procedure)

To perform basic configuration for the 2-Port 10 Gigabit Ethernet XPIM and configure network interfaces for the services gateway with J-Web:

1. In the J-Web interface, select **Configure > Interfaces**.
   A list of the network interfaces present on the device is displayed.

2. Select the interface name (**xe-2/0/1** or **xe-6/0/0**) to edit.

3. Enter information into the configuration pages, as described in Table 49 on page 230.

4. From the configuration main page, click one of the following buttons:
   - Click **OK** to save changes.
   - Click **Cancel** to cancel your entries and return to the previous page.
   - Click **Commit** to apply the configuration and other pending changes (if any).
   - Click **Discard** to discard pending changes.

5. To verify the configuration, see “Verifying the 2-Port 10 Gigabit Ethernet XPIM Configuration” on page 233.

Table 49: Configuring the 2-Port 10 Gigabit Ethernet XPIM Using J-Web

<table>
<thead>
<tr>
<th>Field</th>
<th>Your Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logical Interfaces</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add logical interfaces</td>
<td>Click <strong>Add</strong></td>
<td>Defines one or more logical units that you connect to this physical Gigabit Ethernet interface. You must define at least one logical unit for a Gigabit Ethernet interface.</td>
</tr>
<tr>
<td><strong>Logical Interface</strong></td>
<td>Enter logical interface description</td>
<td>Describes the logical interface.</td>
</tr>
<tr>
<td><strong>IPv4 Addresses</strong></td>
<td>1. Type one or more IPv4 addresses and prefixes.</td>
<td>Specifies one or more IPv4 addresses for the interface.</td>
</tr>
<tr>
<td><strong>Prefixes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For example: 10.10.10.10/24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Add</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>OK</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Source Addresses and Prefixes</strong> box, then click <strong>Delete</strong></td>
<td></td>
</tr>
</tbody>
</table>

To delete an IP address and prefix, select them in the **Source Addresses and Prefixes** box, then click **Delete**.
Table 49: Configuring the 2-Port 10 Gigabit Ethernet XPIM Using J-Web (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Your Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP Address</td>
<td>Type an IPv4 address that you want to associate with the media access control (MAC) address—for example, 10.10.10.1.</td>
<td>Enables the device to create a static Address Resolution Protocol (ARP) entry for this interface by specifying the IP address of a node to associate with its MAC address. The IP address must be in the same subnet as the IPv4 address or prefix of the interface you are configuring. Static ARP entries associate the IP addresses and MAC addresses of nodes on the same subnet, enabling a device to respond to ARP requests having destination addresses that are not local to the incoming interface.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Type the MAC address to be mapped to the ARP entry—for example, 00:12:1E:A9:8A:80.</td>
<td>Specifies the hardware MAC address associated with the ARP address. The MAC address uniquely identifies the system and is expressed in the following format: mm:nn:mm:ss:ss:ss. The first three octets denote the hardware manufacturer ID, and the last three are serial numbers identifying the device.</td>
</tr>
<tr>
<td>Publish</td>
<td>To enable publishing, select the check box. To disable publishing, clear the check box.</td>
<td>Enables the device to reply to ARP requests for the specified address.</td>
</tr>
<tr>
<td>Enable Ethernet Switching</td>
<td>To enable Ethernet switching, select the check box. To disable Ethernet switching, clear the check box.</td>
<td>Enables or disables Ethernet switching.</td>
</tr>
<tr>
<td>Port Mode</td>
<td>Select one of the following: Trunk, Access</td>
<td>Specifies the mode of operation for the port.</td>
</tr>
<tr>
<td>Native VLAN Id</td>
<td>Enter a valid VLAN name or VLAN tag.</td>
<td>VLAN identifier to associate with untagged packets received on the interface.</td>
</tr>
<tr>
<td>Physical Interface Description (Optional)</td>
<td>Type a text description of the Gigabit Ethernet interface to more clearly identify it in monitoring displays.</td>
<td>Adds supplementary information about the physical Gigabit Ethernet interface.</td>
</tr>
<tr>
<td>MTU (bytes)</td>
<td>Type a value between 256 and 9216 bytes. Default MTU: 1514</td>
<td>Specifies the maximum transmission unit (MTU) size for the Gigabit Ethernet interface.</td>
</tr>
</tbody>
</table>
Table 49: Configuring the 2-Port 10 Gigabit Ethernet XPIM Using J-Web (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Your Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per unit scheduler</td>
<td>To enable scheduling, select the check box.</td>
<td>Enables scheduling on logical interfaces. This option allows you to configure multiple output queues on a logical interface and associate an output scheduler and shaping rate with the queues.</td>
</tr>
<tr>
<td></td>
<td>To disable scheduling, clear the check box.</td>
<td></td>
</tr>
<tr>
<td>Framing Mode</td>
<td>Select one of the following:</td>
<td>Specifies the framing mode.</td>
</tr>
<tr>
<td></td>
<td>LAN-mode</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WAN-mode</td>
<td></td>
</tr>
<tr>
<td>Loopback Mode</td>
<td>Select one of the following:</td>
<td>Specifies the loopback mode.</td>
</tr>
<tr>
<td></td>
<td>Local</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Remote</td>
<td></td>
</tr>
<tr>
<td>Path Trace</td>
<td>Enter a text string.</td>
<td>Identifies the circuit.</td>
</tr>
<tr>
<td>Gigabit Ethernet Options</td>
<td>Select Yes to enable the loopback diagnostic option.</td>
<td>Enables or disables the loopback option.</td>
</tr>
<tr>
<td></td>
<td>Select No to disable the loopback option. By default, loopback is disabled.</td>
<td></td>
</tr>
<tr>
<td>Auto Negotiation</td>
<td>Select Yes to enable autonegotiation.</td>
<td>Enables or disables autonegotiation. By default, Gigabit Ethernet interfaces autonegotiate the link mode and speed settings. If you disable autonegotiation and do not manually configure link mode and speed, the link is negotiated at 1000 Mbps, full duplex. When you configure both the link mode and the speed, the link negotiates with the manually configured settings whether autonegotiation is enabled or disabled.</td>
</tr>
<tr>
<td></td>
<td>Select No to disable autonegotiation. By default, autonegotiation is enabled.</td>
<td></td>
</tr>
<tr>
<td>Auto Negotiation Remote Fault</td>
<td>Select the autonegotiation remote fault value from the list of options given.</td>
<td>Indicates the autonegotiation remote fault value.</td>
</tr>
<tr>
<td></td>
<td>local-interface-offline</td>
<td>This field is enabled only if autonegotiation is enabled.</td>
</tr>
<tr>
<td></td>
<td>local-interface-offline</td>
<td></td>
</tr>
</tbody>
</table>
Table 49: Configuring the 2-Port 10 Gigabit Ethernet XPIM Using J-Web (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Your Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source MAC Address Filters</td>
<td>To add MAC addresses, type them in the boxes above the Add button, then click Add.</td>
<td>Displays the list of MAC addresses from which you want to receive packets on this interface. To delete a MAC address, select it in the Source Addresses box, then click Delete.</td>
</tr>
<tr>
<td>Redundant Parent</td>
<td>Enter a redundant Ethernet interface name.</td>
<td>Specifies the name of the redundant Ethernet interface that a physical interface is associated with to form a redundant Ethernet interface pair.</td>
</tr>
<tr>
<td>802.3ad</td>
<td>Enter an aggregated Ethernet logical interface name.</td>
<td>Enables you to group Ethernet interfaces at the Physical Layer to form a single link layer interface.</td>
</tr>
<tr>
<td>Tag Protocol ID</td>
<td>Enter standard Tag Protocol Identifier (TPID) values.</td>
<td>Identifies the frame as an IEEE 802.1Q-tagged frame.</td>
</tr>
<tr>
<td>MAC Learning</td>
<td>Select Yes to enable MAC Learning.</td>
<td>Enables or disabling dynamic source MAC addresses.</td>
</tr>
<tr>
<td></td>
<td>Select No to disable MAC Learning.</td>
<td></td>
</tr>
</tbody>
</table>

NOTE: You can configure the operating mode options (copper and fiber) and speed options for the 2-Port 10 Gigabit Ethernet XPIM in Point and Click CLI option of J-Web interface.

To set the operating mode and speed in Point and Click CLI:

1. Navigate to Configure > CLI tools > Point and Click CLI.
2. Click and expand interfaces field under Configuration.
3. Select the interface name (xe-2/0/1 or xe-6/0/0) to edit.
4. Select Media type to set the operating mode and select Speed to set the operating speed for the 2-Port 10 Gigabit Ethernet XPIM.

Verifying the 2-Port 10 Gigabit Ethernet XPIM Configuration

Purpose: Verify the 2-Port 10 Gigabit Ethernet XPIM default configuration and settings:

Action:
1. Check if the 2-Port 10 Gigabit Ethernet XPIM is installed on the services gateway by entering show chassis hardware command.

The output should display the following values:
- FPC 2, PIC 0 – 2x 10G gPIM
- FPC 6, PIC 0 – 2x 10G gPIM

Sample output:

<table>
<thead>
<tr>
<th>Item</th>
<th>Version</th>
<th>Part number</th>
<th>Serial number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis</td>
<td></td>
<td></td>
<td>AJ0309AC0047</td>
<td>SRX650</td>
</tr>
<tr>
<td>Midplane</td>
<td>REV 04</td>
<td>710-023875</td>
<td>TV3993</td>
<td></td>
</tr>
<tr>
<td>System IO</td>
<td>REV 04</td>
<td>710-023209</td>
<td>TV4035</td>
<td>SRXSM System IO</td>
</tr>
<tr>
<td>Routing Engine</td>
<td>REV 01</td>
<td>710-023224</td>
<td>DTS109</td>
<td>RE-SRXSME-SRE6</td>
</tr>
<tr>
<td>FPC 0</td>
<td></td>
<td></td>
<td></td>
<td>FPC</td>
</tr>
<tr>
<td>PIC 0</td>
<td></td>
<td></td>
<td></td>
<td>4x GE Base PIC</td>
</tr>
<tr>
<td>FPC 2</td>
<td></td>
<td></td>
<td></td>
<td>FPC</td>
</tr>
<tr>
<td>PIC 0</td>
<td></td>
<td></td>
<td></td>
<td>2x 10G gPIM</td>
</tr>
<tr>
<td>FPC 6</td>
<td></td>
<td></td>
<td></td>
<td>FPC</td>
</tr>
<tr>
<td>PIC 0</td>
<td></td>
<td></td>
<td></td>
<td>2x 10G gPIM</td>
</tr>
<tr>
<td>Power Supply 0</td>
<td>REV 01</td>
<td>740-024283</td>
<td>TA00049WSSSS</td>
<td>PS 645W AC</td>
</tr>
</tbody>
</table>

2. Verify the FPC status by entering the `show chassis fpc` command. The output should display FPC status as online.

Sample output:

<table>
<thead>
<tr>
<th>Slot</th>
<th>State</th>
<th>Temp</th>
<th>CPU Utilization (%)</th>
<th>Memory Utilization (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Online</td>
<td>-----</td>
<td>---------------------</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Empty</td>
<td></td>
<td>CPU less FPC</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Online</td>
<td>-----</td>
<td>CPU less FPC</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Online</td>
<td>-----</td>
<td>CPU less FPC</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Empty</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** The 2-Port 10 Gigabit Ethernet XPIM is installed in the second and sixth slot of the SRX650 device chassis; therefore the FPC used here is fpc 2 and fpc 6.

3. Enter `run show interface xe-6/0/0` command and verify the following information in the command output:

- Physical interface — xe-6/0/0, Enabled, Physical link is Up
- MTU — 1514, Link-mode: Full-duplex,
- Speed — 10Gbps
- Loopback — Disabled
- Flow control — Enabled

Sample output

Physical interface: xe-6/0/0, Enabled, Physical link is Up
  Interface index: 144, SNMP ifIndex: 501
  Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, Speed: 10Gbps,
  BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled
  Device flags: Present Running
  Interface flags: SNMP-Traps Internal: 0x0
  Link flags: None
  CoS queues: 8 supported, 8 maximum usable queues
  Current address: 00:1f:12:e0:80:a8, Hardware address: 00:1f:12:e0:80:a8

  Last flapped: 1970-01-01 00:34:22 PST (07:26:29 ago)
  Input rate: 0 bps (0 pps)
  Output rate: 0 bps (0 pps)
  Active alarms: None
  Active defects: None

Logical interface xe-6/0/0.0 (Index 72) (SNMP ifIndex 503)
  Flags: SNMP-Traps Encapsulation: ENET2
  Input packets: 25
  Output packets: 25
  Security: Zone: HOST
  Allowed host-inbound traffic: any-service bfd bgp dvmrp igmp ldp msdp nhrp
  ospf pgm pim rip router-discovery rsvp sap vrrp
  Protocol inet, MTU: 1500
  Flags: Sendicast-pkt-to-re
  Addresses, Flags: Is-Preferred Is-Primary
  Destination: 10.10.10.24, Local: 10.10.10.10, Broadcast: 10.10.10.255
Chapter 9
Voice over Internet Protocol with Avaya

J2320, J2350, J4350, and J6350 Services Routers support voice over IP (VoIP) connectivity for branch offices with the Avaya IG550 Integrated Gateway. The Avaya IG550 Integrated Gateway consists of four VoIP modules—a TGM550 Telephony Gateway Module and three types of Telephony Interface Modules (TIMs).

The VoIP modules installed in a Services Router at a branch office connect the IP and analog telephones and trunk lines at the branch to headquarters and to the public-switched telephone network (PSTN).

You can use either J-Web Quick Configuration or a configuration editor to configure VoIP on the Services Router. Alternatively, you can download a complete router configuration that includes VoIP from an Electronic Preinstallation Worksheet (EPW) and a Disk-on-Key USB memory stick.

For information about which devices support the features documented in this chapter, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.

This chapter contains the following topics:
- Console and Connector Port Pinouts on page 238
- Avaya VoIP Modules on page 244
- VoIP Terms on page 257
- VoIP Overview on page 259
- Before You Begin on page 267
- Configuring VoIP Interfaces with EPW and Disk-on-Key on page 268
- Configuring VoIP Interfaces with Quick Configuration on page 269
- Configuring VoIP with a Configuration Editor on page 272
- Accessing and Administering the TGM550 CLI on page 278
- Verifying the VoIP Configuration on page 283
- Frequently Asked Questions About the VoIP Interface on page 286
Console and Connector Port Pinouts

The Avaya VoIP modules supported on the Services Router accept different kinds of network cables.

- TGM550 Console Port Pinouts on page 238
- TGM550 RJ-11 Connector Pinout for Analog Ports on page 239
- TIM508 Connector Pinout on page 239
- TIM510 RJ-45 Connector Pinout on page 240
- TIM514 Connector Pinout on page 240
- TIM516 Connector Pinout on page 241
- TIM518 Connector Pinout on page 242

**TGM550 Console Port Pinouts**

The console port on a TGM550 Telephony Gateway Module has an RJ-45 connector. Table 50 on page 238 provides TGM550 RJ-45 console connector pinout information. An RJ-45 cable is supplied with the TGM550.

**NOTE:** Two different RJ-45 cables and RJ-45 to DB-9 adapters are provided. Do not use the RJ-45 cable and adapter for the Services Router console port to connect to the TGM550 console port.

To connect the console port to an external management device, you need an RJ-45 to DB-9 serial port adapter, which is also supplied with the TGM550.

**Table 50: TGM550 RJ-45 Console Connector Pinouts**

<table>
<thead>
<tr>
<th>TGM550 RJ-45 Pin</th>
<th>Signal</th>
<th>Terminal DB-9 Pins</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>For future use</td>
<td>NC</td>
</tr>
<tr>
<td>2</td>
<td>TXD (TGM550 input)</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>RXD (TGM550 output)</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>CD</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>GND</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>DTR</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>RTS</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>CTS</td>
<td>7</td>
</tr>
</tbody>
</table>
**TGM550 RJ-11 Connector Pinout for Analog Ports**

The two analog telephone ports and two analog trunk ports on the TGM550 use an RJ-11 cable. Table 51 on page 239 describes the TGM550 RJ-11 connector pinout.

<table>
<thead>
<tr>
<th>Pin</th>
<th>Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No connection</td>
</tr>
<tr>
<td>2</td>
<td>No connection</td>
</tr>
<tr>
<td>3</td>
<td>Ring</td>
</tr>
<tr>
<td>4</td>
<td>Tip</td>
</tr>
<tr>
<td>5</td>
<td>No connection</td>
</tr>
<tr>
<td>6</td>
<td>No connection</td>
</tr>
</tbody>
</table>

**TIM508 Connector Pinout**

The TIM508 Analog Telephony Interface Module uses a B25A unshielded 25-pair Amphenol cable. Table 52 on page 239 describes the TIM508 connector pinout.

<table>
<thead>
<tr>
<th>Pin</th>
<th>Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tip</td>
</tr>
<tr>
<td>2</td>
<td>Tip</td>
</tr>
<tr>
<td>3</td>
<td>Tip</td>
</tr>
<tr>
<td>4</td>
<td>Tip</td>
</tr>
<tr>
<td>5</td>
<td>Tip</td>
</tr>
<tr>
<td>6</td>
<td>Tip</td>
</tr>
<tr>
<td>7</td>
<td>Tip</td>
</tr>
<tr>
<td>8</td>
<td>Tip</td>
</tr>
<tr>
<td>26</td>
<td>R - Receive</td>
</tr>
<tr>
<td>27</td>
<td>Ring</td>
</tr>
<tr>
<td>28</td>
<td>Ring</td>
</tr>
</tbody>
</table>
**Table 52: TIM508 Connector Pinout (continued)**

<table>
<thead>
<tr>
<th>Pin</th>
<th>Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>Ring</td>
</tr>
<tr>
<td>30</td>
<td>Ring</td>
</tr>
<tr>
<td>31</td>
<td>Ring</td>
</tr>
<tr>
<td>32</td>
<td>Ring</td>
</tr>
<tr>
<td>33</td>
<td>Ring</td>
</tr>
</tbody>
</table>

**TIM510 RJ-45 Connector Pinout**

The TIM510 Telephony Interface Module uses an RJ-45 cable. Table 53 on page 240 describes the TIM510 RJ-45 connector pinout.

**Table 53: TIM510 RJ-45 Connector Pinout**

<table>
<thead>
<tr>
<th>Pin</th>
<th>Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ring</td>
</tr>
<tr>
<td>2</td>
<td>Tip</td>
</tr>
<tr>
<td>3</td>
<td>No connection</td>
</tr>
<tr>
<td>4</td>
<td>R1 - Transmit</td>
</tr>
<tr>
<td>5</td>
<td>T1 - Transmit</td>
</tr>
<tr>
<td>6</td>
<td>No connection</td>
</tr>
<tr>
<td>7</td>
<td>No connection</td>
</tr>
<tr>
<td>8</td>
<td>No connection</td>
</tr>
</tbody>
</table>

**TIM514 Connector Pinout**

The TIM514 Telephony Interface Module uses an RJ-11 cable. Table 54 on page 240 describes the TIM514 RJ-11 connector pinout information.

**Table 54: TIM514 RJ-11 Connector Pinout**

<table>
<thead>
<tr>
<th>Pin</th>
<th>Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No connection</td>
</tr>
<tr>
<td>2</td>
<td>No connection</td>
</tr>
</tbody>
</table>
### Table 54: TIM514 RJ-11 Connector Pinout (continued)

<table>
<thead>
<tr>
<th>Pin</th>
<th>Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Ring</td>
</tr>
<tr>
<td>4</td>
<td>Tip</td>
</tr>
<tr>
<td>5</td>
<td>No connection</td>
</tr>
<tr>
<td>6</td>
<td>No connection</td>
</tr>
</tbody>
</table>

### TIM516 Connector Pinout

The TIM516 Analog Telephony Interface Module uses a B25A unshielded 25-pair Amphenol cable. Table 55 on page 241 describes the TIM516 connector pinout.

### Table 55: TIM516 Connector Pinout

<table>
<thead>
<tr>
<th>Pin</th>
<th>Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tip</td>
</tr>
<tr>
<td>2</td>
<td>Tip</td>
</tr>
<tr>
<td>3</td>
<td>Tip</td>
</tr>
<tr>
<td>4</td>
<td>Tip</td>
</tr>
<tr>
<td>5</td>
<td>Tip</td>
</tr>
<tr>
<td>6</td>
<td>Tip</td>
</tr>
<tr>
<td>7</td>
<td>Tip</td>
</tr>
<tr>
<td>8</td>
<td>Tip</td>
</tr>
<tr>
<td>17</td>
<td>Tip</td>
</tr>
<tr>
<td>18</td>
<td>Tip</td>
</tr>
<tr>
<td>19</td>
<td>Tip</td>
</tr>
<tr>
<td>20</td>
<td>Tip</td>
</tr>
<tr>
<td>21</td>
<td>Tip</td>
</tr>
<tr>
<td>22</td>
<td>Tip</td>
</tr>
<tr>
<td>23</td>
<td>Tip</td>
</tr>
<tr>
<td>24</td>
<td>Tip</td>
</tr>
<tr>
<td>26</td>
<td>Ring</td>
</tr>
</tbody>
</table>
### Table 55: TIM516 Connector Pinout (continued)

<table>
<thead>
<tr>
<th>Pin</th>
<th>Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>Ring</td>
</tr>
<tr>
<td>28</td>
<td>Ring</td>
</tr>
<tr>
<td>29</td>
<td>Ring</td>
</tr>
<tr>
<td>30</td>
<td>Ring</td>
</tr>
<tr>
<td>31</td>
<td>Ring</td>
</tr>
<tr>
<td>32</td>
<td>Ring</td>
</tr>
<tr>
<td>33</td>
<td>Ring</td>
</tr>
<tr>
<td>42</td>
<td>Ring</td>
</tr>
<tr>
<td>43</td>
<td>Ring</td>
</tr>
<tr>
<td>44</td>
<td>Ring</td>
</tr>
<tr>
<td>45</td>
<td>Ring</td>
</tr>
<tr>
<td>46</td>
<td>Ring</td>
</tr>
<tr>
<td>47</td>
<td>Ring</td>
</tr>
<tr>
<td>48</td>
<td>Ring</td>
</tr>
<tr>
<td>49</td>
<td>Ring</td>
</tr>
</tbody>
</table>

### TIM518 Connector Pinout

The TIM518 Analog Telephony Interface Module uses a B25A unshielded 25-pair Amphenol cable. Table 56 on page 242 describes the TIM518 connector pinout.

### Table 56: TIM518 Connector Pinout

<table>
<thead>
<tr>
<th>Pin</th>
<th>Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ring</td>
</tr>
<tr>
<td>2</td>
<td>Ring</td>
</tr>
<tr>
<td>3</td>
<td>Ring</td>
</tr>
<tr>
<td>4</td>
<td>Ring</td>
</tr>
<tr>
<td>5</td>
<td>Ring</td>
</tr>
<tr>
<td>6</td>
<td>Ring</td>
</tr>
</tbody>
</table>
### Table 56: TIM518 Connector Pinout (continued)

<table>
<thead>
<tr>
<th>Pin</th>
<th>Signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Ring</td>
</tr>
<tr>
<td>8</td>
<td>Ring</td>
</tr>
<tr>
<td>17</td>
<td>Ring</td>
</tr>
<tr>
<td>18</td>
<td>Ring</td>
</tr>
<tr>
<td>19</td>
<td>Ring</td>
</tr>
<tr>
<td>20</td>
<td>Ring</td>
</tr>
<tr>
<td>21</td>
<td>Ring</td>
</tr>
<tr>
<td>22</td>
<td>Ring</td>
</tr>
<tr>
<td>23</td>
<td>Ring</td>
</tr>
<tr>
<td>24</td>
<td>Ring</td>
</tr>
<tr>
<td>26</td>
<td>Tip</td>
</tr>
<tr>
<td>27</td>
<td>Tip</td>
</tr>
<tr>
<td>28</td>
<td>Tip</td>
</tr>
<tr>
<td>29</td>
<td>Tip</td>
</tr>
<tr>
<td>30</td>
<td>Tip</td>
</tr>
<tr>
<td>31</td>
<td>Tip</td>
</tr>
<tr>
<td>32</td>
<td>Tip</td>
</tr>
<tr>
<td>33</td>
<td>—</td>
</tr>
<tr>
<td>42</td>
<td>Tip</td>
</tr>
<tr>
<td>43</td>
<td>Tip</td>
</tr>
<tr>
<td>44</td>
<td>—</td>
</tr>
<tr>
<td>45</td>
<td>Tip</td>
</tr>
<tr>
<td>46</td>
<td>Tip</td>
</tr>
<tr>
<td>47</td>
<td>Tip</td>
</tr>
<tr>
<td>48</td>
<td>Tip</td>
</tr>
<tr>
<td>49</td>
<td>Tip</td>
</tr>
</tbody>
</table>
Avaya VoIP Modules

The Avaya VoIP modules are installed in a J Series chassis like Physical Interface Modules (PIMs), but they are controlled by Avaya Communication Manager software rather than JUNOS Software.

CAUTION: PIMs and VoIP modules are not hot-swappable. You must power off the Services Router before removing or inserting a PIM or VoIP module. Ensure that the PIMs and VoIP modules are installed in the router chassis before booting up the system.

CAUTION: The grounding cable for J Series devices must be, at minimum, 14 AWG cable.

Avaya VoIP modules are described in the following sections:

- Avaya VoIP Module Summary on page 244
- TGM550 Telephony Gateway Module on page 247
- TIM508 Analog Telephony Interface Module on page 250
- TIM510 E1/T1 Telephony Interface Module on page 251
- TIM514 Analog Telephony Interface Module on page 253
- TIM516 Analog Telephony Interface Module on page 254
- TIM518 Analog Telephony Interface Module on page 255
- TIM521 BRI Telephony Interface Module on page 256

Avaya VoIP Module Summary

Table 57 on page 245 and Table 58 on page 246 provide the module names, software release information, slot and port numbers, maximum number allowed on a chassis, and sample interface names (where applicable) for the Avaya VoIP modules.

CAUTION: Do not install a combination of PIMs in a single chassis that exceeds the maximum power and heat capacity of the chassis. If power management is enabled, PIMs that exceed the maximum power and heat capacity remain offline for a J Series device when the chassis is powered on.

On each J Series device with Avaya VoIP, a single TGM550 Telephony Gateway Module (TGM) and at least one telephony interface module (TIM) is required. No more than four TIMs of any kind can be installed on a single chassis.
## Table 57: J2320 and J2350 Avaya VoIP Module Summary

<table>
<thead>
<tr>
<th>PIM</th>
<th>Also Called</th>
<th>Slot and Port Numbering</th>
<th>Maximum Number on a Chassis</th>
<th>Sample Interface Name (type-pim/0/port)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TGM550 Telephony Gateway Module</td>
<td>TGM550 Gateway Module</td>
<td>J2320—Slots 1 through 3</td>
<td>One (required)</td>
<td>vp-3/0/0</td>
</tr>
<tr>
<td></td>
<td>TGM550</td>
<td>J2350—Slots 1 through 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If more than one TGM550 is installed, only the one in the lowest-numbered slot is enabled. For example, if TGM550s are installed in slots 2 and 3, only the one in slot 2 is enabled.</td>
<td></td>
</tr>
<tr>
<td>TIM508 Analog Telephony Interface Module</td>
<td>TIM508 media module</td>
<td>J2320—Slots 1 through 3</td>
<td>One on J2320</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>TIM508</td>
<td>J2350—Slots 1 through 5</td>
<td>Three on J2350</td>
<td></td>
</tr>
<tr>
<td>TIM510 E1/T1 Telephony Interface Module</td>
<td>TIM510 E1/T1 media module</td>
<td>J2320—Slots 1 through 3</td>
<td>Two</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>TIM510</td>
<td>J2350—Slots 1 through 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TIM514 Analog Telephony Interface Module</td>
<td>TIM514 analog media module</td>
<td>J2320—Slots 1 through 3</td>
<td>Two</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>TIM514</td>
<td>J2350—Slots 1 through 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TIM516 Analog Telephony Interface Module</td>
<td>TIM516 analog media module</td>
<td>J2320—Slots 1 through 3</td>
<td>One on J2320</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>TIM516</td>
<td>J2350—Slots 1 through 5</td>
<td>Three on J2350</td>
<td></td>
</tr>
<tr>
<td>TIM518 Analog Telephony Interface Module</td>
<td>TIM518 analog media module</td>
<td>J2320—Slots 1 through 3</td>
<td>One on J2320</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>TIM518</td>
<td>J2350—Slots 1 through 5</td>
<td>Three on J2350</td>
<td></td>
</tr>
<tr>
<td>TIM521 BRI Telephony Interface Module</td>
<td>TIM521 BRI media module</td>
<td>J2320—Slots 1 through 3</td>
<td>Two</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>TIM521</td>
<td>J2350—Slots 1 through 5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 58: J4350 and J6350 Avaya VoIP Module Summary

<table>
<thead>
<tr>
<th>PIM</th>
<th>Also Called</th>
<th>Slot and Port Numbering</th>
<th>Maximum Number on a Chassis</th>
<th>Sample Interface Name (type-pim/0/port)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TGM550 Gateway Module</td>
<td>TGM550 Gateway Module</td>
<td>Slots 1 through 6</td>
<td>One (required) If more than one TGM550 is installed, only the one in the lowest-numbered slot is enabled. For example, if TGM550s are installed in slots 2 and 3, only the one in slot 2 is enabled.</td>
<td>vp-3/0/0</td>
</tr>
<tr>
<td>- TGM550</td>
<td>TGM550</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TIM508 Analog Telephony Module</td>
<td>TIM508 media module</td>
<td>Slots 1 through 6</td>
<td>Three</td>
<td>–</td>
</tr>
<tr>
<td>- TIM508</td>
<td>TIM508</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TIM510 E1/T1 Module</td>
<td>TIM510 E1/T1 media module</td>
<td>Slots 1 through 6</td>
<td>Two</td>
<td>–</td>
</tr>
<tr>
<td>- TIM510</td>
<td>TIM510</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TIM514 Analog Module</td>
<td>TIM514 analog media module</td>
<td>Slots 1 through 6</td>
<td>Four</td>
<td>–</td>
</tr>
<tr>
<td>- TIM514</td>
<td>TIM514</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TIM516 Analog Module</td>
<td>TIM516 analog media module</td>
<td>Slots 1 through 6</td>
<td>Three</td>
<td>–</td>
</tr>
<tr>
<td>- TIM516</td>
<td>TIM516</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TIM518 Analog Module</td>
<td>TIM518 analog media module</td>
<td>Slots 1 through 6</td>
<td>Three</td>
<td>–</td>
</tr>
<tr>
<td>- TIM518</td>
<td>TIM518</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TIM521 BRI Module</td>
<td>TIM521 BRI media module</td>
<td>Slots 1 through 6</td>
<td>Two</td>
<td>–</td>
</tr>
<tr>
<td>- TIM521</td>
<td>TIM521</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**TGM550 Telephony Gateway Module**

The TGM550 Telephony Gateway Module (Figure 31 on page 247), also known as the TGM550 Gateway Module, has two analog telephone ports, two analog trunk ports, and a serial console port.

The TGM550 enables routers to provide VoIP services to telephones and trunks that do not directly support VoIP by translating voice and signaling data between VoIP and the system used by the telephones and trunks.

**Figure 31: TGM550 Telephony Gateway Module**

The TGM550 provides the following key features:

- **Voice**
  - VoIP Media Gateway services.
  - Two analog telephone (LINE) ports to support two analog telephones or incoming analog direct inward dialing (DID) trunks with either wink start or immediate start. An analog relay supports emergency transfer relay (ETR).
  - Two analog trunk (TRUNK) ports to support loop start, ground start, centralized automatic message accounting (CAMA), and direct inward and outward dialing (DIOD) trunks (for Japan only).
  - Survivability features for continuous voice services.
  - Call center capabilities.

- **Provisioning**
  - Avaya Communication Manager (CM) media server management.
  - Extensive alarm and troubleshooting features.

- **Survivability**
  - Media Gateway Controller (MGC) automatic switchover, migration, and survivability features.
  - Modem backup connection to the MGC.
  - Dynamic call admission control (CAC) for WAN interfaces.

- **Management**
  - One serial port for console access over an RJ-45 connector cable.
NOTE: The RJ-45 console cable and DB-9 adapter supplied with the TGM550 are different from those supplied with the Services Router. You cannot use the RJ-45 cable and DB-9 adapter supplied with the Services Router for console connections to the TGM550.

Table 59 on page 248 lists the maximum number of media servers, telephones, and so on that are supported by the TGM550 installed on a J4350, J6350, J2320, or J2350 device.

Table 59: TGM550 Maximum Media Gateway Capacities

<table>
<thead>
<tr>
<th>Hardware or Feature</th>
<th>TGM550 Maximum Capacity</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>TGM550s that can be controlled by an Avaya S8500 or S8700 Media Server</td>
<td>250</td>
<td>This number also applies if a combination of Avaya G700 Media Gateways, G250 Media Gateways, and G350 Media Gateways are controlled by the same media server.</td>
</tr>
<tr>
<td>TGM550s that can be controlled by an Avaya S8400 Media Server</td>
<td>5</td>
<td>This number also applies if a combination of Avaya G700 Media Gateways, G250 Media Gateways, and G350 Media Gateways are controlled by the same media server.</td>
</tr>
<tr>
<td>TGM550s that can be controlled by an Avaya S8300 Media Server</td>
<td>49</td>
<td>This capacity is 50 if a combination of Avaya G700 Media Gateways, G250 Media Gateways, and G350 Media Gateways are controlled by the same media server. The S8300 must reside in a G700 or G350 media gateway. Therefore, the maximum of 50 H.248 gateways supported by the S8300 means that only 49 of the 50 can be TGM550s.</td>
</tr>
<tr>
<td>Media servers that can be registered as Media Gateway Controllers (MGCs) on a TGM550</td>
<td>4</td>
<td>If an MGC becomes unavailable, the TGM550 uses the next MGC on the list. The built-in SLS module can be considered a fifth MGC, although its functionality is limited from that of a full-scale media server.</td>
</tr>
<tr>
<td>Fixed analog line ports</td>
<td>2</td>
<td>—</td>
</tr>
<tr>
<td>Fixed analog trunk ports</td>
<td>2</td>
<td>—</td>
</tr>
</tbody>
</table>
Table 59: TGM550 Maximum Media Gateway Capacities (continued)

<table>
<thead>
<tr>
<th>Hardware or Feature</th>
<th>TGM550 Maximum Capacity</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital signal processors (DSPs)</td>
<td>1 (up to 80 channels)</td>
<td>For calls using voice codec sets with 20ms or higher packet sizes, the DSP supports:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 80 channels</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 20 channels</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ 10 channels</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For calls with 10 ms or-lower packet sizes, the 80–channel DSP supports 40 channels.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For TTY, fax, or modem over IP calls, the 80–channel DSP supports 40 channels.</td>
</tr>
<tr>
<td>Busy Hour Call Completion Rate (BHCC)</td>
<td>800</td>
<td>—</td>
</tr>
<tr>
<td>Total of IP and analog telephones</td>
<td>70 (J4350)</td>
<td>Maximum includes a combination of analog and IP telephones</td>
</tr>
<tr>
<td>that can be connected to a TGM550</td>
<td>100 (J6350)</td>
<td></td>
</tr>
<tr>
<td>and TIMs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Touch-tone recognition (TTR)</td>
<td>32</td>
<td>Receivers</td>
</tr>
<tr>
<td>Tone generation</td>
<td>As much as necessary for all TDM calls</td>
<td>—</td>
</tr>
<tr>
<td>Announcements (VAL)</td>
<td>16 playback channels for playing announcements, one of which can be used for recording</td>
<td></td>
</tr>
<tr>
<td></td>
<td>20 minutes for G711-quality stored announcements and music-on-hold</td>
<td></td>
</tr>
<tr>
<td></td>
<td>256 maximum announcements stored</td>
<td></td>
</tr>
</tbody>
</table>

**CAUTION:** Some capacities may change. For the most recent list, see System Capacities Table for Avaya Communication Manager on Avaya Media Servers at [http://support.avaya.com](http://support.avaya.com).

For pinouts of the TGM550 RJ-45 console connector, see “TGM550 Console Port Pinouts” on page 238. For pinouts of cable connectors for the TGM550 analog ports, see “TGM550 RJ-11 Connector Pinout for Analog Ports” on page 239.

TGM550 LEDs indicate link status and activity. Table 60 on page 250 describes the meaning of the LEDs.
Table 60: LEDs for TGM550 Gateway Module

<table>
<thead>
<tr>
<th>Label</th>
<th>Color</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALM</td>
<td>Red</td>
<td>On steadily</td>
<td>Alarm. A failure in the TGM550 requires monitoring or maintenance.</td>
</tr>
<tr>
<td>ACT</td>
<td>Yellow</td>
<td>On steadily</td>
<td>Active. The TGM550 is online with network traffic.</td>
</tr>
<tr>
<td>ASB</td>
<td>Green</td>
<td>On steadily</td>
<td>Alternate software bank. The software is not running from the selected boot bank.</td>
</tr>
<tr>
<td>ETR</td>
<td>Green</td>
<td>On steadily</td>
<td>Emergency transfer relay (ETR) feature is active.</td>
</tr>
</tbody>
</table>

For more information about the TGM550, see *Hardware Description and Reference for Avaya Communication Manager* at [http://support.avaya.com](http://support.avaya.com).

**TIM508 Analog Telephony Interface Module**

The TIM508 Analog Telephony Interface Module (Figure 32 on page 250), also known as the TIM508 analog media module, has eight analog telephone lines that can be used as trunk ports.

**Figure 32: TIM508 Analog Telephony Interface Module**

![TIM508 Analog Telephony Interface Module](image)

**NOTE:** All eight analog lines can be configured as analog direct inward dialing (DID) trunks.

You can configure TIM508 ports as described in Table 61 on page 250.

Table 61: TIM508 Possible Port Configurations

<table>
<thead>
<tr>
<th>Possible Analog Telephone Line Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wink-start or immed-start DID trunk</td>
</tr>
</tbody>
</table>

250  | Avaya VoIP Modules
Table 61: TIM508 Possible Port Configurations (continued)

<table>
<thead>
<tr>
<th>Possible Analog Telephone Line Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analog tip/ring devices such as single-line telephones with or without LED message-waiting indication</td>
</tr>
</tbody>
</table>

The TIM508 also provides the following features:

- Three ringer loads, the ringer equivalency number for up to 2,000 ft (610 m), for all eight lines
- Up to eight simultaneously ringing lines
- Type 1 caller ID and Type 2 caller ID for lines
- Ring voltage generation for a variety of international frequencies and cadences

For pinouts of cable connectors for the TIM508, see “TIM508 Connector Pinout” on page 239.

TIM508 LEDs indicate link status and activity. Table 62 on page 251 describes the meaning of the LEDs.

Table 62: LEDs for TIM508

<table>
<thead>
<tr>
<th>Label</th>
<th>Color</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALM</td>
<td>Red</td>
<td>On steadily</td>
<td>Alarm. A TIM508 failure requires monitoring or maintenance.</td>
</tr>
<tr>
<td>ACT</td>
<td>Yellow</td>
<td>Blinking</td>
<td>Active. A device connected to the TIM508 is in use. This situation can include a telephone that is off the hook.</td>
</tr>
</tbody>
</table>

For more information about the TIM508, see Hardware Description and Reference for Avaya Communication Manager at http://support.avaya.com.

TIM510 E1/T1 Telephony Interface Module

The TIM510 E1/T1 Telephony Interface Module (Figure 33 on page 252), also known as the TIM510 E1/T1 media module, terminates an E1 or T1 trunk. The TIM510 T1/E1 media module has a built-in channel service unit (CSU) so an external CSU is not necessary. The CSU is used for a T1 circuit only. Up to two TIM510s can be installed in any of the slots on the Services Router.
The TIM510 provides the following key features:

- One E1 or T1 trunk port with up to 30 channels on an E1 port and 24 channels on a T1 port.
- DS1-level support for a variety of E1 and T1 trunk types.
- Trunk signaling to support U.S. and international central office (CO) or tie trunks.
- Echo cancellation in either direction—incoming or outgoing.

For pinouts of cable connectors for the TIM510, see “TIM510 RJ-45 Connector Pinout” on page 240.

TIM510 LEDs indicate link status and activity. Table 63 on page 252 describes the meaning of the LEDs.

### Table 63: LEDs for TIM510

<table>
<thead>
<tr>
<th>Label</th>
<th>Color</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALM</td>
<td>Red</td>
<td>On steadily</td>
<td>Alarm. A TIM510 failure requires monitoring or maintenance.</td>
</tr>
<tr>
<td>ACT</td>
<td>Green</td>
<td>On steadily</td>
<td>Active. The TIM510 is online with network traffic.</td>
</tr>
<tr>
<td>TST</td>
<td>Yellow</td>
<td>On steadily</td>
<td>Test. A test is being performed on the TIM510 through the Media Gateway Controller (MGC).</td>
</tr>
<tr>
<td>SIG</td>
<td>Green</td>
<td>On steadily</td>
<td>Signal. The link to the central office (CO) is active.</td>
</tr>
</tbody>
</table>

For more information about the TIM510, see *Hardware Description and Reference for Avaya Communication Manager* at [http://support.avaya.com](http://support.avaya.com).
**TIM514 Analog Telephony Interface Module**

The TIM514 Analog Telephony Interface Module (Figure 34 on page 253), also known as the TIM514 analog media module, has four analog telephone ports and four analog trunk ports.

![Figure 34: TIM514 Analog Telephony Interface Module](image)

**NOTE:** For analog direct inward dialing (DID) trunks, you must use the four analog telephone (LINE) ports. You cannot use the four analog trunk (TRUNK) ports for analog DID trunks.

You can configure TIM514 ports as described in Table 64 on page 253.

**Table 64: TIM514 Possible Port Configurations**

<table>
<thead>
<tr>
<th>Possible Analog Telephone (LINE) Port Configurations</th>
<th>Possible Analog Trunk (TRUNK) Port Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wink-start or immediate-start DID trunk</td>
<td>Loop-start or ground-start central office trunk with a loop current of 18 to 120 mA.</td>
</tr>
<tr>
<td>Analog tip/ring devices such as single-line telephones with or without LED message-waiting indication</td>
<td>Two-wire analog outgoing centralized automatic message accounting (CAMA) emergency E911 trunk, for connectivity to the PSTN.</td>
</tr>
<tr>
<td></td>
<td>Multifrequency (MF) signaling is supported for CAMA ports.</td>
</tr>
</tbody>
</table>

The TIM514 also provides the following features:

- Three ringer loads, the ringer equivalency number for up to 2,000 ft (610 m), for all eight ports.
- Up to four simultaneously ringing ports.
- Type 1 caller ID and Type 2 caller ID.
- Ring voltage generation for a variety of international frequencies and cadences.

For pinouts of cable connectors for the TIM514, see “TIM514 Connector Pinout” on page 240.
TIM514 LEDs indicate link status and activity. Table 65 on page 254 describes the meaning of the LEDs.

**Table 65: LEDs for TIM514**

<table>
<thead>
<tr>
<th>Label</th>
<th>Color</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALM</td>
<td>Red</td>
<td>On steadily</td>
<td>Alarm. A TIM514 failure requires monitoring or maintenance.</td>
</tr>
<tr>
<td>ACT</td>
<td>Yellow</td>
<td>Blinking</td>
<td>Active. A device connected to the TIM514 is in use. This situation can include a telephone that is off the hook.</td>
</tr>
</tbody>
</table>

For more information about the TIM514, see *Hardware Description and Reference for Avaya Communication Manager* at [http://support.avaya.com](http://support.avaya.com).

**TIM516 Analog Telephony Interface Module**

The TIM516 Analog Telephony Interface Module (Figure 35 on page 254), also known as the TIM516 analog media module, has 16 analog telephone lines.

**Figure 35: TIM516 Analog Telephony Interface Module**

You can configure TIM516 lines as described in Table 66 on page 254.

**Table 66: TIM516 Possible Port Configurations**

| Possible Analog Telephone (LINE) Line Configurations | Analog tip/ring devices such as single-line telephones with or without LED message-waiting indication |

The TIM516 also provides the following features:

- Three ringer loads, the ringer equivalency number for up to 2,000 ft (610 m), for all 16 lines
- Up to 16 simultaneously ringing lines
Type 1 caller ID and Type 2 caller ID for line lines
Ring voltage generation for a variety of international frequencies and cadences

For pinouts of cable connectors for the TIM516, see “TIM516 Connector Pinout” on page 241.

TIM516 LEDs indicate link status and activity. Table 67 on page 255 describes the meaning of the LEDs.

### Table 67: LEDs for TIM516

<table>
<thead>
<tr>
<th>Label</th>
<th>Color</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALM</td>
<td>Red</td>
<td>On steadily</td>
<td>Alarm. A TIM516 failure requires monitoring or maintenance.</td>
</tr>
<tr>
<td>ACT</td>
<td>Yellow</td>
<td>Blinking</td>
<td>Active. A device connected to the TIM516 is in use. This situation can include a telephone that is off the hook.</td>
</tr>
</tbody>
</table>

For more information about the TIM516, see the Avaya manual *Hardware Description and Reference for Avaya Communication Manager*.

**TIM518 Analog Telephony Interface Module**

The TIM518 Analog Telephony Interface Module (Figure 36 on page 255), also known as the TIM518 analog media module, has eight analog telephone lines and eight analog trunk lines.

**Figure 36: TIM518 Analog Telephony Interface Module**

NOTE: For analog direct inward dialing (DID) trunks, you can use all eight analog telephone lines.

You can configure eight TIM518 analog telephone lines as described in Table 68 on page 256.
Table 68: TIM518 Possible Port Configurations

<table>
<thead>
<tr>
<th>Possible Analog Telephone Port Configurations</th>
<th>Possible Analog Trunk Port Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wink-start or immed-start DID trunk</td>
<td>Loop-start or ground-start central office trunk with a loop current of 18 to 120 mA</td>
</tr>
<tr>
<td>Analog tip/ring devices such as single-line phones with or without LED message-waiting indication</td>
<td>Two-wire analog outgoing centralized automatic message accounting (CAMA) emergency E911 trunk for connectivity to the PSTN</td>
</tr>
</tbody>
</table>

The TIM518 also provides the following features:

- Three ringer loads, the ringer equivalency number for up to 2,000 ft (610 m), for all 16 lines
- Up to 16 simultaneously ringing lines
- Type 1 caller ID and Type 2 caller ID for line lines
- Type 1 caller ID for trunk lines
- Ring voltage generation for a variety of international frequencies and cadences

For pinouts of cable connectors for the TIM518, see “TIM518 Connector Pinout” on page 242.

TIM518 LEDs indicate link status and activity. Table 69 on page 256 describes the meaning of the LEDs.

Table 69: LEDs for TIM518

<table>
<thead>
<tr>
<th>Label</th>
<th>Color</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALM</td>
<td>Red</td>
<td>On steadily</td>
<td>Alarm. A TIM518 failure requires monitoring or maintenance.</td>
</tr>
<tr>
<td>ACT</td>
<td>Yellow</td>
<td>Blinking</td>
<td>Active. A device connected to the TIM518 is in use. This situation can include a telephone that is off the hook.</td>
</tr>
</tbody>
</table>

For more information about the TIM518, see Hardware Description and Reference for Avaya Communication Manager at http://support.avaya.com.

TIM521 BRI Telephony Interface Module

The TIM521 BRI Telephony Interface Module (Figure 37 on page 257), also known as the TIM521 BRI media module, has four ports with RJ-45 jacks that can be administered as ISDN Basic Rate Interface (BRI) trunk connections. Each ISDN BRI port has two B-channels plus a D-channel. Up to two TIM521 modules (with four BRI trunk ports each) can be installed in any of the slots on the Services Router.
For ISDN BRI trunking, the TIM521 supports up to four BRI interfaces to the central office at the ISDN T reference point. Information is communicated on each port in two ways:

- Over two 64-Kbps B-channels, called B1 and B2, that can be circuit-switched simultaneously

**NOTE:** The TIM521 does not support BRI stations or combining both B-channels together to form a 128-Kbps channel.

- Over a 16-Kbps channel, called the D-channel, that is used for signaling. The TIM521 occupies one time slot for all four D-channels

The circuit-switched connections have an a-law or mu-law option for voice operation. The circuit-switched connections operate as 64-Kbps clear channels transmitting data.

TIM521 LEDs indicate link status and activity. Table 70 on page 257 describes the meaning of the LEDs.

<table>
<thead>
<tr>
<th>Label</th>
<th>Color</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALM</td>
<td>Red</td>
<td>On steadily</td>
<td>Alarm. A TIM521 failure requires monitoring or maintenance.</td>
</tr>
<tr>
<td>ACT</td>
<td>Yellow</td>
<td>On steadily</td>
<td>Active. A trunk connected to the TIM521 is in use.</td>
</tr>
</tbody>
</table>

For more information about the TIM521, see *Hardware Description and Reference for Avaya Communication Manager* at [http://support.avaya.com](http://support.avaya.com).

**VoIP Terms**

Before configuring VoIP, become familiar with the terms defined in Table 71 on page 258.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>bearer bandwidth limit (BBL)</td>
<td>Maximum bandwidth available for voice traffic on an interface when dynamic call admission control is configured on the interface. See also dynamic CAC.</td>
</tr>
<tr>
<td>call admission control (CAC)</td>
<td>Method of limiting voice traffic over a particular link in a network. See also dynamic CAC.</td>
</tr>
<tr>
<td>centralized automatic message accounting (CAMA)</td>
<td>Recording of toll calls at a central point.</td>
</tr>
<tr>
<td>direct inward dialing (DID)</td>
<td>Feature of a trunk line that allows incoming calls to be routed directly to selected stations without help from an attendant.</td>
</tr>
<tr>
<td>direct outward dialing (DOD)</td>
<td>Feature of a trunk line that allows outgoing calls to be routed directly without help from an attendant.</td>
</tr>
<tr>
<td>direct inward and outward dialing (DIOD)</td>
<td>Feature of a trunk line that allows both incoming and outgoing calls to be routed directly without help from an attendant. See also direct inward dialing (DID) and direct outward dialing (DOD).</td>
</tr>
<tr>
<td>Disk-on-Key</td>
<td>Memory device (stick) that plugs into a USB port to load a complete JUNOS configuration with VoIP onto a Services Router. You must first use an Electronic Preinstallation Worksheet (EPW) to download the configuration to the Disk-on-Key device. The EPW and Disk-on-Key device provide an alternative method to configure the router for VoIP.</td>
</tr>
<tr>
<td>dynamic CAC</td>
<td>Application that blocks calls on a WAN interface when the bandwidth is exhausted. See also call admission control (CAC).</td>
</tr>
<tr>
<td>Electronic Preinstallation Worksheet (EPW)</td>
<td>Customized Microsoft Excel spreadsheet used with a Disk-on-Key USB memory stick to configure VoIP on a Services Router. You download the EPW from an Avaya Web site.</td>
</tr>
<tr>
<td>emergency transfer relay (ETR)</td>
<td>Feature that provides an emergency link between the telephone connected to the first LINE port on the TGM550 and the trunk connected to the TRUNK port on the TGM550 if power is disconnected from the Services Router or if the TGM550 becomes unregistered from its Media Gateway Controller (MGC).</td>
</tr>
<tr>
<td>IEEE 802.1p standard</td>
<td>IEEE standard for a Layer 2 frame structure that supports virtual LAN (VLAN) identification and class-of-service (CoS) traffic classification.</td>
</tr>
<tr>
<td>IEEE 802.3af standard</td>
<td>IEEE standard that defines a method for powering network devices through an Ethernet cable. Also known as Power over Ethernet (PoE), this standard enables remote devices (such as VoIP telephones) to operate without a separate, external power source. See also Power over Ethernet (PoE).</td>
</tr>
<tr>
<td>ITU H.248 standard</td>
<td>International Telecommunications Union (ITU) standard for communication between a gateway controller and a media gateway.</td>
</tr>
<tr>
<td>ITU H.323 standard</td>
<td>International Telecommunications Union (ITU) standard for packet-based multimedia communications over networks that do not guarantee class of service (CoS), such as IP networks. H323, modeled after ISDN PRI, is the standard for voice over IP (VoIP) and conferencing.</td>
</tr>
</tbody>
</table>
Table 71: VoIP Terminology (continued)

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Gateway Controller (MGC)</td>
<td>Avaya media server that controls the parts of the call state that pertain to connection control for media channels in a media gateway. The MGC is the controlling entity in an H.248 relationship.</td>
</tr>
<tr>
<td>Power over Ethernet (PoE)</td>
<td>Electrical current run to networking devices over Ethernet Category 5 or higher data cables. No extra AC power cord or outlets are needed at the product location.</td>
</tr>
<tr>
<td>public switched telephone network (PSTN)</td>
<td>The public worldwide voice telephone network.</td>
</tr>
<tr>
<td>standard local survivability (SLS)</td>
<td>Configurable software feature that enables a TGM550 to provide limited Media Gateway Controller (MGC) functionality when no link is available to a registered MGC.</td>
</tr>
<tr>
<td>time-division multiplexing (TDM)</td>
<td>A form of multiplexing that divides a transmission channel into successive time slots.</td>
</tr>
<tr>
<td>TGM550</td>
<td>Avaya Telephony Gateway Module. Avaya VoIP H.248 media gateway module installed in a Services Router along with one or more Telephony Interface Modules (TIMs) to connect VoIP and legacy analog telephones and trunks over IP networks. Only the TGM550 has an interface configurable through the J-Web interface or JUNOS CLI. The TIMs are configured and administered from the TGM550 CLI.</td>
</tr>
<tr>
<td>TIM510</td>
<td>Avaya E1/T1 Telephony Interface Module. Avaya VoIP module installed in a Services Router to provide an E1 or T1 trunk connection over the Internet to a telephone central office (CO). A TIM510 is configured and administered from a TGM550 installed in the same router.</td>
</tr>
<tr>
<td>TIM514</td>
<td>Avaya Analog Telephony Interface Module. Avaya VoIP module installed in a Services Router to connect individual telephones or trunk lines to the Internet. A TIM514 is configured and administered from a TGM550 installed in the same router.</td>
</tr>
<tr>
<td>TIM521</td>
<td>Avaya BRI Telephony Interface Module. Avaya VoIP module installed in a Services Router to connect ISDN Basic Rate Interface (BRI) trunk lines to a telephone central office (CO) over the Internet for data or voice transmission. A TIM521 is configured and administered from a TGM550 installed in the same router.</td>
</tr>
</tbody>
</table>

VoIP Overview

This section contains the following topics.

- About the Avaya IG550 Integrated Gateway on page 260
- VoIP Interfaces on page 261
- Avaya VoIP Modules Overview on page 262
- Media Gateway Controller on page 263
- Avaya Communication Manager on page 264
- Dynamic Call Admission Control Overview on page 264
About the Avaya IG550 Integrated Gateway

The Avaya IG550 Integrated Gateway consists of the TGM550 Telephony Gateway Module and one or more Telephony Interface Modules (TIMs) that are installed in the slots on the J4350 and J6350 Services Routers to provide VoIP connectivity. The TGM550 is an H.248 media gateway that works with the TIMs to connect IP and legacy analog telephones and trunks over IP networks and enable IP telephones to communicate through analog telephone lines and trunks.

The TGM550 is also connected over a LAN or WAN to a Media Gateway Controller (MGC)—an Avaya media server running Avaya Communication Manager (CM) call processing software. The telephony services on the TGM550 are managed by an MGC located at headquarters or in a branch office. When the primary MGC is located at a remote location, the TGM550 uses standard local survivability (SLS) for partial MGC backup in the event that the connection to the primary MGC is lost. Devices can thereby provide reliable telephony services to branch offices.

Figure 38 on page 261 shows a typical VoIP topology. The small branch office shown in the expanded illustration on the right is connected over the corporate WAN to the head office through a J6300 Services Router with VoIP modules installed. The Avaya Media Gateway Controller, S8700 Media Server, and integrated Management tools at the head office manage telephony services for headquarters and the branch offices on the WAN, connecting the corporation’s legacy analog telephones, VoIP telephones, PCs, and fax machines to the PSTN.
VoIP Interfaces

Four types of interfaces on Avaya VoIP modules provide VoIP connectivity on J4350 and J6350 Services Routers:

- Analog telephone or trunk port
- T1 port
- E1 port
- ISDN BRI telephone or trunk port

These interfaces are available on the field-replaceable Avaya VoIP modules listed in Table 72 on page 262. For more information about interface names, see “Network Interface Naming” on page 9. For more information about the modules, see “Avaya VoIP Modules Overview” on page 262.
Table 72: Interfaces on Avaya VoIP Modules

<table>
<thead>
<tr>
<th>Module Name</th>
<th>Description</th>
<th>VoIP Interfaces</th>
<th>JUNOS Interface</th>
</tr>
</thead>
</table>
| TGM550        | Avaya Telephony Gateway Module (TGM)       | ■ Two analog telephone ports  
■ Two analog trunk ports  
■ One serial port for console access | vp-pim/0/0  
On a VoIP interface, the port is always 0. |
| TIM510        | Avaya E1/T1 Telephony Interface Module (TIM)| One E1/T1 trunk port providing up to 30 E1 or 24 T1 channels                  | –                                      |
| TIM514        | Avaya Analog TIM                           | ■ Four analog telephone ports  
■ Four analog trunk ports | –                                      |
| TIM521        | Avaya BRI TIM                              | Four ISDN BRI trunk ports providing up to eight channels                      | –                                      |

Only the TGM550 has a JUNOS interface. Because the TIMs do not have corresponding physical interfaces, you cannot configure or administer them with the J-Web interface or the JUNOS CLI. However, you can display TGM550 and TIM status from J-Web Monitor > Chassis pages and with the CLI `show chassis` command.

**NOTE:** TIMs are configured and administered from the TGM550 CLI. For more information, see the Administration Guide and CLI Reference for the Avaya IG550 Integrated Gateway at [http://support.avaya.com](http://support.avaya.com).

**CAUTION:** The TGM550 and TIMs are not hot-swappable. You must power off the router before installing or removing the Avaya VoIP modules. Ensure that the Avaya VoIP modules are installed in the router chassis before booting up the system.

Avaya VoIP Modules Overview

A TGM550 and one or more TIMs installed in a Services Router provide telephony exchange services to a branch office over IP networks. Different TIMs have access ports for different types of VoIP and analog telephones and telephone lines. You connect the telephones and lines to the ports on the TGM550 and the TIMs. VoIP telephones require connection to a Power over Ethernet (PoE) adapter or switch that is plugged into an Ethernet port on the Services Router.

VoIP capabilities on the TGM550 enable the Services Router to provide VoIP services to telephones and trunks that do not directly support VoIP. The TGM550 translates voice and signaling data between VoIP and the system used by the telephones and
Media Gateway Controller

A Media Gateway Controller (MGC) is a media server (call controller) that controls telephone services on the TGM550. An Avaya media server running Avaya Communication Manager (CM) software acts as an MGC for the TGM550.

The following media servers running Avaya Communication Manager can be used as an MGC with the TGM550:

- **Avaya S8300 Media Server**—Controls up to 49 TGM550s.
- **Avaya S8400 Media Server**—Controls up to 5 TGM550s.
- **Avaya S8500 Media Server**—Controls up to 250 TGM550s.
- **Avaya S8700 Media Server**—Controls up to 250 TGM550s.
- **Avaya S8710 Media Server**—Controls up to 250 TGM550s.
- **Avaya S8720 Media Server**—Controls up to 250 TGM550s.

To provide telephony services, the TGM550 must be registered with at least one Media Gateway Controller (MGC). You can configure the IP addresses of up to four MGCs that the TGM550 can connect to in the event of a link failure. The MGC list consists of the IP addresses of the MGCs to connect to and the order in which to reestablish the H.248 link. The first MGC on the list is the primary MGC. The TGM550 searches for the primary MGC first. If it cannot connect to the primary MGC or loses its connection to the primary MGC, it attempts to connect to the next MGC in the list, and so on.

**NOTE:** The MGC list is stored in the TGM550. It is not written to the JUNOS configuration file.

You must also administer Avaya Communication Manager on the configured Media Gateway Controllers to support the TGM550. For more information, see the following Avaya IG550 Integrated Gateway manuals at [http://support.avaya.com](http://support.avaya.com):

- *Installing and Configuring the Avaya IG550 Integrated Gateway*
- *Administration Guide and CLI Reference for the Avaya IG550 Integrated Gateway*
- *Administrator Guide for Avaya Communication Manager*
- *Avaya Maintenance Procedures for Communication Manager, Media Servers, and Media Gateways*
- *Avaya Maintenance Commands for Communication Manager, Media Servers, and Media Gateways*
- *Avaya Maintenance Alarms for Communication Manager, Media Servers, and Media Gateways*
Avaya Communication Manager

Avaya Communication Manager (CM) software manages the Media Gateway Controller (MGC). Avaya CM allows you to do the following:

- Assign numbers to local telephones.
- Determine where to connect your telephone call based on the number you dial.
- Play dial tones, busy signals, and prerecorded voice announcements.
- Allow or prohibit access to outside lines for specific telephones.
- Assign telephone numbers and buttons to special features.
- Exchange call switching information with older telephone switches that do not support VoIP.

**NOTE:** The TGM550 supports Avaya Communication Manager (CM) release 4.0 and later releases. The TGM550 does not support Avaya Communication Manager (CM) releases earlier than release 4.0.

For more information about Avaya CM, see the *Administrator Guide for Avaya Communication Manager* at [http://support.avaya.com](http://support.avaya.com).

Dynamic Call Admission Control Overview

Dynamic call admission control (CAC) enables the Media Gateway Controller (MGC) to automatically assign the bandwidth available for voice traffic on WAN interfaces and block new calls when the existing call bandwidth is completely engaged. You configure dynamic CAC on a high-bandwidth primary interface and on one or more backup interfaces with less bandwidth.

Without dynamic CAC, the MGC cannot detect the switchover to the backup link or the resulting changes in network topology and available bandwidth. As a result, the MGC continues to admit calls at the bandwidth of the primary link, causing network congestion and possible jitter, delay, and loss of calls.

**Supported Interfaces**

Dynamic CAC must be configured on each Services Router interface responsible for providing call bandwidth. You can configure dynamic CAC on the following types of interfaces on Services Routers:

- ADSL
- E1
- E3
- Fast Ethernet
- Gigabit Ethernet
Bearer Bandwidth Limit and Activation Priority

The dynamic CAC bearer bandwidth limit (BBL) configured on an interface specifies the maximum bandwidth available for voice traffic on the interface. The TGM550 reports the BBL to the MGC. When the call bandwidth exceeds the BBL, the MGC blocks new calls and alerts the user with a busy tone.

You configure the dynamic CAC activation priority value on interfaces to specify the order in which the interfaces are used for providing call bandwidth.

Rules for Determining Reported BBL

To assess the WAN interfaces that have an activation priority value and determine a single BBL to report to the MGC, the TGM550 uses the following rules. The reported BBL (RBBL) allows the MGC to automatically control the call bandwidth when interfaces responsible for providing call bandwidth become available or unavailable.

- Report the BBL of the active interface with the highest activation priority. For example, if one interface has the activation priority of 200 and a BBL of 1500 Kbps and another interface has the activation priority of 100 and a BBL of 1000 Kbps, the RBBL is 1500 Kbps.

- If more than one active interface has the same activation priority, report a BBL that is the number of interfaces times their lowest BBL. For example, if two interfaces with the same activation priority have BBLs of 2000 Kbps and 1500 Kbps, the RBBL is 3000 Kbps (2 x 1500 Kbps).

- If the interface with the highest activation priority is unavailable, report the BBL of the active interface with the next highest activation priority.

- If all the interfaces on which dynamic CAC is configured are inactive, report a BBL of 0. The MGC does not allow calls to go through when the RBBL is 0.

**NOTE:** Dynamic CAC works in conjunction with the Avaya Communication Manager (CM) Call Admission Control: Bandwidth Limitation (CAC-BL) feature. If you configure dynamic CAC on WAN interfaces, you must also configure CAC-BL on Avaya CM. For more information about configuring CAC-BL, see the Administrator Guide for Avaya Communication Manager at [http://support.avaya.com](http://support.avaya.com).
**TGM550 Firmware Compatibility with JUNOS Internet Software**

The TGM550 firmware version must be compatible with the JUNOS Software version installed on the device. For compatibility information, see the *Communication Manager Software & Firmware Compatibility Matrix* at [http://support.avaya.com](http://support.avaya.com).

**CAUTION:** If the TGM550 firmware version is not compatible with the JUNOS Internet software version on the router, the router does not detect the VoIP interface (`vp-pim/0/0`) and the interface is unavailable. For more information, see “TGM550 Is Installed But the VoIP Interface Is Unavailable” on page 286.

If you are upgrading both the TGM550 firmware and the JUNOS Software on the router, first upgrade the TGM550 firmware, and then upgrade the JUNOS Software.

For information about upgrading the TGM550 firmware, see the *Administration Guide and CLI Reference for the Avaya IG550 Integrated Gateway* at [http://support.avaya.com](http://support.avaya.com).

**TGM550 IP Addressing Guidelines**

For operational purposes, the TGM550 is identified as a host on the device. Hence, the TGM550 needs to be assigned an IP address that is reachable both externally and internally from the device. The TGM550 uses this IP address to identify itself when communicating with other devices, particularly the Media Gateway Controller (MGC).

To assign the IP address for the TGM550, you configure the destination address on the `vp-pim/0/0` interface. For information about configuring the `vp-pim/0/0` interface, see “Configuring VoIP Interfaces with Quick Configuration” on page 269 or “Configuring the VoIP Interface (Required)” on page 272.

**CAUTION:** Applying a new or modified IP address resets the TGM550. Before modifying the IP address, take the following precautions:

- Log into the TGM550 and enter `copy running-config startup-config` to save the TGM550 configuration. (For login instructions, see “Accessing and Administering the TGM550 CLI” on page 278.)
- Ensure that the TGM550 is not currently handling voice traffic.

To enable easier administration of the TGM550, we recommend the following guidelines for assigning the IP address of the TGM550:

- Assign an address from one of the subnets that is already configured in the branch office where the device is installed.
- Decide on a block of IP addresses for VoIP services, and assign an IP address from that block to the TGM550.
- Do not assign the following IP addresses to the TGM550:
Before You Begin

Before you configure VoIP interfaces, you need to perform the following tasks:

- Install Services Router hardware, including the TGM550 and the TIMs. Before power is connected, ensure that the router is grounded with a 10 AWG cable. For installation and grounding instructions, see the \textit{J4350 and J6350 Services Router Getting Started Guide}.

\textbf{CAUTION:} The original grounding cable for SSG Services Routers is 14 AWG only and must be replaced with a 10 AWG cable.

- Verify that you have connectivity to at least one Avaya media server running Avaya Communication Manager (CM) release 4.0 or later. For more information about Avaya media servers, see “Media Gateway Controller” on page 263.

- Verify that the Services Router is running JUNOS Release 8.2R1 or later.

- Download and install the most recent firmware for the TGM550. Verify that the TGM550 firmware version is compatible with the JUNOS Software version installed on the Services Router. For more information, see “TGM550 Firmware Compatibility with JUNOS Internet Software” on page 266.

- If you are configuring VoIP using the Avaya Electronic Preinstallation Worksheet (EPW) and a Disk-on-Key USB memory stick, order a Disk-on-Key USB memory stick. For Disk-on-Key requirements, see “Configuring VoIP Interfaces with EPW and Disk-on-Key” on page 268.

- Establish basic connectivity. For more information, see the \textit{J4350 and J6350 Services Router Getting Started Guide}.

- If you do not already have a basic understanding of physical and logical interfaces and Juniper Networks interface conventions, read “Interfaces Overview” on page 3.

- Applying an IP address to the TGM550 resets the module. If you are updating an existing VoIP configuration by modifying the TGM550 IP address, take the following precautions:
  - Log into the TGM550 and enter \texttt{copy running-config startup-config} to save the TGM550 configuration. (For login instructions, see “Accessing and Administering the TGM550 CLI” on page 278.)
Ensure that the TGM550 is not currently handling voice traffic.

**Configuring VoIP Interfaces with EPW and Disk-on-Key**

If you have a new J4350 or J6350 Services Router with the TGM550 and TIMs installed in the router, you can use the Avaya Electronic Preinstallation Worksheet (EPW) and a Disk-on-Key USB memory stick to configure VoIP on the router.

The EPW is a customized Microsoft Excel spreadsheet that you use to collect a complete set of VoIP configuration information and create a configuration file named `juniper-config.txt`. You can copy the `juniper-config.txt` file to a Disk-on-Key device and boot the router from the device to configure VoIP on the router.

This configuration method has the following requirements:

- A management device (PC or laptop) running Microsoft Excel version 2000 or later.
- A Disk-on-Key device with one of the following 16-bit or 32-bit file allocation table (FAT) file systems:
  - DOS 3.0+ 16-bit FAT (up to 32 MB)
  - DOS 3.31+ 16-bit FAT (over 32 MB)
  - WIN95 OSR2 FAT32
  - WIN95 OSR2 FAT32, LBA-mapped
  - WIN95 DOS 16-bit FAT, LBA-mapped
- A Services Router with the factory configuration and the TGM550 and TIMs installed. If other JUNOS configuration files exist on the Services Router, the router cannot read the `juniper-config.txt` file from the Disk-on-Key device. To remove the configuration files from the router, press and hold the **RESET CONFIG** button for 15 seconds or more, until the **STATUS** LED blinks red.

**CAUTION:** Pressing and holding the **RESET CONFIG** button for 15 seconds or more—until the **STATUS** LED blinks red—deletes all configurations on the router, including the backup configurations and rescue configuration, and loads and commits the factory configuration.
To configure a VoIP interface using EPW and Disk-on-Key:

1. Follow these instructions to download the EPW to a PC or laptop computer.
   b. On the Avaya support page, click Find Documentation and Technical Information by Product Name.
   c. Scroll down and click Integrated Management — Provisioning & Installation Manager.
   d. Select the 4.0 release from the select a release drop-down box and click View all documents.
   e. Scroll down and double-click the Electronic Preinstallation Worksheet for Provisioning Installation Manager link.
   f. Scroll down and double-click the View XLS link.
   g. In the File Open window, click the Open button.
   h. In the Security Warning window, open the EPW by clicking Enable Macros. Be sure to open the EPW in Microsoft Excel version 2000 or later versions.

2. Enter information in the individual worksheets. Ensure that all mandatory fields (highlighted in blue color) are filled in.

3. Select File > Save.

4. Open the InitialConfig worksheet and click Create Configuration File. The Select Location page is displayed.

5. Choose a location where you want to create the configuration file. The configuration file with the name juniper-config.txt is created.

6. Copy the juniper-config.txt file to a Disk-on-Key device.

7. Press and release the power button to power off the router. Wait for the POWER LED to turn off.

8. Plug the Disk-on-Key device into the USB port on the Services Router.

9. Press the POWER button on the front panel of the router. Verify that the POWER LED on the front panel turns green. The router reads the juniper-config.txt file from the Disk-on-Key device and commits the configuration.

10. Remove the Disk-on-Key device.

---

**Configuring VoIP Interfaces with Quick Configuration**

You can use the VoIP Interfaces Quick Configuration pages to configure the VoIP interface on a router.
To configure a VoIP interface with Quick Configuration:

1. From the Quick Configuration page, as shown in Figure 16 on page 82, select the VoIP interface—for example, `vp-5/0/0`—you want to configure.

   See “Network Interface Naming” on page 9.

2. Enter information into the Quick Configuration page, as described in Table 73 on page 270.

3. Click one of the following buttons:
   - To apply the configuration and stay on the Quick Configuration page, click **Apply**.
   - To apply the configuration and return to the main configuration page, click **OK**.
   - To cancel your entries and return to the main page, click **Cancel**.

4. To verify that the VoIP interface is configured correctly, see “Verifying the VoIP Configuration” on page 283.

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VoIP Logical Interfaces</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add logical interfaces</td>
<td>Defines logical unit 0 as the physical VoIP interface to which you connect. You must define one logical unit for the VoIP interface.</td>
<td>Click <strong>Add</strong>.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>You cannot define more than one logical unit for the VoIP interface. The logical unit number must be 0.</td>
<td></td>
</tr>
<tr>
<td>Logical Interface Description</td>
<td>(Optional) Describes the logical interface.</td>
<td>Type a text description of the logical interface to more clearly identify it in monitoring displays.</td>
</tr>
<tr>
<td>Field</td>
<td>Function</td>
<td>Your Action</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>IPv4 Address and Prefix</td>
<td>Specifies the IPv4 address for the interface.</td>
<td>Type the IPv4 address with /32 as the subnet mask. For example: 10.10.10.1/32</td>
</tr>
<tr>
<td></td>
<td>The following rules apply:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ You cannot specify more than one IPv4 address.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Do not assign the following IPv4 addresses:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ A broadcast address (255.255.255.255)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ A class E address (240.0.0.0 to 255.255.255.254)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ A loopback address (127.0.0.0 to 127.255.255.255)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ A multicast address (224.0.0.0 to 239.255.255.255)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ An address with 0 as the first byte or an address with 0 or 255 as the last byte</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ The VoIP interface needs a point-to-point connection to the TGM550. To configure the point-to-point connection, specify /32 as the subnet mask in the IPv4 address.</td>
<td></td>
</tr>
<tr>
<td>Destination Address</td>
<td>Specifies the IP address of the TGM550.</td>
<td>Type the IP address of the TGM550—for example, 10.10.10.2.</td>
</tr>
<tr>
<td></td>
<td>CAUTION: Applying a new or modified IP address resets the TGM550. For existing configurations, ensure that the TGM550 configuration is saved (see “Saving the TGM550 Configuration” on page 283) and that the TGM550 module is carrying no voice traffic. You cannot specify more than one IP address. For more information, see “TGM550 IP Addressing Guidelines” on page 266.</td>
<td></td>
</tr>
<tr>
<td>Physical Interface Description</td>
<td>(Optional) Adds supplemental information about the VoIP physical interface on the router.</td>
<td>Type a text description of the physical VoIP interface in the box to clearly identify it in monitoring displays.</td>
</tr>
</tbody>
</table>

**TGM Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGC List</td>
<td>Specifies the IP address of at least one and up to four Media Gateway Controllers (MGCs) with which the TGM550 must be registered.</td>
</tr>
<tr>
<td></td>
<td>The first MGC in the list is the primary MGC. The TGM550 searches for the primary MGC first. If it cannot connect to the primary MGC, the TGM550 searches for the next MGC on the list, and so on.</td>
</tr>
</tbody>
</table>

1. Type the IP address of the MGC.  
2. Click **Add**.  
To delete an IP address, select it in the MGC List box, then click **Delete**.
Configuring VoIP with a Configuration Editor

To configure VoIP on a device, perform the following tasks marked (Required). Perform other tasks if needed on your network.

- Configuring the VoIP Interface (Required) on page 272
- Configuring the Media Gateway Controller List (Required) on page 273
- Configuring Dynamic Call Admission Control on WAN Interfaces (Optional) on page 275
- Modifying the IP Address of the TGM550 on page 277

Configuring the VoIP Interface (Required)

You must assign a local IP address to the vp-pim/0/0 interface on the Services Router and also a destination IP address to the TGM550 so that they can communicate with each other.

To configure the VoIP interface on the device:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 74 on page 272.
3. If you are finished configuring the router, commit the configuration.
4. Continue with “Configuring the Media Gateway Controller List (Required)” on page 273.

Table 74: Configuring the VoIP Interface

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Interfaces level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI</td>
<td>From the [edit] hierarchy level, enter edit interfaces vp-3/0/0</td>
</tr>
<tr>
<td></td>
<td>2. Next to Interfaces, click Edit.</td>
<td>Enter edit interfaces vp-3/0/0</td>
</tr>
<tr>
<td>Select the VoIP interface—for example, vp-3/0/0.</td>
<td>In the Interface name column, click the VoIP interface name vp-3/0/0.</td>
<td>Enter edit unit 0</td>
</tr>
<tr>
<td>Create the logical unit 0.</td>
<td>1. Next to Unit, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. In the Interface unit number box, type 0.</td>
<td></td>
</tr>
</tbody>
</table>

NOTE: You cannot configure more than one logical unit on the VoIP interface. The logical unit number must be 0.
### Table 74: Configuring the VoIP Interface (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the source IPv4 address—for example, 10.10.10.1/32—for the VoIP interface.</td>
<td>1. Under Family, select the <strong>Inet</strong> check box and click <strong>Configure</strong>.</td>
<td>Enter</td>
</tr>
<tr>
<td></td>
<td>2. Next to Address, click <strong>Add new entry</strong>.</td>
<td>set family inet address 10.10.10.1/32 destination 10.10.10.2</td>
</tr>
<tr>
<td></td>
<td>3. In the Source box, type 10.10.10.1/32.</td>
<td></td>
</tr>
<tr>
<td>The following rules apply:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ You cannot specify more than one IPv4 address.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Do not assign the following IPv4 addresses:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ A broadcast address (255.255.255.255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ A class E address (240.0.0.0 to 255.255.255.254)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ A loopback address (127.0.0.0 to 127.255.255.255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ A multicast address (224.0.0.0 to 239.255.255.255)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ An address with 0 as the first byte or an address with 0 or 255 as the last byte</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ The VoIP interface needs a point-to-point connection to the TGM550. To configure the point-to-point connection, specify /32 as the subnet mask in the IPv4 address.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the destination IP address—for example 10.10.10.2—for the TGM550.</td>
<td>1. In the Destination box, type 10.10.10.2.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>OK</strong> until you return to the Interfaces page.</td>
<td></td>
</tr>
<tr>
<td>The TGM550 uses this IP address to identify itself when communicating with other devices, particularly the Media Gateway Controller (MGC).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CAUTION:</strong> Applying a new or modified IP address resets the TGM550. For existing configurations, ensure that the TGM550 configuration is saved (see “Saving the TGM550 Configuration” on page 283) and that the TGM550 module is carrying no voice traffic.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>You cannot specify more than one IP address. For more information, see “TGM550 IP Addressing Guidelines” on page 266.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring the Media Gateway Controller List (Required)

To provide telephony services, the TGM550 must be registered with at least one Media Gateway Controller (MGC). You can configure the IP addresses of up to four
MGCs that the TGM550 can connect to in the event of a link failure. For more information, see “Media Gateway Controller” on page 263.

In addition to configuring the MGC list from a J-Web Quick Configuration page (see Table 75 on page 270) and the JUNOS CLI, you can log in to the TGM550 and configure the list. For more information, see the Administration for the Avaya IG550 Integrated Gateway at http://support.avaya.com.

This section contains the following topics:

- Configuring an MGC List and Adding Addresses on page 274
- Clearing an MGC List on page 275

### Configuring an MGC List and Adding Addresses

In the following example, a TGM550 installed in slot 2 of a Services Router has the IP address 10.10.10.2. The TGM550 needs to have registered a primary MGC at address 172.16.0.0, and second and third MGC at addresses 10.10.10.30 and 10.10.10.40.

To configure the MGC list with the JUNOS CLI:

1. Enter operational mode on the JUNOS CLI.
2. Configure the IP addresses of the Media Gateway Controllers, by entering the `set tgm fpc slot media-gateway-controller` command with the IP addresses of the primary, second, and third MGC:

   ```
   user@host> set tgm fpc 2 media-gateway-controller [172.16.0.0 10.10.10.30 10.10.10.40]
   ```

   **NOTE:** Running the `set tgm fpc slot media-gateway-controller` command updates the startup configuration on the TGM550. You do not need to run the `copy running-config start-config` command to save the configuration on the module.

3. Log in to the TGM550 with SSH, and verify that each MGC can be reached over the network.

   ```
   user@host> ssh 10.10.10.2
   password> root
   TGM550-00<root>#! ping 172.16.0.0
   ... 
   TGM550-00<root>#! ping 10.10.10.30
   ... 
   TGM550-00<root>#! ping 10.10.10.40
   ... 
   ```

4. Do one of the following:
To control bandwidth assignments for voice traffic, continue with “Configuring Dynamic Call Admission Control on WAN Interfaces (Optional)” on page 275.

To verify that VoIP is configured correctly on the router, see “Verifying the VoIP Configuration” on page 283.

Clearing an MGC List

In the following example, a TGM550 is installed in slot 2 of the router.

To remove all the IP addresses from the MGC list:
1. Enter operational mode on the CLI.
2. Enter the `clear tgm fpc slot media-gateway-controller` command:

   ```
   user@host> clear tgm fpc 2 media-gateway-controller
   ```

   The `clear` command removes all the MGC IP addresses. You cannot clear the IP address of a single MGC with this command.
3. Add one or more new MGC IP addresses. (See “Configuring an MGC List and Adding Addresses” on page 274.)

Configuring Dynamic Call Admission Control on WAN Interfaces (Optional)

To configure dynamic call admission control (CAC), you define the bearer bandwidth limit (BBL) and activation priority on each WAN interface responsible for providing call bandwidth.

- The activation priority has a range from 1 through 255. The default value is 50.
- The BBL has a range from 0 Kbps through 9999 Kbps. The default BBL value of –1 Kbps indicates that the complete bandwidth of the interface is available for voice traffic. Use a BBL of 0, which indicates that no bandwidth is available for bearer traffic on the MGC, to use the interface for signaling only.

In this example, a Gigabit Ethernet, T1, and ISDN BRI interface are configured with the BBL and activation priority values shown in Table 75 on page 275.

### Table 75: Dynamic CAC Configuration Example

<table>
<thead>
<tr>
<th>Interface Providing Call Bandwidth</th>
<th>Bearer Bandwidth Limit (BBL) Value</th>
<th>Activation Priority Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigabit Ethernet</td>
<td>3000 Kbps</td>
<td>200</td>
</tr>
<tr>
<td>T1</td>
<td>1000 Kbps</td>
<td>150</td>
</tr>
<tr>
<td>ISDN BRI</td>
<td>128 Kbps</td>
<td>100</td>
</tr>
</tbody>
</table>
The Gigabit Ethernet interface is used as the primary link for providing call bandwidth because it has the highest activation priority value. When the Gigabit Ethernet interface is active, the TGM550 reports its BBL value of 3000 Kbps to the MGC. If the Gigabit Ethernet interface fails, the TGM550 automatically switches over to the T1 interface because it has the next highest activation priority. The TGM550 now reports the BBL value of the T1 interface to the MGC. If the T1 interface also fails, the TGM550 switches over to the ISDN BRI interface and reports the BBL value of the ISDN BRI interface to the MGC. Configuring dynamic CAC on multiple WAN interfaces allows the MGC to automatically control the call bandwidth when interfaces responsible for providing call bandwidth are unavailable.

For more information about dynamic CAC, see “Dynamic Call Admission Control Overview” on page 264.

To configure dynamic CAC on Services Router WAN interfaces:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 76 on page 276.
3. If you are finished configuring the router, commit the configuration.
5. Verify that dynamic CAC is configured correctly, see “Verifying the VoIP Configuration” on page 283.

Table 76: Configuring Dynamic CAC

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Interfaces</strong> level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI</td>
<td>From the [edit] hierarchy level, enter edit interfaces ge-0/0/3</td>
</tr>
<tr>
<td></td>
<td>2. Next to Interfaces, click Edit</td>
<td></td>
</tr>
<tr>
<td>Select the Gigabit Ethernet interface—for example, <strong>ge-0/0/3</strong>.</td>
<td>In the Interface name column, click <strong>ge-0/0/3</strong></td>
<td></td>
</tr>
<tr>
<td>Configure dynamic CAC on logical unit 0 of the Gigabit Ethernet interface with the activation priority and BBL values given in Table 75 on page 275.</td>
<td>1. Under Unit, next to 0, click Edit</td>
<td>1. Enter edit unit 0</td>
</tr>
<tr>
<td></td>
<td>2. Next to Dynamic call admission control, click <strong>Configure</strong> or <strong>Edit</strong></td>
<td>2. Enter set dynamic-call-admission-control activation-priority 200 bearer-bandwidth-limit 3000</td>
</tr>
<tr>
<td></td>
<td>3. In the Activation priority box, type 200</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. In the Bearer bandwidth limit box, type 3000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>OK</strong> until you return to the Interfaces page</td>
<td></td>
</tr>
</tbody>
</table>
Table 76: Configuring Dynamic CAC (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the T1 interface—for example, t1-6/0/0.</td>
<td>In the Interface name column, click t1-6/0/0.</td>
<td>From the [edit] hierarchy level, enter edit interfaces t1-6/0/0.</td>
</tr>
</tbody>
</table>
| Configure dynamic CAC on logical unit 0 of the T1 interface with the activation priority and BBL values given in Table 75 on page 275. | 1. Under Unit, next to 0, click Edit.  
2. Next to Dynamic call admission control, click Configure or Edit.  
3. In the Activation priority box, type 150.  
4. In the Bearer bandwidth limit box, type 1000.  
5. Click OK until you return to the Interfaces page. | 1. Enter edit unit 0  
2. Enter set dynamic-call-admission-control activation-priority 150 bearer-bandwidth-limit 1000 |
| Select the ISDN BRI interface—for example, br-1/0/3. | In the Interface name column, click br-1/0/3. | From the [edit] hierarchy level, enter edit interfaces br-1/0/3. |
| Configure dynamic CAC on logical unit 0 of the ISDN BRI interface with the activation priority and BBL values given in Table 75 on page 275. | 1. Under Unit, next to 0, click Edit.  
2. Next to Dynamic call admission control, click Configure or Edit.  
3. In the Activation priority box, type 100.  
4. In the Bearer bandwidth limit box, type 128.  
5. Click OK. | 1. Enter edit unit 0  
2. Enter set dynamic-call-admission-control activation-priority 100 bearer-bandwidth-limit 128 |

Modifying the IP Address of the TGM550

**CAUTION:** The TGM550 is reset when you commit the configuration after modifying the IP address. Before modifying the TGM550 IP address, take the following precautions:

- Log into the TGM550 and enter `copy running-config startup-config` to save the TGM550 configuration. (For login instructions, see “Accessing and Administering the TGM550 CLI” on page 278.)
- Ensure that the TGM550 is not currently handling voice traffic.

To modify the IP address of the TGM550:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 77 on page 278.
3. If you are finished configuring the router, commit the configuration.

Table 77: Modifying the IP Address of the TGM550

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Interfaces level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit interfaces vp-3/0/0 unit 0</td>
</tr>
<tr>
<td></td>
<td>2. Next to Interfaces, click Edit.</td>
<td></td>
</tr>
<tr>
<td>Select the logical VoIP interface—for example, vp-3/0/0.0.</td>
<td>1. In the Interface name column, click the VoIP interface name vp-3/0/0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. In the Interface unit number box, click 0.</td>
<td></td>
</tr>
<tr>
<td>Modify the destination IP address for the TGM550 to a different address—for example, 10.10.10.80.</td>
<td>1. Under Family, next to Inet, click Edit.</td>
<td>Enter set family inet address 10.10.10.1/32 destination 10.10.10.80</td>
</tr>
<tr>
<td>For guidelines, see “TGM550 IP Addressing Guidelines” on page 266.</td>
<td>2. Under Address, in the Broadcast column, click Edit.</td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> You cannot specify more than one IP address.</td>
<td>3. In the Destination box, type 10.10.10.80.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Click OK.</td>
<td></td>
</tr>
</tbody>
</table>

Accessing and Administering the TGM550 CLI

The CLI on the TGM550 allows you to configure, monitor, and diagnose the TGM550 and TIMs installed in a Services Router. You can access the TGM550 from a management device attached to the TGM550 console port or by opening a Telnet or secure shell (SSH) session from the JUNOS CLI on the Services Router.

You can also open a remote Telnet or SSH session directly to the TGM550 from a network location, or indirectly through the JUNOS CLI from a dial-up connection with a USB modem attached to the router.

This section contains the following topics. For complete information about the TGM550 CLI, see the Administration Guide and CLI Reference for the Avaya IG550 Integrated Gateway.

- TGM550 Access Requirements on page 279
- Connecting Through the TGM550 Console Port on page 279
- Connecting to the TGM550 with SSH on page 280
- Accessing the TGM550 with Telnet on page 280
- Accessing the Services Router from the TGM550 on page 282
TGM550 Access Requirements

Administrators can use the root password to access the TGM550 initially, but all users need a TGM550 user account (username and password) set up by the network administrator for regular access to the module. For information about user accounts on a TGM550, see the Administration Guide and CLI Reference for the Avaya IG550 Integrated Gateway at http://support.avaya.com.

NOTE: You cannot use a Services Router user account to access the TGM550 CLI.

- A console connection requires the Ethernet rollover cable and adapter provided with the TGM550. (See “Connecting Through the TGM550 Console Port” on page 279.)
- An SSH connection requires that the TGM550 have an IP address assigned.
- A Telnet connection to the TGM550 requires that the module have an IP address and that Telnet service be enabled on the module.

To assign an IP address to the TGM550, see “Configuring VoIP Interfaces with Quick Configuration” on page 269 or “Configuring the VoIP Interface (Required)” on page 272.

To enable Telnet, see “Accessing the TGM550 with Telnet” on page 280.

Connecting Through the TGM550 Console Port

To connect to the TGM550 through its console port:

1. Turn off the power to the management device, such as a PC or laptop computer, that you are using to access the TGM550.

2. Plug one end of an Ethernet rollover cable provided with the TGM550 into the Rj-45 to DB-9 serial port adapter provided with the TGM550.

3. Plug the Rj-45 to DB-9 serial port adapter provided with the TGM550 into the serial port on the management device.

4. Connect the other end of the Ethernet rollover cable to the console port (CONSOLE) on the TGM550.

5. Turn on power to the management device.
6. Start your asynchronous terminal emulation application (such as Microsoft Windows Hyper Terminal), and select the appropriate COM port to use (for example, COM1).

7. Configure the port settings as follows:
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: Hardware

8. At the login prompt, type your username and press Enter.

9. At the password prompt, type your password and press Enter.

**Connecting to the TGM550 with SSH**

To connect to the TGM550 with SSH:

1. Ensure that the TGM550 has an IP address. (See “Configuring VoIP Interfaces with Quick Configuration” on page 269 or “Configuring the VoIP Interface (Required)” on page 272.)

2. From the JUNOS CLI or a remote connection, enter the following command:

   ```bash
   ssh ip-address
   ```

**Accessing the TGM550 with Telnet**

By default, Telnet service is not enabled on the TGM550. You must enable Telnet service on the TGM550 before you can telnet to the TGM550 from other devices or from the TGM550 to other devices.

---

**CAUTION:** Telnet connections are not encrypted and therefore can be intercepted.

---

This section contains the following topics:

- Enabling Telnet Service on the TGM550 on page 280
- Connecting to the TGM550 with Telnet on page 281
- Disabling Telnet Service on the TGM550 on page 281

**Enabling Telnet Service on the TGM550**

To enable Telnet service on the TGM550:
1. Connect to the TGM550 through the console port. (See “Connecting Through the TGM550 Console Port” on page 279.

2. Enable incoming Telnet connections, by entering the following command, replacing port with the Telnet port number:

   ```
   TGM550-004(super)# ip telnet port port
   ```

3. Enable outgoing Telnet connections from the TGM550 to other devices, by entering

   ```
   TGM550-004(super)# ip telnet-client
   ```

4. Save the configuration by entering:

   ```
   TGM550-004(super)# copy running-config startup-config
   ```

### Connecting to the TGM550 with Telnet

To connect to the TGM550 with Telnet:

1. Ensure that Telnet is enabled on the TGM550. (See “Enabling Telnet Service on the TGM550” on page 280.)

2. Ensure that the TGM550 has an IP address. (See “Configuring VoIP Interfaces with Quick Configuration” on page 269 or “Configuring the VoIP Interface (Required)” on page 272.)

3. From the JUNOS CLI or a remote connection, enter the following command:

   ```
   telnet ip-address
   ```

### Disabling Telnet Service on the TGM550

To disable Telnet service on the TGM550:

1. Connect to the TGM550 through the console port. For more information, see “Connecting Through the TGM550 Console Port” on page 279.

2. Disable incoming Telnet connections, by entering the following command, replacing port with the Telnet port number:

   ```
   TGM550-004(super)# no ip telnet
   ```

3. Disable outgoing Telnet connections from the TGM550 to other devices, by entering

   ```
   TGM550-004(super)# no ip telnet-client
   ```

4. Save the configuration:

   ```
   TGM550-004(super)# copy running-config startup-config
   ```
Accessing the Services Router from the TGM550

You can access the Services Router from the CLI on its installed TGM550 in the following ways:

- Enter the `session chassis` command.
- Enter the `telnet` or `ssh` command.

**NOTE:** Before using the TGM550 CLI `telnet` command, ensure that Telnet service is enabled on the TGM550. For more information, see “Enabling Telnet Service on the TGM550” on page 280.

Resetting the TGM550

**CAUTION:** Before resetting the TGM550, take the following precautions:

- Log into the TGM550 and enter `copy running-config startup-config` to save the TGM550 configuration. (For login instructions, see “Accessing and Administering the TGM550 CLI” on page 278.)
- Ensure that the TGM550 is not currently handling voice traffic.

You can reset the TGM550 from the module itself or from the Services Router.

To reset the TGM550 from the module itself, do one of the following:

- Press the RST button on the TGM550.
- Log into the TGM550, and enter the `reset` command. (For login instructions, see “Accessing and Administering the TGM550 CLI” on page 278.)

To reset the TGM550 from the device:

1. Enter operational mode in the CLI.
2. Enter the `request chassis fpc slot slot-number restart` command.
   
   For example, to reset a TGM550 installed in slot 2 on the router chassis, enter
   
   `user@host> request chassis fpc slot 2 restart`

**NOTE:** You cannot reset the TIMs using the `request chassis fpc slot slot-number restart` command. TIMs are administered only from the TGM550.
Saving the TGM550 Configuration

To save the configuration on the TGM550:

1. Log in to the TGM550. (For login instructions, see “Accessing and Administering the TGM550 CLI” on page 278.)
2. Save the configuration, by entering

   TGM550-004(super)# copy running-config startup-config

For more information about saving a TGM550 configuration, see the Administration Guide and CLI Reference for the Avaya IG550 Integrated Gateway at http://support.avaya.com.

Verifying the VoIP Configuration

To verify the VoIP configuration, perform the following tasks:

- Verifying the VoIP Interface on page 283
- Verifying the Media Gateway Controller List on page 285
- Verifying Bandwidth Available for VoIP Traffic on page 285

Verifying the VoIP Interface

**Purpose**  
Verify that the VoIP interface is correctly configured.

**Action**  
From the CLI, enter the `show interfaces extensive` command.

**Sample Output**  

```
user@host> show interfaces vp-3/0/0 extensive
Physical interface: vp-3/0/0, Enabled, Physical link is Up
   Interface index: 141, SNMP ifIndex: 21, Generation: 142
   Type: VP-AV, Link-level type: VP-AV, MTU: 1518, Speed: 10mbps
Device flags   : Present Running
Link type      : Full-Duplex
Link flags     : None
Physical info  : Unspecified
CoS queues     : 8 supported, 8 maximum usable queues
Last flapped   : 2006-09-29 09:28:32 UTC (4d 18:35 ago)
Statistics last cleared: Never
Traffic statistics:
   Input  bytes  :  8886912         0 bps
   Output bytes :   6624354         0 bps
   Input  packets:      90760         0 pps
   Output packets:     65099          0 pps
Input errors:
   Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards: 0,
   Resource errors: 0
Output errors:
   Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors: 0
   Egress queues: 8 supported, 8 in use
```
The output shows a summary of interface information. Verify the following information:

- **The physical interface is Enabled.** If the interface is shown as Disabled, do either of the following:
  - In the CLI configuration editor, delete the disable statement at the [edit interfaces interface-name] level of the configuration hierarchy.
  - In the J-Web configuration editor, clear the Disable check box on the Interfaces > interface-name page.

- **The physical link is Up.** A link state of Down indicates that the interface is disabled. Do one of the following:
  - In the CLI configuration editor, delete the disable statement at the [edit interfaces interface-name] level of the configuration hierarchy.
  - In the J-Web configuration editor, clear the Disable check box on the Interfaces > interface-name page.

- **The Last Flapped time is an expected value.** The Last Flapped time indicates the last time the physical interface became unavailable and then available again. Unexpected flapping indicates likely link-layer errors.

- **The traffic statistics reflect expected input and output rates.** Verify that the number of inbound and outbound bytes and packets matches expected throughput for the physical interface. To clear the statistics and see only new changes, use the clear interfaces statistics interface-name command.
Verifying the Media Gateway Controller List

Purpose   Verify that the Media Gateway Controller (MGC) list is correctly configured and that the MGCs are reachable over the network.

Action   From the operational mode in the CLI, enter `show tgm fpc slot-number media-gateway-controller`.

Sample Output   

```
user@host> show tgm fpc 2 media-gateway-controller
Media gateway controller(s): 173.26.232.77
                          10.10.10.30
                          10.10.10.40
```

Meaning   The output shows the configured MGC list. Verify the following:

- The IP addresses and the order of the IP addresses in the MGC list are correct. The first MGC on the list is the primary MGC. The TGM550 searches for the primary MGC first. If it cannot connect to the primary MGC or loses its connection to the primary MGC, it attempts to connect to the next MGC in the list, and so on.
- Use the JUNOS CLI `ping` command or the J-Web ping host tool (**Troubleshoot > Ping Host**) to verify that the configured MGCs can be reached over the network.

Related Topics   For a complete description of `show tgm fpc` output, see the **Junos Interfaces Command Reference**.

Verifying Bandwidth Available for VoIP Traffic

Purpose   Verify that the dynamic call admission control (CAC) configuration supports sufficient bandwidth for VoIP traffic.

Action   From the operational mode in the CLI, enter `show tgm dynamic-call-admission-control`.

Sample Output   

```
user@host> show tgm dynamic-call-admission-control
Reported bearer bandwidth limit: 3000  Kbps

Interface       State       Activation priority  Bearer bandwidth limit (Kbps)
                 limit (Kbps)          
ge-0/0/3.0      up           200                 3000
t1-6/0/0.0      up           150                 1000
br-1/0/3.0      up           50                  128
```

Meaning   The output shows the dynamic CAC configuration. Verify the following information:
The activation priority and bearer bandwidth limit (BBL) configured on individual interfaces are correct.

The Reported bearer bandwidth limit field displays the bandwidth available for VoIP traffic. Ensure that the bandwidth is sufficient for VoIP traffic.

Related Topics For a complete description of `show tgm dynamic-call-admission-control` output, see the Junos Interfaces Command Reference.

Frequently Asked Questions About the VoIP Interface

Use answers to the following question to solve configuration problems on a VoIP interface:

TGM550 Is Installed But the VoIP Interface Is Unavailable

**Problem**—I installed the TGM550 Telephony Gateway Module and configured the VoIP interface—for example, `vp-3/0/0`—but the interface is not accessible. The `show chassis hardware` command displays the TGM550 installed on slot 3. However, the `show interfaces terse` command does not display the `vp-3/0/0` interface, and the `show interfaces vp-3/0/0` command displays an error:

```
user@host> show interfaces vp-3/0/0
error: device vp-3/0/0 not found
```

**Solution**—The VoIP interface might be unavailable because the TGM550 firmware version is not compatible with the JUNOS Software version installed on the device. For more information, see “TGM550 Firmware Compatibility with JUNOS Internet Software” on page 266.

To correct the TGM550 firmware and JUNOS Software version compatibility error:

1. Check the router’s system log messages for a version incompatibility error similar to the following:

```
Jan 5 11:07:03 host fwdd[2857]: TGMT: RE (1.0) - TGM (2.0) major protocol version mismatch: not marking TGM slot ready
```

2. If the error exists, connect to the TGM550 through the console port. (See “Connecting Through the TGM550 Console Port” on page 279.

3. View the TGM550 firmware version, by entering

```
TGM550-003(super)# show image version
```

<table>
<thead>
<tr>
<th>Bank</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>A (current)</td>
<td>26.23.0</td>
</tr>
<tr>
<td>B</td>
<td>26.22.0</td>
</tr>
</tbody>
</table>

In this example, the current TGM550 firmware version is 26.23.0.
4. Refer to the *Communication Manager Software & Firmware Compatibility Matrix* at [http://support.avaya.com](http://support.avaya.com) to identify the JUNOS Software version that is compatible with the current TGM550 firmware version.

5. Upgrade the router with the compatible JUNOS Software version.
Chapter 10
Configuring Point-to-Point Protocol over Ethernet

Point-to-Point Protocol over Ethernet (PPPoE) connects multiple hosts on an Ethernet LAN to a remote site through a single customer premises equipment (CPE) device—a Juniper Networks device. Hosts share a common digital subscriber line (DSL), a cable modem, or a wireless connection to the Internet. To use PPPoE, you must initiate a PPPoE session, encapsulate Point-to-Point Protocol (PPP) packets over Ethernet, and configure the device as a PPPoE client.

NOTE: Juniper Networks devices with asymmetric digital subscriber line (ADSL) or symmetric high-speed DSL (SHDSL) interfaces can use PPPoE over Asynchronous Transfer Mode (ATM) to connect through DSL lines only, not for direct ATM connections.

You can use the J-Web Quick Configuration, J-Web configuration editor, or CLI configuration editor to configure PPPoE.

For information about which devices support the features documented in this chapter, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.

This chapter contains the following topics:
- PPPoE Terms on page 290
- PPPoE Overview on page 291
- Before You Begin on page 293
- Configuring PPPoE Interfaces with Quick Configuration on page 293
- Configuring PPPoE Encapsulation on an Ethernet Interface on page 296
- Configuring PPPoE Encapsulation on an ATM-over-ADSL or ATM-over-SHDSL Interface on page 297
- Configuring PPPoE Interfaces on page 298
- Configuring CHAP on a PPPoE Interface (Optional) on page 300
- Verifying a PPPoE Configuration on page 303
**PPPoE Terms**

Before configuring PPPoE, become familiar with the terms defined in Table 78 on page 290.

**Table 78: PPPoE Terms**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>customer premises equipment (CPE)</td>
<td>Device that acts as a PPPoE client in a PPPoE session— for example, a Juniper Networks device.</td>
</tr>
<tr>
<td>Logical Link Control (LLC)</td>
<td>Encapsulation protocol that allows transport of multiple protocols over a single ATM virtual connection.</td>
</tr>
<tr>
<td>Point-to-Point Protocol (PPP)</td>
<td>Encapsulation protocol for transporting IP traffic over point-to-point links.</td>
</tr>
<tr>
<td>PPP over Ethernet (PPPoE)</td>
<td>Network protocol that encapsulates PPP frames in Ethernet frames and connects multiple hosts over a simple bridging access device to a remote access concentrator.</td>
</tr>
<tr>
<td>PPPoE Active Discovery Initiation (PADI) packet</td>
<td>Initiation packet that is broadcast by the client to start the discovery process.</td>
</tr>
<tr>
<td>PPPoE Active Discovery Offer (PADO) packet</td>
<td>Offer packets sent to the client by one or more access concentrators in reply to a PADI packet.</td>
</tr>
<tr>
<td>PPPoE Active Discovery Request (PADR) packet</td>
<td>Packet sent by the client to one selected access concentrator to request a session.</td>
</tr>
<tr>
<td>PPPoE Active Discovery Session-Confirmation (PADS) packet</td>
<td>Packet sent by the selected access concentrator to confirm the session.</td>
</tr>
<tr>
<td>PPPoE Active Discovery Termination (PADT) packet</td>
<td>Packet sent by either the client or the access concentrator to terminate a session.</td>
</tr>
<tr>
<td>PPPoE over ATM</td>
<td>Network protocol that encapsulates PPPoE frames in Asynchronous Transfer Mode (ATM) frames for asymmetric digital subscriber line (ADSL) or symmetric high-speed DSL (SHDSL) transmission, and connects multiple hosts over a simple bridging access device to a remote access concentrator.</td>
</tr>
<tr>
<td>virtual path identifier (VPI)</td>
<td>An identifier of the virtual path that establishes a route between two devices in a network.</td>
</tr>
</tbody>
</table>
| virtual channel identifier (VCI)                    | An identifier of the virtual channel inside a virtual path. Each virtual path identifier (VPI) can contain multiple virtual channels, each represented by a VCI. }
PPPoE Overview

On the Juniper Networks device, PPPoE establishes a point-to-point connection between the client (Juniper Networks device) and the server, also called an access concentrator. Multiple hosts can be connected to the device, and their data can be authenticated, encrypted, and compressed before the traffic is sent to the PPPoE session on the Juniper Networks device’s Fast Ethernet, Gigabit Ethernet, ATM-over-ADSL, or ATM-over-SHDSL interface. PPPoE is easy to configure and allows services to be managed on a per-user basis rather than on a per-site basis.

This overview contains the following topics:
- PPPoE Interfaces on page 291
- PPPoE Stages on page 292
- Optional CHAP Authentication on page 293

PPPoE Interfaces

The device’s PPPoE interface to the access concentrator can be a Fast Ethernet interface, a Gigabit Ethernet interface, an ATM-over-ADSL interface, or an ATM-over-SHDSL interface. The PPPoE configuration is the same for all interfaces. The only difference is the encapsulation for the underlying interface to the access concentrator:
- If the interface is Ethernet, use a PPPoE encapsulation.
- If the interface is ATM-over-ADSL or ATM-over-SHDSL, use a PPPoE over ATM encapsulation.

Ethernet Interface

The device encapsulates each PPP frame in an Ethernet frame and transports the frames over an Ethernet loop. Figure 39 on page 291 shows a typical PPPoE session between a device and an access concentrator on the Ethernet loop.

Figure 39: PPPoE Session on the Ethernet Loop

ATM-over-ADSL or ATM-over-SHDSL Interface

When an ATM network is configured with a point-to-point connection, PPPoE can use ATM Adaptation Layer 5 (AAL5) for framing PPPoE-encapsulated packets. The
AAL5 protocol provides a virtual connection between the client and the server within the same network. The device encapsulates each PPPoE frame in an ATM frame and transports each frame over an ADSL or SHDSL loop and a digital subscriber line access multiplexer (DSLAM). For example, Figure 40 on page 292 shows a typical PPPoE over ATM session between a device and an access concentrator on an ADSL loop.

Figure 40: PPPoE Session on an ADSL Loop

**PPPoE Stages**

PPPoE has two stages, the discovery stage and the PPPoE session stage. In the discovery stage, the client discovers the access concentrator by identifying the Ethernet media access control (MAC) address of the access concentrator and establishing a PPPoE session ID. In the PPPoE session stage, the client and the access concentrator build a point-to-point connection over Ethernet, based on the information collected in the discovery stage.

**PPPoE Discovery Stage**

A device initiates the PPPoE discovery stage by broadcasting a PPPoE Active Discovery Initiation (PADI) packet. To provide a point-to-point connection over Ethernet, each PPPoE session must learn the Ethernet MAC address of the access concentrator and establish a session with a unique session ID. Because the network might have more than one access concentrator, the discovery stage allows the client to communicate with all of them and select one.

**NOTE:** A device cannot receive PPPoE packets from two different access concentrators on the same physical interface.

**PPPoE Session Stage**

The PPPoE session stage starts after the PPPoE discovery stage is over. The access concentrator can start the PPPoE session after it sends a PPPoE Active Discovery Session-Confirmation (PADS) packet to the client, or the client can start the PPPoE session after it receives a PADS packet from the access concentrator. A device supports multiple PPPoE sessions on each interface, but no more than 256 PPPoE sessions per device.
Each PPPoE session is uniquely identified by the Ethernet address of the peer and the session ID.

**Optional CHAP Authentication**

For interfaces with PPPoE encapsulation, you can configure interfaces to support the PPP Challenge Handshake Authentication Protocol (CHAP). When you enable CHAP on an interface, the interface can authenticate its peer and be authenticated by its peer.

If you set the `passive` option to handle incoming CHAP packets only, the interface does not challenge its peer. However, if the interface is challenged, it responds to the challenge. If you do not set the `passive` option, the interface always challenges its peer.

You can configure Remote Authentication Dial-In User Service (RADIUS) authentication of PPP sessions using CHAP. CHAP enables you to send RADIUS messages through a routing instance to customer RADIUS servers in a private network. For more information, see the *Junos System Basics Configuration Guide*.

For more information about CHAP, see the *Junos Network Interfaces Configuration Guide*.

**Before You Begin**

Before you begin configuring PPPoE, complete the following tasks:

- Establish basic connectivity. See the Getting Started Guide for your device.
- Configure network interfaces. See “Configuring a Fast Ethernet Interface with Quick Configuration,” “Configuring Gigabit Ethernet Interfaces—Quick Configuration,” or “Configuring Digital Subscriber Line Interfaces.”

**Configuring PPPoE Interfaces with Quick Configuration**

To configure properties on a PPPoE interface:

1. In the J-Web user interface, select **Configure > Interfaces**.

   A list of the network interfaces present on the device is displayed, as shown in Figure 12 on page 74 (see “Network Interface Naming” on page 16). The third column indicates whether the interface has been configured.

2. Select `pp0`.

   The PPPoE Interfaces Quick Configuration main page is displayed, as shown in Figure 41 on page 294.
3. Enter information into the Quick Configuration pages, as described in Table 79 on page 295.

4. From the PPPoE Interfaces Quick Configuration main page, click one of the following buttons:
   - To apply the configuration and stay on the PPPoE Quick Configuration main page, click **Apply**.
   - To apply the configuration and return to the Interfaces Quick Configuration page, click **OK**.
   - To cancel your entries and return to the Interfaces Quick Configuration page, click **Cancel**.

5. To verify that the PPPoE interface is configured correctly, see “Verifying a PPPoE Configuration” on page 303.
### Table 79: PPPoE Quick Configuration Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logical Interfaces</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Interfaces</td>
<td>Lists the logical interfaces for the PPPoE physical interface.</td>
<td>■ To add a logical interface, click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ To edit a logical interface, select the interface from the list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ To delete a logical interface, select the check box next to the name and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>click <strong>Delete</strong>.</td>
</tr>
<tr>
<td>Add logical interfaces</td>
<td>Defines one or more logical units that you connect to this physical PPPoE</td>
<td>Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>interface. You must define at least one logical unit for a PPPoE interface.</td>
<td></td>
</tr>
<tr>
<td>Logical Interface Description</td>
<td>(Optional) Describes the logical interface.</td>
<td>Type a text description of the logical interface to more clearly identify it in monitoring displays.</td>
</tr>
<tr>
<td>IPv4 Addresses and Prefixes</td>
<td>Specifies one or more IPv4 addresses for the interface.</td>
<td>1. Type one or more IPv4 addresses and prefixes. For example: 10.10.10.10/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Physical Interface Description</td>
<td>(Optional) Adds supplementary information about the physical PPPoE interface.</td>
<td>Type a text description of the PPPoE interface to more clearly identify it in monitoring displays.</td>
</tr>
<tr>
<td><strong>PPP Options</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable CHAP</td>
<td>Enables or disables CHAP authentication on a PPPoE interface.</td>
<td>■ To enable CHAP, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ To disable CHAP, clear the check box.</td>
</tr>
<tr>
<td>CHAP Local Identity (available if CHAP is enabled)</td>
<td>Specifies that the PPPoE interface uses the device's system hostname in CHAP challenge and response packets.</td>
<td>■ To enable, select the check box (the default).</td>
</tr>
<tr>
<td>Use System Host Name</td>
<td></td>
<td>■ To disable, clear the check box.</td>
</tr>
<tr>
<td></td>
<td>If Use System Host Name is disabled, specifies the local name for CHAP to use.</td>
<td>Type a local name for this PPPoE interface.</td>
</tr>
<tr>
<td>Local Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHAP Peer Identity (required if CHAP is enabled)</td>
<td>Identifies the client or peer with which the device communicates on this PPPoE interface.</td>
<td>Type the CHAP client name.</td>
</tr>
<tr>
<td>CHAP Secret (required if CHAP is enabled)</td>
<td>Specifies the secret password for CHAP authentication, known to both sides of the connection.</td>
<td>Type a password that is known to the other side of the connection. Use a combination of letters and numbers that is difficult for others to guess.</td>
</tr>
</tbody>
</table>
Table 79: PPPoE Quick Configuration Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PPPoE Options</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Concentrator</td>
<td>Identifies the access concentrator by a unique name.</td>
<td>Type a name for the access concentrator—for example, ispl.com.</td>
</tr>
<tr>
<td>Auto Reconnect Time</td>
<td>Specifies the number of seconds to wait before reconnecting after a PPPoE session is terminated.</td>
<td>Type a value from 1 through 4294947295 for automatic reconnection—for example, 100 seconds. Type 0 (the default) for immediate reconnection.</td>
</tr>
<tr>
<td>Idle Timeout</td>
<td>Specifies the number of seconds a session can be idle without disconnecting.</td>
<td>Type a value for the timeout. Type 0 if you do not want the session to time out.</td>
</tr>
<tr>
<td>Service Name</td>
<td>Identifies the type of service provided by the access concentrator, such as the name of the Internet service provider (ISP), class, or quality of service.</td>
<td>Type the type of service provided by the access concentrator. For example, <a href="mailto:video@ispl.com">video@ispl.com</a>.</td>
</tr>
<tr>
<td>Underlying Interface</td>
<td>Specifies the logical Ethernet interface or the logical ATM interface as the underlying interface for the PPPoE session.</td>
<td>From the list, select the underlying interface for the PPPoE session—for example, ge-0/0/1.0 or at-2/0/0.0.</td>
</tr>
</tbody>
</table>

**Configuring PPPoE Encapsulation on an Ethernet Interface**

For PPPoE on an Ethernet interface, you configure encapsulation on the logical interface.

In this example, you configure the interface ge-0/0/1 for PPPoE encapsulation.

You can use either J-Web or the CLI configuration editor to configure PPPoE encapsulation on an Ethernet interface.

This topic covers:
- J-Web Configuration on page 296
- CLI Configuration on page 297
- Related Topics on page 297

**J-Web Configuration**

To configure PPPoE encapsulation on an Ethernet interface:

1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Interfaces, click Configure or Edit.
3. In the Interface name box, click ge-0/0/1.
4. In the Interface unit number box, click 0.
5. From the Encapsulation list, select `ppp-over-ether`.
6. Click OK.

**CLI Configuration**

To configure PPPoE encapsulation on an Ethernet interface:

```
user@host# set interfaces ge-0/0/1 unit 0 encapsulation ppp-over-ether
```

**Related Topics**

- Configuring PPPoE Interfaces on page 298
- Configuring CHAP on a PPPoE Interface (Optional) on page 300

**Configuring PPPoE Encapsulation on an ATM-over-ADSL or ATM-over-SHDSL Interface**

For PPPoE on an ATM-over-ADSL or ATM-over-SHDSL interface, you must configure encapsulation on both the physical and logical interfaces. To configure encapsulation on an ATM-over-ADSL or ATM-over-SHDSL physical interface, use Ethernet over ATM encapsulation. To configure encapsulation on an ATM-over-ADSL or ATM-over-SHDSL logical interface, use PPPoE over AAL5 logical link control (LLC) encapsulation. LLC encapsulation allows a single ATM virtual connection to transport multiple protocols.

In this example, you configure the physical interface `at-2/0/0` for Ethernet over ATM encapsulation and then create a logical interface for PPPoE over LLC encapsulation.

You can use either J-Web or the CLI configuration editor to configure PPPoE on an ATM-over-ADSL or ATM-over-SHDSL interface.

This topic covers:

- J-Web Configuration on page 297
- CLI Configuration on page 298
- Related Topics on page 298

**J-Web Configuration**

To set the virtual path identifier (VPI) on an ATM-over-ADSL physical interface:

1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Interfaces, click Configure or Edit.
3. In the Interface name box, click `at-2/0/0`.
4. Next to ATM options, click Configure.
5. Next to Vpi, click Add new entry.
6. In the Vpi number box, type 0.
7. Click OK twice.
To configure the ADSL operating mode on the ATM-over-ADSL physical interface:
1. Next to Dsl options, click Configure.
2. From the Operating mode list, select auto.
3. Click OK twice.

To configure PPPoE encapsulation on the ATM-over-ADSL physical interface:
1. From the Encapsulation list, select ethernet-over-atm.

To create an ATM-over-ADSL logical interface and configure LLC encapsulation:
1. Next to Unit, click Add new entry.
2. In the Interface unit number box, type 0.
3. From the Encapsulation list, select ppp-over-ether-over-atm-llc.
4. In the Multicast vci box, type 0.120.
5. Click OK twice.

**CLI Configuration**

To set the virtual path identifier (VPI) on an ATM-over-ADSL physical interface:
user@host# set interfaces at-2/0/0 atm-options vpi 0

To configure the ADSL operating mode on the ATM-over-ADSL physical interface:
user@host# set interfaces at-2/0/0 dsl-options operating-mode auto

To configure PPPoE encapsulation on the ATM-over-ADSL physical interface:
user@host# set interfaces at-2/0/0 encapsulation ethernet-over-atm

To create an ATM-over-ADSL logical interface and configure LLC encapsulation:
user@host# set interfaces at-2/0/0 unit 0 encapsulation ppp-over-ether-over-atm-llc vci 0.120

**Related Topics**

- Configuring PPPoE Interfaces on page 298
- Configuring CHAP on a PPPoE Interface (Optional) on page 300

**Configuring PPPoE Interfaces**

You create a PPPoE interface with a logical interface unit 0, then specify a logical Ethernet or ATM interface as the underlying interface for the PPPoE session. You then specify other PPPoE options, including the access concentrator and PPPoE session parameters.
In this example, you create the PPPoE interface pp0.0 and specify the logical Ethernet interface ge-0/0/1.0 as the underlying interface. You also set the access concentrator and PPPoE session parameters.

To clear a PPPoE session on the pp0.0 interface, use the clear pppoe sessions pp0.0 command. To clear all sessions on the interface, use the clear pppoe sessions command.

You can use either J-Web or the CLI configuration editor to create and configure the PPPoE interface.

This topic covers:
- J-Web Configuration on page 299
- CLI Configuration on page 300
- Related Topics on page 300

**J-Web Configuration**

To create a PPPoE interface:
1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Interfaces, click Configure or Edit.
3. Next to Interface, click Add new entry.
4. In the Interface name box, type pp0.
5. Click OK.
6. Under Interface name, click pp0.
7. Next to Unit, click Add new entry.
8. In the Interface unit number box, type 0.

To configure PPPoE options:
1. In the Underlying interface box, type ge-0/0/1.0.
2. In the Access concentrator box, type ispl.com.
3. In the Auto reconnect box, type 100.
4. In the Idle timeout box, type 100.
5. Next to Chap, click Configure.
6. In the Client box, type Yes.
7. In the Service name box, type video@ispl.com.

To configure the maximum transmission unit (MTU) of the IPv4 family:
1. In the Inet box, select Yes and then click Configure.
2. In the Mtu box, type 1492.
3. Click OK until you return to the Unit page.
To configure the PPPoE interface address:
1. Next to Inet, click **Edit**.
2. Next to Negotiate address, select **Yes**.
3. Click **OK** until you return to the Unit page.

**CLI Configuration**

To create a PPPoE interface and configure PPPoE options:

```
user@host# set interfaces pp0 unit 0 pppoe-options underlying-interface ge-0/0/1.0
access-concentrator ispl.com auto-reconnect 100 idle-timeout 100 client
service-name video@ispl.com
```

To configure the maximum transmission unit (MTU) of the IPv4 family:

```
user@host# set interfaces pp0 unit 0 family inet mtu 1492
```

To configure the PPPoE interface address:

```
user@host# set interfaces pp0 unit 0 family inet negotiate-address
```

**Related Topics**

- Configuring CHAP on a PPPoE Interface (Optional) on page 300

**Configuring CHAP on a PPPoE Interface (Optional)**

You can configure interfaces with PPPoE encapsulation to support the PPP Challenge Handshake Authentication Protocol (CHAP). When you enable CHAP on an interface, the interface can authenticate its peer and be authenticated by its peer.

In this example, you configure a CHAP access profile, and then apply it to the PPPoE interface **pp0**. You also configure the hostname to be used in CHAP challenge and response packets, and set the passive option for handling incoming CHAP packets.

You can use either J-Web or the CLI configuration editor to configure CHAP on a PPPoE interface.

This topic covers:
- J-Web Configuration on page 300
- CLI Configuration on page 301
- Configuring the PPPoE-Based Radio-Router Protocol on page 302

**J-Web Configuration**

To configure a CHAP access profile:
1. Select **Configure > CLI Tools > Point and Click CLI**.
2. Next to Access, click **Configure** or **Edit**.
3. Next to Profile, click **Add new entry**.
4. In the Profile name box, type **A-ppp-client**.
5. Next to Client, click **Add new entry**.
6. In the Name box, type **client1**.
7. In the Chap secret box, type **my-secret**.
8. Click **OK** until you return to the main Configuration page.

To configure a PPPoE interface with the CHAP access profile:

1. On the main Configuration page next to Interfaces, click **Configure** or **Edit**.
2. In the Interface name box, click **pp0**.
3. In the Interface unit number box, click **0**.
4. Next to Ppp options, click **Configure**.
5. Next to Chap, click **Configure**.
6. In the Access profile box, type **A-ppp-client**.

To configure a hostname for the CHAP challenge and response packets:

1. In the Local name box, type **A-ge-0/0/1.0**.

To set the passive option to handle incoming CHAP packets only:

1. In the Passive box, click **Yes**.
2. Click **OK**.

**CLI Configuration**

To configure a CHAP access profile:

```
user@host# set access profile A-ppp-client client client1 chap-secret my-secret
```

To configure a PPPoE interface with the CHAP access profile:

```
user@host# set interfaces pp0 unit 0 ppp-options chap access-profile A-ppp-client
```

To configure a hostname for the CHAP challenge and response packets:

```
user@host# set interfaces pp0 unit 0 ppp-options chap local-name A-ge-0/0/1.0
```

To set the passive option to handle incoming CHAP packets only:

```
user@host# set interfaces pp0 unit 0 ppp-options chap passive
```
**Configuring the PPPoE-Based Radio-Router Protocol**

Point-to-Point Protocol over Ethernet (PPPoE)-based radio-to-router protocols include messages that define how an external system will provide the device with timely information about the quality of a link's connection. They also include a flow control mechanism to indicate how much data the device can forward. The device can then use the information provided in the PPPoE messages to dynamically adjust the interface speed of PPP links.

For example, a High-band Networking Waveform (HNW) radio provides ground-to-ground or ground-to-air communications with like devices. When the HNW picks up a signal from another device, it initiates a PPPoE session with a directly connected device (router). The PPPoE session encapsulates the packets that are relayed over a PPP link between the local and remote devices. The remote radio then forwards traffic to a remote device using an independent PPPoE session. The two devices exchange Link Control Protocol (LCP) and Internet Protocol Control Protocol (IPCP) messages to configure the link and exchange OSPF messages to establish the network topology.

Each HNW radio monitors the link every 50 milliseconds for changes in the link bandwidth, quality, and utilization. If any changes are detected, the radios announce the new set of metrics to the respective devices through a PPPoE Active Discovery Quality (PADQ) message, which is a nonstandard extension to the PPPoE Discovery Protocol [RFC2516]. The device transforms these metrics into a bandwidth value for the PPP link and compares it to the value currently in use. When the device detects that the difference exceeds a user-specified threshold, it adjusts the speed of the PPP link. OSPF is notified of the change and announces any resulting routing topology changes to its neighbors.

**Overview of CLI Statements**

The CLI statement, `radio-router`, indicates that metrics announcements received on the interface will be processed by the device. When a PPPoE logical interface refers to this as an underlying interface, the device then processes incoming PADQ messages and uses information from the host’s messages to control the flow of traffic and manage the speed of the link, resulting in a corresponding adjustment of the OSPF cost. If this option is not specified, then PADQ messages received over the underlying interface are ignored.

The radio-router statement includes bandwidth, resource, latency, and quality statements. These subsequent statements provide control over the weights used when transforming PADQ link metrics into an interface speed for the virtual link. The default value for all four weights is 100.

The radio-router statement includes a threshold statement. The threshold value specifies how much of a difference is required between the calculated and the current interface speeds. The threshold value, expressed as a percentage, defaults to 10.

To support credit-based flow control extensions described in RFC4938, PPPoE peers can now grant each other forwarding credits using the radio-router credit statement. The grantee is then allowed to forward traffic to the peer only when it has a sufficient
number of credits to do so. The subsequent credit interval statement controls how frequently the device generates credit announcement messages.

Here is a brief description of the available settings for radio-router:

- **bandwidth**: Weight of current (vs. maximum) data rate (value 0–100)
- **credit**: Credit-based scheduling parameters
  - **interval**: Grant rate interval (value 1–60 seconds)
- **latency**: Latency weight (value 0–100)
- **quality**: Relative Link Quality weight (value 0–100)
- **resource**: Resource weight (value 0–100)
- **threshold**: Percentage bandwidth change required for routing updates

### CLI Configuration

```
user@host# edit interfaces ge-3/0/3 unit 1 radio-router bandwidth 100 resource 100 latency 100 quality 100 resource 100 threshold 10

user@host# edit interfaces pp0 unit 1 pppoe-options underlying-interface ge-3/0/3
user@host# edit interfaces pp0 unit 1 pppoe-options server test
user@host# edit interfaces pp0 unit 1 family inet unnumbered-address lo0.0 destination 192.168.1.2
user@host# edit interfaces pp0 unit 1 family inet6 unnumbered-address lo0.0 destination fec0:1:1:1::2
```

### CLI Hierarchy

```
user@host# set interfaces ge-0/0/1.0 radio-router {
  bandwidth;
  credit {
    interval;
  }
  latency;
  quality;
  resource;
  threshold;
}
```

## Verifying a PPPoE Configuration

To verify PPPoE configuration, perform the following tasks:

- Displaying a PPPoE Configuration for an Ethernet Interface on page 304
- Displaying a PPPoE Configuration for an ATM-over-ADSL or ATM-over-SHDSL Interface on page 304
- Verifying PPPoE Interfaces on page 305
- Verifying PPPoE Sessions on page 307
Displaying a PPPoE Configuration for an Ethernet Interface

Purpose  Verify the PPPoE configuration for an Ethernet interface.

Action  From the J-Web interface, select Configure > CLI Tools > CLI Viewer. Alternatively, from configuration mode in the CLI, enter the show interfaces command from the top level.

```
[edit]
user@host# show interfaces
ge-3/0/0 {  
  unit 1 {  
  }
}
pp0 {  
  unit 1 {  
    pppoe-options {  
      underlying-interface ge-3/0/0.0;  
      idle-timeout 123;  
      access-concentrator myac;  
      service-name myserv;  
      auto-reconnect 10;  
      client;  
    }
    family inet {  
      address 22.2.2.1/32 {  
        destination 22.2.2.2;  
      }
    }
    family inet6 {  
      address 3004::1/128 {  
        destination 3004::2;  
      }
    }
  }
}
```

Meaning  Verify that the output shows the intended configuration of PPPoE.

Related Topics  For more information about the format of a configuration file, see the J-Web Interface User Guide or the Junos CLI User Guide.

Displaying a PPPoE Configuration for an ATM-over-ADSL or ATM-over-SHDSL Interface

Purpose  Verify the PPPoE configuration for an ATM-over-ADSL or ATM-over-SHDSL interface.
**Action**  From the J-Web interface, select **Configure > CLI Tools > CLI Viewer**. Alternatively, from configuration mode in the CLI, enter the `show interfaces` command from the top level.

```
[edit]
user@host#show interfaces
at-6/0/0 {
  encapsulation ethernet-over-atm;
  atm-options {
    vpi 0;
  }
  dsl-options {
    operating-mode itu-dmt;
  }
  unit 0 {
    encapsulation ppp-over-ether-over-atm-llc;
    vci 35;
  }
}
pp0 {
  unit 0 {
    pppoe-options {
      underlying-interface at-6/0/0.0;
      idle-timeout 123;
      access-concentrator myac;
      service-name myserv;
      auto-reconnect 10;
      client;
    }
    family inet {
      address 11.1.1.1/32 {
        destination 11.1.1.2;
      }
    }
    family inet6 {
      address 2004::1/128 {
        destination 2004::2;
      }
    }
    family mpls;
  }
}
```

**Meaning**  Verify that the output shows the intended configuration of PPPoE.

**Related Topics**  For more information about the format of a configuration file, see the *J-Web Interface User Guide* or the *Junos CLI User Guide*.

**Verifying PPPoE Interfaces**

**Purpose**  Verify that the PPPoE device interfaces are configured properly.
Action From the CLI, enter the `show interfaces pp0` command.

Sample Output

```
user@host> show interfaces pp0
Physical interface: pp0, Enabled, Physical link is Up
Interface index: 67, SNMP ifIndex: 317
Type: PPPoE, Link-level type: PPPoE, MTU: 9192
Device flags  : Present Running
Interface flags: Point-To-Point SNMP-Traps
Link type     : Full-Duplex
Link flags    : None
Last flapped  : Never
Input rate    : 0 bps (0 pps)
Output rate   : 0 bps (0 pps)

Logical interface pp0.0 (Index 1) (SNMP ifIndex 330)
Flags: Point-To-Point SNMP-Traps 16384 Encapsulation: PPPoE
PPPoE:
  State: SessionUp, Session ID: 3304,
  Session AC name: isp1.com, AC MAC address: 00:90:1a:40:f6:4c,
  Service name: video@isp1.com, Configured AC name: isp1.com,
  Auto-reconnect timeout: 60 seconds
  Underlying interface: ge-5/0/0.0 (Index 71)
Input packets : 23
Output packets: 22
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive: Input: 16 (00:00:26 ago), Output: 0 (never)
LCP state: Opened
CHAP state: Success
Protocol inet, MTU: 1492
Flags: Negotiate-Address
Addresses, Flags: Kernel Is-Preferred Is-Primary
  Destination: 211.211.211.2, Local: 211.211.211.1
```

Meaning The output shows information about the physical and the logical interface. Verify the following information:

- The physical interface is enabled and the link is up.
- The PPPoE session is running on the correct logical interface.
- Under State, the state is active (up).
- Under Underlying interface, the physical interface on which the PPPoE session is running is correct:
  - For an Ethernet connection, the underlying interface is Fast Ethernet or Gigabit Ethernet—for example, ge-5/0/0.0.
  - For an ATM-over-ADSL or ATM-over-SHDSL connection, the underlying interface is ATM—for example, at-2/0/0.0.

Related Topics For a complete description of `show interfaces pp0` output, see the Junos Interfaces Command Reference.
Verifying PPPoE Sessions

Purpose  Verify that a PPPoE session is running properly on the logical interface.

Action  From the CLI, enter the `show pppoe interfaces` command.

Sample Output  
```
user@host> show pppoe interfaces
pp0.0 Index 67
    State: Session up, Session ID: 31,
    Service name: video@isp1.com, Configured AC name: isp1.com,
    Session AC name: belur, AC MAC address: 00:90:1a:40:f6:4e,
    Auto-reconnect timeout: 1 seconds,
    Underlying interface: ge-0/0/1.0 Index 69
```

Meaning  The output shows information about the PPPoE sessions. Verify the following information:
- The PPPoE session is running on the correct logical interface.
- Under `State`, the session is active (up).
- Under `Underlying interface`, the physical interface on which the PPPoE session is running is correct:
  - For an Ethernet connection, the underlying interface is Fast Ethernet or Gigabit Ethernet—for example, `ge-0/0/1.0`.
  - For an ATM-over-ADSL or ATM-over-SHDSL connection, the underlying interface is ATM—for example, `at-2/0/0.0`.

Related Topics  For a complete description of `show pppoe interfaces` output, see the *Junos Interfaces Command Reference*.

Verifying the PPPoE Version

Purpose  Verify the version information of the PPPoE protocol configured on the device interfaces.

Action  From the CLI, enter the `show pppoe version` command.

Sample Output  
```
user@host> show pppoe version
Point-to-Point Protocol Over Ethernet, version 1. rfc2516
    PPPoE protocol = Enabled
    Maximum Sessions = 256
    PADI resend timeout = 2 seconds
    PADR resend timeout = 16 seconds
    Max resend timeout = 64 seconds
    Max Configured AC timeout = 4 seconds
```

Meaning  The output shows PPPoE protocol information. Verify the following information:
- The correct version of the PPPoE protocol is configured on the interface.
- Under **PPPoE protocol**, the PPPoE protocol is enabled.

**Related Topics** For a complete description of `show pppoe version` output, see the *Junos Interfaces Command Reference*.

### Verifying PPPoE Statistics

**Purpose** Display statistics information about PPPoE interfaces.

**Action** From the CLI, enter the `show pppoe statistics` command.

**Sample Output**

```
user@host> show pppoe statistics
Active PPPoE sessions: 4

<table>
<thead>
<tr>
<th>PacketType</th>
<th>Sent</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>PADI</td>
<td>502</td>
<td>0</td>
</tr>
<tr>
<td>PADO</td>
<td>0</td>
<td>219</td>
</tr>
<tr>
<td>PADR</td>
<td>219</td>
<td>0</td>
</tr>
<tr>
<td>PADS</td>
<td>0</td>
<td>219</td>
</tr>
<tr>
<td>PADT</td>
<td>0</td>
<td>161</td>
</tr>
<tr>
<td>Service name error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>AC system error</td>
<td>0</td>
<td>13</td>
</tr>
<tr>
<td>Generic error</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Malformed packets</td>
<td>0</td>
<td>41</td>
</tr>
<tr>
<td>Unknown packets</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Timeout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PADI</td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>PADO</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>PADR</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
```

**Meaning** The output shows information about active sessions on PPPoE interfaces. Verify the following information:
- Total number of active PPPoE sessions running on the interface.
- Under **Packet Type**, the number of packets of each type sent and received during the PPPoE session.

**Related Topics** For a complete description of `show pppoe statistics` output, see the *Junos Interfaces Command Reference*.
Chapter 11

Configuring ISDN

ISDN connectivity is supported on J Series devices as a backup for a primary Internet connection. J Series devices can be configured to “fail over” to an ISDN interface when the primary connection experiences interruptions in Internet connectivity.

Use ISDN also at the central office to terminate calls that originate at branch office routers and for central office callback for security, accounting, or cost savings at the branch office.

You can use either J-Web Quick Configuration or a configuration editor to configure ISDN BRI interfaces. To configure ISDN PRI, you use either the J-Web configuration editor or CLI configuration editor.

NOTE: This chapter provides instructions for configuring basic ISDN BRI service and features such as dial backup, dial-in, or callback for both ISDN BRI and ISDN PRI. To configure basic ISDN PRI service, see “Configuring Channelized T1/E1/ISDN PRI Interfaces” on page 117.

For information about which devices support the features documented in this chapter, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.

This chapter contains the following topics:
- ISDN Terms on page 309
- ISDN Overview on page 312
- Before You Begin on page 313
- Configuring ISDN BRI Interfaces with Quick Configuration on page 314
- Configuring ISDN Interfaces and Features with a Configuration Editor on page 321
- Verifying the ISDN Configuration on page 343

ISDN Terms

Before configuring ISDN, become familiar with the terms defined in Table 80 on page 310.
### Table 80: ISDN Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth on demand</td>
<td>ISDN cost-control feature defining the bandwidth threshold that must be reached on all links before a J Series device initiates additional ISDN data connections to provide more bandwidth.</td>
</tr>
<tr>
<td>Basic Rate Interface (BRI)</td>
<td>ISDN service intended for home and small enterprise applications. ISDN BRI consists of two 64-Kbps B-channels to carry voice or data and one 16-Kbps D-channel for control and signaling.</td>
</tr>
<tr>
<td>bearer channel (B-channel)</td>
<td>64-Kbps channel used for voice or data transfer on an ISDN interface.</td>
</tr>
<tr>
<td>callback</td>
<td>Alternative feature to dial-in that enables a J Series device to call back the caller from the remote end of a backup ISDN connection. Instead of accepting a call from the remote end of the connection, the device rejects the call, waits a configured period of time, and calls a number configured on the device's dialer interface. See also dial-in.</td>
</tr>
<tr>
<td>caller ID</td>
<td>Telephone number of the caller on the remote end of a backup ISDN connection, used to dial in and also to identify the caller. Multiple caller IDs can be configured on an ISDN dialer interface. During dial-in, the device matches the incoming call’s caller ID against the caller IDs configured on its dialer interfaces. Each dialer interface accepts calls from only callers whose caller IDs are configured on it.</td>
</tr>
<tr>
<td>delta-channel (D-channel)</td>
<td>Circuit-switched channel that carries signaling and control for B-channels. In ISDN Basic Rate Interface (BRI) applications, a D-channel can also support customer packet data traffic at speeds up to 9.6 Kbps.</td>
</tr>
<tr>
<td>demand circuit</td>
<td>Network segment whose cost varies with usage, according to a service level agreement with a service provider. Demand circuits limit traffic based on either bandwidth (bits or packets transmitted) or access time. For example, ISDN interfaces can be configured for dial-on-demand routing backup. In OSPF, the demand circuit reduces the amount of OSPF traffic by removing all OSPF protocols when the routing domain is in a steady state.</td>
</tr>
<tr>
<td>dial backup</td>
<td>Feature that reestablishes network connectivity through one or more backup ISDN dialer interfaces after a primary interface fails. When the primary interface is reestablished, the ISDN interface is disconnected.</td>
</tr>
<tr>
<td>dialer filter</td>
<td>Stateless firewall filter that enables dial-on-demand routing backup when applied to a physical ISDN interface and its dialer interface configured as a passive static route. The passive static route has a lower priority than dynamic routes. If all dynamic routes to an address are lost from the routing table and the device receives a packet for that address, the dialer interface initiates an ISDN backup connection and sends the packet over it. See also dial-on-demand routing backup, floating static route.</td>
</tr>
<tr>
<td>dialer interface (dl)</td>
<td>Logical interface for configuring dialing properties and the control interface for a backup ISDN connection.</td>
</tr>
<tr>
<td><strong>Term</strong></td>
<td><strong>Definition</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>dial-in</td>
<td>Feature that enables J Series devices to receive calls from the remote end of a backup ISDN connection. The remote end of the ISDN call might be a service provider, a corporate central location, or a customer premises equipment (CPE) branch office. All incoming calls can be verified against caller IDs configured on the device’s dialer interface. See also <em>callback</em>.</td>
</tr>
<tr>
<td>dial-on-demand routing (DDR) backup</td>
<td>Feature that provides a J Series device with full-time connectivity across an ISDN line. When routes on a primary serial T1, E1, T3, E3, Fast Ethernet, Gigabit Ethernet, or PPPoE interface are lost, an ISDN dialer interface establishes a backup connection. To save connection time costs, the device drops the ISDN connection after a configured period of inactivity. Devices with ISDN interfaces support two types of dial-on-demand routing backup: on-demand routing with a dialer filter and dialer watch. See also <em>dialer filter; dialer watch</em>.</td>
</tr>
<tr>
<td>dialer profile</td>
<td>Set of characteristics configured for the ISDN dialer interface. Dialer profiles allow the configuration of physical interfaces to be separated from the logical configuration of dialer interfaces required for ISDN connectivity. This feature also allows physical and logical interfaces to be bound together dynamically on a per-connection basis.</td>
</tr>
<tr>
<td>dialer watch</td>
<td>Dial-on-demand routing (DDR) backup feature that provides reliable connectivity without relying on a dialer filter to activate the ISDN interface. The ISDN dialer interface monitors the existence of each route on a watch list. If all routes on the watch list are lost from the routing table, dialer watch initiates the ISDN interface for failover connectivity. See also <em>dial-on-demand routing backup</em>.</td>
</tr>
<tr>
<td>floating static route</td>
<td>Route with an administrative distance greater than the administrative distance of the dynamically learned versions of the same route. The static route is used only when the dynamic routes are no longer available. When a floating static route is configured on an interface with a dialer filter, the interface can be used for backup.</td>
</tr>
<tr>
<td>Integrated Services Digital Network (ISDN)</td>
<td>Digital communication service provided by telecommunication service providers. It is an all-digital dialup (on-demand) service that carries voice, data, and video transmissions over telephone lines.</td>
</tr>
<tr>
<td>Primary Rate Interface (PRI)</td>
<td>ISDN service intended for higher-bandwidth applications than ISDN BRI. ISDN PRI consists of a single D-channel for control and signaling, plus a number of 64-Kbps B-channels—either 23 B-channels on a T1 line or 30 B-channels on an E1 line—to carry network traffic.</td>
</tr>
<tr>
<td>service profile identifier (SPID)</td>
<td>Number that specifies the services available to you on the service provider switch and defines the feature set ordered when the ISDN service is provisioned.</td>
</tr>
<tr>
<td>terminal endpoint identifier (TEI)</td>
<td>Number that identifies a terminal endpoint, an ISDN-capable device attached to an ISDN network through an ISDN interface on the device. The TEI is a number between 0 and 127. The numbers 0–63 are used for static TEI assignment, 64–126 are used for dynamic assignment, and 127 is used for group assignment.</td>
</tr>
</tbody>
</table>
ISDN Overview

Integrated Services Digital Network (ISDN) is a set of standards for digital transmission over different media created by the Consultative Committee for International Telegraph and Telephone (CCITT) and International Telecommunication Union (ITU). As a dial-on-demand service, it has fast call setup and low latency as well as the ability to carry high-quality voice, data, and video transmissions. ISDN is also a circuit-switched service that can be used on both multipoint and point-to-point connections.

You configure two types of interfaces for ISDN service: at least one physical interface and a logical interface called the dialer interface.

ISDN Interfaces

The following interfaces on a device are available for ISDN connectivity:

- For ISDN BRI, up to six of the following field-replaceable units (FRUs):
  - 4-port S/T PIM supporting ITU-T I.430, ETSI TS 101080, and GR-1089-Core Type III
  - 4-port U PIM supporting ANSI T.601 and GR-1089-Core

- For ISDN PRI, up to six Dual-Port Channelized T1/E1/ISDN PRI PIMs, supporting ITU-T Q.920, Q.921: LAPD, Q.930, and Q.931

ISDN BRI Interface Types

A J Series device with one or more ISDN BRI ports has the following types of ISDN interfaces:

- Physical ISDN BRI interface—br_pim/0/port
- Physical B-channel interface—bc_pim/0/port
- Physical D-channel interface—dc_pim/0/port
- Logical dialer interface—dl

For information about interface names, see “Network Interface Naming” on page 9.

To configure ISDN BRI service on a J Series device, you configure the physical ISDN BRI interface and the logical dialer interface.

Each ISDN BRI port has two B-channels for transport, identified as br_pim/0/port:1 and br_pim/0/port:2, and one D-channel for control, identified as dc_pim/0/port. On ISDN BRI interfaces, the B-channels and D-channel have no configurable settings, but you can monitor them for interface status and statistics.
ISDN PRI Interface Types

On a J Series device with one or more Dual-Port Channelized T1/E1/ISDN PRI PIMs, you can configure each port on the PIM for either T1, E1, or ISDN PRI service, or for a combination of ISDN PRI and either T1 or E1 service. For ISDN PRI service, you configure the following types of ISDN interfaces as channels on the channelized T1 or E1 interface:

- **Physical B-channel interface** — `bc-pim/0/port:channel`
  - On a channelized T1 interface, up to 23 time slots can be configured as ISDN PRI B-channels.
  - On a channelized E1 interface, up to 30 time slots can be configured as ISDN PRI B-channels.

- **Physical D-channel interface** — `dc-pim/0/port:channel`
  - On a channelized T1 interface, you configure time slot 24 as the D-channel.
  - On a channelized E1 interface, you configure time slot 16 as the D-channel.

- **Logical dialer interface** — `dl`

For information about interface names, see “Network Interface Naming” on page 9.

For more information about channelized T1/E1/ISDN PRI interfaces, see “Configuring Channelized T1/E1/ISDN PRI Interfaces” on page 117.

**Dialer Interface**

The dialer (`dl`) interface is a logical interface on which you configure dialing properties for ISDN connections. The interface can be configured in two modes:

- Multilink mode using Multilink PPP encapsulation
- Normal mode using PPP or Cisco High-Level Data Link Control (HDLC) encapsulation

The dialer interface can perform backup, dialer filter, and dialer watch functions, but these operations are mutually exclusive. You can configure a single dialer interface to operate in only one of the following ways:

- As a backup interface—for one primary interface
- As a dialer filter
- As a dialer watch interface

**Before You Begin**

Before you configure ISDN interfaces, you need to perform the following tasks:
Install J Series device hardware. For more information, see the J Series Services Routers Hardware Guide.

Establish basic connectivity. For more information, see the Getting Started Guide for your device.

Order an ISDN line from your telecommunications service provider. Contact your service provider for more information.

If you do not already have a basic understanding of physical and logical interfaces and Juniper Networks interface conventions, read “Interfaces Overview” on page 3.

Although it is not a requirement, you might also want to plan how you are going to use the ISDN interfaces on your network before you begin configuring them. (To display a list of installed ISDN BRI interfaces, select Configuration > Quick Configuration > Interfaces.)

### Configuring ISDN BRI Interfaces with Quick Configuration

You can use the ISDN Interfaces Quick Configuration pages to configure ISDN BRI interfaces on a J Series device. The Quick Configuration pages allow you to configure ISDN BRI connectivity on a device to back up a primary Internet connection.

**NOTE:** To configure an ISDN PRI interface, you must use the J-Web or CLI configuration editor.

You configure the physical ISDN BRI interface first and then the backup method on the logical dialer interface.

This section contains the following topics:

- Configuring ISDN BRI Physical Interfaces with Quick Configuration on page 314
- Configuring ISDN BRI Dialer Interfaces with Quick Configuration on page 317

### Configuring ISDN BRI Physical Interfaces with Quick Configuration

To configure ISDN BRI physical interfaces with Quick Configuration:

1. In the J-Web interface, select **Configure > Interfaces**. A list of network interfaces installed on the device is displayed.
2. Click the br-pim/0/port interface name for the ISDN BRI port you want to configure.

The ISDN BRI Physical Interface Quick Configuration page is displayed as shown in Figure 42 on page 315.
3. Enter information into the ISDN Quick Configuration pages, as described in Table 81 on page 315.

4. From the ISDN Physical Interfaces Quick Configuration page:
   - To apply the configuration and stay on the ISDN Physical Interfaces Quick Configuration page, click **Apply**.
   - To apply the configuration and return to the Interfaces Quick Configuration page, click **OK**.
   - To cancel your entries and return to the Interfaces Quick Configuration page, click **Cancel**.

5. Go on to “Configuring ISDN BRI Dialer Interfaces with Quick Configuration” on page 317.

**Table 81: ISDN BRI Quick Configuration Page Summary**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuring ISDN Interfaces</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Interface Description</td>
<td>(Optional) Adds supplemental information about the ISDN physical interface on the device.</td>
<td>Type a text description of the physical ISDN BRI interface in the box to clearly identify it in monitoring displays.</td>
</tr>
</tbody>
</table>
Table 81: ISDN BRI Quick Configuration Page Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clocking</td>
<td>Enables internal or external clocking sources for the interface on the device.</td>
<td>Select <strong>internal</strong> or <strong>external</strong> from the list.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>internal</strong>—device’s own system clock (the default)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ <strong>external</strong>—Clock received from the T1 interface</td>
<td></td>
</tr>
</tbody>
</table>

**Dialer Pool Options**

<table>
<thead>
<tr>
<th>Dialer Pools</th>
<th>Displays the list of configured ISDN dialer pools on the device.</th>
<th>■ To add a dialer pool to the interface, click <strong>Add</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>■ To edit a dialer pool, select the name from the list. You can change the priority, but not the name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ To delete a dialer pool, select the check box and click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dialer Pool Name (required)</th>
<th>Specifies the group of physical interfaces to be used by the dialer interface.</th>
<th>Type the dialer pool name—for example, <strong>isdn-dialer-pool</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Specifies the priority of this interface within the dialer pool. Interfaces with a higher priority are the first to interact with the dialer interface.</td>
<td>1. Type a priority value from <strong>0</strong> (lowest) to <strong>255</strong> (highest). The default is <strong>0</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click <strong>OK</strong> to return to the Quick Configuration page.</td>
</tr>
</tbody>
</table>

**ISDN Options**

<table>
<thead>
<tr>
<th>Calling Number</th>
<th>Configures the dialing number used to connect with the service provider.</th>
<th>Type the outgoing calling number for the service provider.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISDN Switch Type</td>
<td>Specifies the type of ISDN switch used by the service provider.</td>
<td>Select one of the following switch types:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>att5e</strong>—AT&amp;T 5ESS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>etsi</strong>—NET3 for the UK and Europe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>ni1</strong>—National ISDN-1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>ntdms-100</strong>—Northern Telecom DMS-100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ <strong>ntt</strong>—NTT Group switch for Japan</td>
</tr>
<tr>
<td>Service Profile Identifier</td>
<td>Configures the service profile identifier (SPID) provided by your ISDN service.</td>
<td>Type the SPID in the box. If you have a NTDMS-100 or NI1 switch, an additional SPID field is provided.</td>
</tr>
</tbody>
</table>
Table 81: ISDN BRI Quick Configuration Page Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static TEI Value</td>
<td>Configures the static terminal endpoint identifier (TEI) value from your service provider. The TEI number identifies a terminal endpoint, an ISDN-capable device attached to an ISDN network through an ISDN interface on the device. The TEI is a number between 0 and 127. The numbers 0–63 are used for static TEI assignment, 64–126 are used for dynamic assignment, and 127 is used for group assignment. Type a value between 0 and 63. If this value is not supplied, the device dynamically acquires a TEI. If you configured more than one SPID, the TEI must be acquired dynamically.</td>
<td></td>
</tr>
<tr>
<td>TEI Option</td>
<td>Configures when the TEI negotiates with the ISDN provider. ■ Select first-call to activate the connection when the call setup is sent to the ISDN provider. ■ Select power-up (the default) to activate the connection when the device is powered on.</td>
<td>■ Select first-call to activate the connection when the call setup is sent to the ISDN provider. ■ Select power-up (the default) to activate the connection when the device is powered on.</td>
</tr>
<tr>
<td>Timer T310 Value</td>
<td>Sets the Q.931 timer value in seconds. Type a value between 1 and 65536. The default value is 10 seconds.</td>
<td>Type a value between 1 and 65536. The default value is 10 seconds.</td>
</tr>
</tbody>
</table>

Configuring ISDN BRI Dialer Interfaces with Quick Configuration

When ISDN BRI interfaces are installed on the device, links to ISDN Quick Configuration pages for dialer options are displayed on the Interfaces Quick Configuration page as shown in Figure 43 on page 318.

You can use these Quick Configuration pages to configure an ISDN BRI dialer interface for either dial backup or dialer watch. For dial backup you specify the serial interface to back up. For dialer watch you specify a watch list of one or more routes to monitor.
To configure ISDN BRI dialer interfaces with Quick Configuration:

1. In the J-Web interface, select Configure > Interfaces. A list of network interfaces installed on the device is displayed.
2. Click ISDN Dialer Options under the interfaces list.
3. Select a backup method to configure on the dialer interface:
   - Click Dial Backup to allow one or more dialer interfaces to back up the primary interface. The backup interfaces are activated only when the primary interface fails.
   - Click Dialer Watch to monitor a specified route and initiate dialing of the backup link if that route is not present.
4. Do one of the following:
   - To edit an existing dialer interface, click the dialer interface name. For example, click dl0 to edit the dialer physical interface, and then click dl0.0 to edit the dialer logical interface.
   - To add a dialer interface, click Add. In the Interface Name box, type a name for the logical interface—for example, dl1—then click Add under Logical Interfaces.

Figure 44 on page 319 shows the ISDN Quick Configuration page for dialer logical interfaces.
5. Enter information into the ISDN Quick Configuration page for dialer logical interfaces, as described in Table 82 on page 319.

6. Click one of the following buttons on the ISDN Quick Configuration page:
   - To apply the configuration and stay on the current Quick Configuration page, click **Apply**.
   - To apply the configuration and return to the previous Quick Configuration page, click **OK**.
   - To cancel your entries and return to the previous Quick Configuration page, click **Cancel**.

7. To verify that the ISDN interface is configured correctly, see “Verifying the ISDN Configuration” on page 343.

Table 82: ISDN BRI Dialer Interface Quick Configuration Page Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Dialer Interfaces</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical Interface Description</td>
<td>Describes the logical interface.</td>
<td>Type a text description of the interface in the box.</td>
</tr>
</tbody>
</table>
Table 82: ISDN BRI Dialer Interface Quick Configuration Page Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Addresses and</td>
<td>Displays the IPv4 addresses for the interfaces to which the dialer</td>
<td>Type an IP address and a prefix in the boxes. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Prefixes</td>
<td>interface is assigned.</td>
<td>To delete an IP address, highlight it in the list, and click <strong>Delete</strong>.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>**Ensure that the same IP subnet address is not configured on different</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dialer interfaces.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuring the same IP subnet address on different dialer interfaces can</td>
<td></td>
</tr>
<tr>
<td></td>
<td>result in inconsistency in the route and packet loss. Packets can be</td>
<td></td>
</tr>
<tr>
<td></td>
<td>routed through any of the dialer interfaces with the IP subnet address,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>instead of being routed through the dialer interface to which the ISDN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>call is mapped.</td>
<td></td>
</tr>
</tbody>
</table>

**Dialer Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation Delay</td>
<td>Displays the time to wait before activating the backup interface once the</td>
<td>Type a value, in seconds—for example, <strong>30</strong>.</td>
</tr>
<tr>
<td></td>
<td>primary interface is down.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is 0 seconds with a maximum value of 60 seconds.</td>
</tr>
<tr>
<td>Deactivation Delay</td>
<td>Displays the time to wait before deactivating the backup interface once</td>
<td>Type a value, in seconds—for example, <strong>30</strong>.</td>
</tr>
<tr>
<td></td>
<td>the primary interface is up.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is 0 seconds with a maximum value of 60 seconds.</td>
</tr>
<tr>
<td>Dial String (required)</td>
<td>Displays the dialing number from your ISDN service provider.</td>
<td>Type the dialing number and click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To delete a dial string, highlight it and click <strong>Delete</strong>.</td>
</tr>
<tr>
<td>Pool (required)</td>
<td>Displays a list of dialer pools configured on <strong>br-pim/0/port</strong> interfaces.</td>
<td>Select a dialer pool from the list.</td>
</tr>
</tbody>
</table>

**Multilink Dialer Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load Interval</td>
<td>Defines the interval used to calculate the average load on the dialer</td>
<td>Type a value, in seconds—for example, <strong>30</strong>.</td>
</tr>
<tr>
<td></td>
<td>interface for bandwidth on demand.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is 60 seconds with a range of 20–80. The value must be a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>multiple of 10.</td>
</tr>
<tr>
<td>Load Threshold</td>
<td>Defines the threshold at which an additional ISDN interface is activated</td>
<td>Type a percentage—for example, <strong>80</strong>.</td>
</tr>
<tr>
<td></td>
<td>for bandwidth-on-demand. You specify the threshold as a percentage of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the cumulative load of all UP links.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is <strong>100</strong> with a range of 0–100.</td>
</tr>
</tbody>
</table>

**Backup Interface (for dial backup only)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface to Backup</td>
<td>Displays a list of interfaces for ISDN backup.</td>
<td>Select an interface from the list for ISDN backup.</td>
</tr>
</tbody>
</table>

**Dialer Watch List (for dial watch only)**
Table 82: ISDN BRI Dialer Interface Quick Configuration Page Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Addresses and Prefixes</td>
<td>Displays the IPv4 addresses in the list of routes to be monitored by the dialer interface</td>
<td>Type an IP address and a prefix in the boxes. Click Add.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To delete an IP address, highlight it in the list, and click Delete.</td>
</tr>
</tbody>
</table>

**Configuring ISDN Interfaces and Features with a Configuration Editor**

To configure ISDN interfaces on a J Series device, you first configure the basic ISDN interface—either “Adding an ISDN BRI Interface (Required)” on page 321 or “Configuring Channelized T1/E1/ISDN PRI Interfaces for ISDN PRI Operation” on page 125. Second, configure the dialer interface by performing “Configuring Dialer Interfaces (Required)” on page 324.

To configure ISDN interfaces to back up primary device interfaces, you then configure a backup method—either “Configuring Dial Backup” on page 327, “Configuring Dialer Filters for Dial-on-Demand Routing Backup” on page 328, or “Configuring Dialer Watch” on page 330.

To configure ISDN interfaces for dial-in or callback, configure the basic ISDN BRI or PRI interface and then perform “Configuring Dial-In and Callback (Optional)” on page 337.

Perform other tasks as needed on your network.

This section contains the following topics:

- Adding an ISDN BRI Interface (Required) on page 321
- Configuring Dialer Interfaces (Required) on page 324
- Configuring Dial Backup on page 327
- Configuring Dialer Filters for Dial-on-Demand Routing Backup on page 328
- Configuring Dialer Watch on page 330
- Configuring Dial-on-Demand Routing Backup with OSPF Support (Optional) on page 331
- Configuring Bandwidth on Demand (Optional) on page 332
- Configuring Dial-In and Callback (Optional) on page 337
- Disabling Dialing Out Through Dialer Interfaces on page 342
- Disabling ISDN Signaling on page 343

**Adding an ISDN BRI Interface (Required)**

To enable ISDN BRI interfaces installed on your J Series device to work properly, you must configure the interface properties.
To configure an ISDN BRI network interface for the J Series device:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 83 on page 322.
3. Go on to “Configuring Dialer Interfaces (Required)” on page 324.

Table 83: Adding an ISDN BRI Interface

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Interfaces level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit interfaces br-1/0/3</td>
</tr>
<tr>
<td></td>
<td>2. Next to Interfaces, click Configure or Edit.</td>
<td></td>
</tr>
<tr>
<td>Create the new interface—for example, br-1/0/3.</td>
<td>1. Next to Interface, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. In the Interface name box, type the name of the new interface, br-1/0/3.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Click OK.</td>
<td></td>
</tr>
<tr>
<td>Configure dialer options.</td>
<td>1. In the Encapsulation column, next to the new interface, click Edit.</td>
<td>From the [edit interfaces br-1/0/3] hierarchy, enter set dialer-options pool isdn-dialer-group priority 255</td>
</tr>
<tr>
<td>■ Name the dialer pool—for example, isdn-dialer-group.</td>
<td>2. Next to Dialer options, select Yes, and then click Configure.</td>
<td></td>
</tr>
<tr>
<td>■ Set the dialer pool priority—for example, 255.</td>
<td>3. Next to Pool, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td>Dialer pool priority has a range from 1 to 255, with 1 designating lowest-priority interfaces and 255 designating the highest-priority interfaces.</td>
<td>4. In the Pool identifier box, type isdn-dialer-group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. In the Priority box, type 255.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Click OK twice.</td>
<td></td>
</tr>
</tbody>
</table>
Table 83: Adding an ISDN BRI Interface (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure ISDN BRI properties.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Calling number sent to the ISDN switch during the call setup, which represents the caller's number—for example, 18005555555.</td>
<td>Next to Isdn options, click <strong>Configure</strong>.</td>
<td>1. To set the ISDN options, enter set isdn-options calling-number 18005555555.</td>
</tr>
<tr>
<td>■ Service provider ID (SPID)—for example, 00108005555555.</td>
<td></td>
<td>2. Enter set isdn-options spid1 00108005555555.</td>
</tr>
<tr>
<td>■ Static TEI between 0 and 63 from your service provider—for example, 23. If the field is left blank, the device dynamically acquires a TEI. Also, if you have configured a second SPID, you cannot set a static TEI value. If you have a NTDMS-100 or NI1 switch, an additional box for a service provider ID is provided. If you are using a service provider that requires SPIDs, you cannot place calls until the interface sends a valid, assigned SPID to the service provider when accessing the ISDN connection.</td>
<td>Next to Incoming called number, click <strong>Add new entry</strong>.</td>
<td>3. Enter set isdn-options static-tei-val 23</td>
</tr>
<tr>
<td>■ Incoming called number—for example, 18883333456. Configure incoming call properties if you have remote locations dialing into the device through the ISDN interface.</td>
<td>In the Called number box, type 18883333456. Click <strong>OK</strong>.</td>
<td>4. set isdn-options incoming-called-number 18883333456</td>
</tr>
</tbody>
</table>

Select the type of ISDN switch—for example, ATT5E. The following switches are compatible with J Series devices:

- ATT5E—AT&T 5ESS
- ETSI—NET3 for the UK and Europe
- N1—National ISDN-1
- NTDMS—100—Northern Telecom DMS-100
- NTT—NTT Group switch for Japan

From the Switch type list, select **att5e**. To select the switch type, enter set isdn-options switch-type att5e

Configure the Q.931 timer. Q.931 is a Layer 3 protocol for the setup and termination of connections. The default value for the timer is 10 seconds, but can be configured between 1 and 65536 seconds—for example, 15.

In the T310 box, type 15. set isdn-options t310 15
Table 83: Adding an ISDN BRI Interface (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure when the TEI negotiates with the ISDN provider.</td>
<td>From the Tei option list, select <strong>power-up</strong>.</td>
<td>To initiate activation at power-up, enter set isdn-options tei-option power-up.</td>
</tr>
<tr>
<td>■ <strong>first-call</strong>—Activation does not occur until a call is sent.</td>
<td>1. Click <strong>OK</strong> to return to the Interfaces page.</td>
<td></td>
</tr>
<tr>
<td>■ <strong>power-up</strong>—Activation occurs when the device is powered on. This is the default value.</td>
<td>2.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Dialer Interfaces (Required)

The dialer interface (dl) is a logical interface configured to establish ISDN connectivity. You can configure multiple dialer interfaces for different functions on the J Series device.

After configuring the dialer interface, you must configure a backup method—either dial backup, a dialer filter, or dialer watch.

To configure a logical dialer interface for the J Series device:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 84 on page 324.
3. To configure a backup method, go on to one of the following tasks:
   ■ “Configuring Dial Backup” on page 327.
   ■ “Configuring Dialer Filters for Dial-on-Demand Routing Backup” on page 328.
   ■ “Configuring Dialer Watch” on page 330.

Table 84: Adding a Dialer Interface to a Device

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Interfaces</strong> level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit interfaces.</td>
</tr>
<tr>
<td></td>
<td>2. Next to Interfaces, click <strong>Configure</strong> or <strong>Edit</strong>.</td>
<td></td>
</tr>
</tbody>
</table>
Table 84: Adding a Dialer Interface to a Device (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create the new interface—for example, dl0.</td>
<td>1. Next to Interface, click Add new entry.</td>
<td>Create and name the interface: 1. edit dl0</td>
</tr>
<tr>
<td>Adding a description can differentiate between different dialer interfaces—for example, T1-backup.</td>
<td>2. In the Interface name box, type dl0.</td>
<td>2. set description T1-backup</td>
</tr>
<tr>
<td>3. In the Description box, type T1-backup.</td>
<td>4. Click OK.</td>
<td></td>
</tr>
<tr>
<td>Configure encapsulation options—for example, Cisco HDLC.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Cisco HDLC—for normal mode (when the device is using only one B-channel). Cisco-compatible High-Level Data Link Control is a group of protocols for transmitting data between network points.</td>
<td>1. In the Encapsulation column, next to the new interface, click Edit.</td>
<td>Enter set encapsulation cisco-hdlc</td>
</tr>
<tr>
<td>• PPP—for normal mode (when the device is using only one ISDN B-channel per call). Point-to-Point Protocol is for communication between two computers using a serial interface.</td>
<td>2. From the Encapsulation list, select cisco-hdlc.</td>
<td></td>
</tr>
<tr>
<td>• Multilink PPP—for multilink mode, when the device is using multiple B-channels per call. Multilink Point-to-Point Protocol (MLPPP) is a protocol for aggregating multiple constituent links into one larger PPP bundle. You can bundle up to eight B-channels.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOTE: MPLS over ISDN is supported only with MLPPP encapsulation. If you use PPP or Cisco-HDLC, MPLS packets might be dropped.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enter a hold-time value in milliseconds—for example, 60. The hold-time value is used to damp interface transitions. When an interface goes from up to down, it is not advertised as down to the rest of the system until it remains unavailable for the hold-time period. Similarly, an interface is not advertised as up until it remains operational for the hold-time period. The hold time is three times the interval at which keepalive messages are sent.</td>
<td>1. In the Hold time section, type 60 in the Down box.</td>
<td>Enter set hold-time down 60</td>
</tr>
<tr>
<td>2. In the Up box, type 60.</td>
<td>2. Enter set hold-time up 60</td>
<td></td>
</tr>
<tr>
<td>Create the logical unit—for example, 0.</td>
<td>1. Next to Unit, click Add new entry.</td>
<td>Enter set unit 0</td>
</tr>
<tr>
<td>NOTE: You can set the logical unit to 0 only, unless you are configuring the dialer interface for Multilink PPP encapsulation.</td>
<td>2. In the Interface unit number box, type 0.</td>
<td></td>
</tr>
<tr>
<td>3. Next to Dialer options, select Yes, and then click Configure.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 84: Adding a Dialer Interface to a Device (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure dialer options.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ <strong>Activation delay</strong>—Time to wait before activating the backup interface once the primary interface is down—for example, 30. Default value is 0 seconds with a maximum value of 60 seconds. Use only for dialer backup and dialer watch.</td>
<td>1. In the Activation delay box, type 60.</td>
<td>1. Enter edit unit 0 dialer-options</td>
</tr>
<tr>
<td>■ <strong>Deactivation delay</strong>—Time to wait before deactivating the backup interface once the primary interface is up—for example, 30. Default value is 0 seconds with a maximum value of 60 seconds. Use only for dialer backup and dialer watch.</td>
<td>2. In the Deactivation delay box, type 30.</td>
<td>2. Enter set activation-delay 60</td>
</tr>
<tr>
<td>■ <strong>Idle timeout</strong>—Time a connection is idle before disconnecting—for example, 30. Default value is 120 seconds with a range from 0 to 4294967295. This option is used only to configure a dialer filter.</td>
<td>3. In the Pool box, type isdn-dialer-group.</td>
<td>3. Enter set deactivation-delay 30</td>
</tr>
<tr>
<td>■ <strong>Initial route check</strong>—Time to wait before checking if the primary interface is up—for example, 30. Default value is 120 seconds with a range of 1 to 300 seconds. This option is used only to configure dialer watch.</td>
<td>4. In the Redial delay box, type 5.</td>
<td>4. Enter set pool isdn-dialer-group</td>
</tr>
<tr>
<td>■ <strong>Pool</strong>—Name of a group of ISDN interfaces configured to use the dialer interface—for example, isdn-dialer-group.</td>
<td></td>
<td>5. Enter set redial-delay 5</td>
</tr>
<tr>
<td>■ <strong>Redial delay</strong>—Number of seconds to wait before redialing a failed outgoing ISDN call. Default value is 3 seconds with a range from 2 to 255.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configure the remote destination to call—for example, 5551212.

1. Next to Dial string, click Add new entry.
2. In the Value box, type 5551212.
3. Click OK until you return to the Unit page.

Configure source and destination IP addresses for the dialer interface—for example, 172.20.10.2 and 172.20.10.1. (The destination IP address is optional.)

**NOTE:** If you configure multiple dialer interfaces, ensure that the same IP subnet address is not configured on different dialer interfaces. Configuring the same IP subnet address on multiple dialer interfaces can result in inconsistency in the route and packet loss. The device might route packets through another dialer interface with the IP subnet address instead of through the dialer interface to which the ISDN modem call is mapped.

1. Select Inet under Family, and click Edit.
2. Next to Address, click Add new entry.
3. In the Source box, type 172.20.10.2.
4. In the Destination box, type 172.20.10.1.
5. Click OK.

From the [edit] hierarchy level, enter

1. edit interfaces di0 unit 0
2. set family inet address 172.20.10.2 destination 172.20.10.1
Configuring Dial Backup

Dial backup allows one or more dialer interfaces to be configured as the backup link for a primary interface. The backup dialer interfaces are activated only when the primary interface fails. ISDN backup connectivity is supported on all interfaces except Isq-0/0/0.

To configure a primary interface for backup connectivity:
1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 85 on page 327.
3. If you are finished configuring the device, commit the configuration.
4. Go on to any of the following optional tasks:
   - “Configuring Dial-on-Demand Routing Backup with OSPF Support (Optional)” on page 331.
   - “Configuring Bandwidth on Demand (Optional)” on page 332.
   - Configuring Dial-In and Callback (Optional) on page 337
5. To verify that the network interface is configured correctly, see “Verifying the ISDN Configuration” on page 343.

Table 85: Configuring an Interface for ISDN Backup

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Interfaces level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI. 2. Next to Interfaces, click Configure or Edit.</td>
<td>From the [edit] hierarchy level, enter edit interfaces ge-0/0/0/unit 0</td>
</tr>
<tr>
<td>Select the physical interface for backup ISDN connectivity.</td>
<td>1. In the Interface name column, click the physical interface name. 2. Under Unit, in the Nested Configuration column, click Edit.</td>
<td></td>
</tr>
<tr>
<td>Configure the backup dialer interface—for instance, dl0.0.</td>
<td>1. Next to Backup options, click Configure. 2. In the Interface box, type dl0.0. 3. Click OK until you return to the Interfaces page.</td>
<td>Enter set backup-options interface dl0.0</td>
</tr>
</tbody>
</table>
Configuring Dialer Filters for Dial-on-Demand Routing Backup

This dial-on-demand routing backup method allows an ISDN line to be activated only when network traffic configured as an “interesting packet” arrives on the network. Once the network traffic is sent, an inactivity timer is triggered and the connection is closed after the timer expires.

You define an interesting packet using the dialer filter feature of the device. There are two steps to configuring dial-on-demand routing backup using a dialer filter:

- Configuring the Dialer Filter on page 328
- Applying the Dial-on-Demand Dialer Filter to the Dialer Interface on page 329

Configuring the Dialer Filter

To configure the dialer filter:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 86 on page 328.
3. Go on to “Applying the Dial-on-Demand Dialer Filter to the Dialer Interface” on page 329.

Table 86: Configuring a Dialer Filter for Interesting Packets

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Firewall level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI 2. Next to Firewall, click Configure or Edit</td>
<td>From the [edit] hierarchy level, enter edit firewall</td>
</tr>
<tr>
<td>Configure the dialer filter name—for example, int-packet.</td>
<td>1. Next to Inet, click Configure or Edit 2. Next to Dialer filter, click Add new entry 3. In the Filter name box, type int-packet.</td>
<td>1. Enter edit family inet 2. Then enter edit dialer-filter int-packet</td>
</tr>
<tr>
<td>Configure the dialer filter rule name—for example, term1. Configure term behavior. For example, you might want to configure your interesting packet as an ICMP packet. To configure the term completely, include both from and then statements.</td>
<td>1. Next to Term, click Add new entry. 2. In the Rule name box, type term1. 3. Next to From, click Configure. 4. From the Protocol choice list, select Protocol 5. Next to Protocol, click Add new entry. 6. From the Value keyword list, select icmp. 7. Click OK twice to return to the Term page.</td>
<td>Enter set term term1 from protocol icmp</td>
</tr>
</tbody>
</table>
Table 86: Configuring a Dialer Filter for Interesting Packets (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Configure the then part of the dialer filter. | 1. Next to Then, click **Configure**.  
2. From the Designation list, select **Note**.  
3. Click **OK**. | Enter set term1 then note |

Applying the Dial-on-Demand Dialer Filter to the Dialer Interface

To complete dial-on-demand routing with dialer filter configuration:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 87 on page 329.
3. When you are finished configuring the device, commit the configuration.
4. Go on to any of the following optional tasks:
   - “Configuring Dial-on-Demand Routing Backup with OSPF Support (Optional)” on page 331.
   - “Configuring Bandwidth on Demand (Optional)” on page 332.
   - Configuring Dial-In and Callback (Optional) on page 337
5. To verify that the network interface is configured correctly, see “Verifying the ISDN Configuration” on page 343.

Table 87: Applying the Dialer Filter to the Dialer Interface

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Navigate to the **Interfaces** level in the configuration hierarchy. | 1. In the J-Web interface, select **Configure > CLI Tools > Point and Click CLI**  
2. Next to Interfaces, click **Configure** or **Edit**. | From the [edit] hierarchy level, enter edit interfaces dl0 unit 0 |
| Select the dialer interface to apply the filter—for example, dl0. | 1. In the Interface name column, click **dl0**  
2. Under Unit, in the Mtu column, click **Edit**. | |
| Select the dialer filter and apply it to the dialer interface. | 1. In the Family section, next to Inet, click **Edit**.  
2. Next to Filter, click **Configure**.  
3. In the Dialer box, type **int-packet**, the dialer-filter configured in “Configuring the Dialer Filter” on page 328, as the dialer-filter.  
4. Click **OK**. | 1. Enter **edit family inet filter**  
2. Enter **set dialer int-packet** |
**Configuring Dialer Watch**

Dialer watch is a backup method that integrates backup dialing with routing capabilities and provides reliable connectivity without relying on a dialer filter to trigger outgoing ISDN connections. With dialer watch, the device monitors the existence of a specified route and if the route disappears, the dialer interface initiates the ISDN connection as a backup connection.

**Adding a Dialer Watch Interface on the Device**

To configure dialer watch:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 88 on page 330.
3. Go on to “Configuring the ISDN Interface for Dialer Watch” on page 330.

**Table 88: Adding a Dialer Watch Interface**

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Interfaces level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit interfaces</td>
</tr>
<tr>
<td></td>
<td>2. Next to Interfaces, click Configure or Edit.</td>
<td></td>
</tr>
<tr>
<td>Select a dialer interface—for example, dl0. Adding a description, such as dialer-watch, can help you identify one dialer interface from another.</td>
<td>1. Under Interface name, select dl0.</td>
<td>1. Enter edit dl0</td>
</tr>
<tr>
<td></td>
<td>2. In the Description box, type dialer-watch.</td>
<td>2. Enter set description dialer-watch</td>
</tr>
<tr>
<td>On a logical interface—for example, 0—specify a dial pool—for example, dw-group—to link the dialer interface to at least one ISDN physical interface. Then configure the list of routes for dialer watch—for example, 172.27.27.0/24.</td>
<td>1. Under Unit, click the logical unit number 0.</td>
<td>1. Enter edit unit 0 dialer-options</td>
</tr>
<tr>
<td></td>
<td>2. Next to Dialer options, click Edit.</td>
<td>2. Enter set pool dw-group</td>
</tr>
<tr>
<td></td>
<td>3. In the Pool box, type dw-group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Next to Watch list, click Add new entry.</td>
<td>3. Enter set watch-list 172.27.27.0/24</td>
</tr>
<tr>
<td></td>
<td>5. In the Prefix box, type 172.27.27.0/24.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Click OK.</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring the ISDN Interface for Dialer Watch**

To configure the ISDN interface to participate as a dialer watch interface:
1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 89 on page 331.
3. If you are finished configuring the device, commit the configuration.
4. Go on to any of the following optional tasks:
   ■ “Configuring Dial-on-Demand Routing Backup with OSPF Support (Optional)” on page 331.
   ■ “Configuring Bandwidth on Demand (Optional)” on page 332.
   ■ Configuring Dial-In and Callback (Optional) on page 337.
5. To verify that the network interface is configured correctly, see “Verifying the ISDN Configuration” on page 343.

### Table 89: Configuring an ISDN Interface for Dialer Watch

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Interfaces</strong> level in the configuration hierarchy, and select an ISDN physical interface—for example, br-1/0/3 for ISDN BRI. For ISDN PRI, select a channelized T1/E1/ISDN PRI interface—for example, ct1-1/0/1.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI. 2. Next to Interfaces, click <strong>Configure or Edit</strong>. 3. Under Interface name:  ■ For ISDN BRI, click <strong>br-1/0/3</strong>  ■ For ISDN PRI, click <strong>ct1-1/0/1</strong>.</td>
<td>From the [edit] hierarchy level:  ■ For ISDN BRI, enter edit interfaces br-1/0/3 dialer-options pool isdn-dialer-group  ■ For ISDN PRI, enter edit interfaces ct1-1/0/1 dialer-options isdn-dialer-group</td>
</tr>
<tr>
<td>Configure dialer watch options for each ISDN interface participating in the dialer watch feature. Each ISDN interface must have the same pool identifier to participate in dialer watch. Therefore, the dialer pool name isdn-dialer-group, for the dialer watch interface configured in Table 88 on page 330, is used when configuring the ISDN interface.</td>
<td>1. Next to Dialer options, click <strong>Edit</strong>. 2. Next to Pool, click <strong>Add new entry</strong>. 3. In the Pool identifier box, type isdn-dialer-group. 4. Click <strong>OK</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Dial-on-Demand Routing Backup with OSPF Support (Optional)

Two types of routing protocol traffic are used by OSPF to establish and maintain network structure. First, periodic hello packets are sent over each link for neighbor discovery and maintenance. Second, OSPF protocol traffic achieves and maintains link-state database synchronization between devices. The OSPF demand circuit feature removes the periodic nature of both traffic types and reduces the amount of OSPF traffic by removing all OSPF protocol traffic from a demand circuit when the routing domain is in a steady state. This feature allows the underlying data-link connections to be closed when no application traffic is on the network.
You must configure OSPF on the device before configuring on-demand routing backup with OSPF support. For information on configuring OSPF, see Junos OS Routing Protocols and Policies Configuration Guide for Security Devices.

To configure OSPF demand circuits:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 90 on page 332.
3. If you are finished configuring the device, commit the configuration.
4. To verify that the network interface is configured correctly, see “Verifying the ISDN Configuration” on page 343.

Table 90: Configuring OSPF Demand Circuits

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Protocols level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit protocols ospf area 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>2. Next to Protocols, click Configure or Edit.</td>
<td>edit protocols ospf area 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td>3. Next to Ospf, click Configure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Next to Area, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. In the Area id box, type 0.0.0.0.</td>
<td></td>
</tr>
<tr>
<td>Configure OSPF on-demand circuits for each ISDN dialer interface participating as an on-demand routing interface—for example, dl0.</td>
<td>1. Next to Interface, click Add new entry.</td>
<td>1. Enter edit interface dl0</td>
</tr>
<tr>
<td></td>
<td>2. In the Interface name box, type dl0.0.</td>
<td>2. Enter set demand-circuit</td>
</tr>
<tr>
<td></td>
<td>3. Select Demand circuit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Click OK.</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring Bandwidth on Demand (Optional)**

You can define a threshold for network traffic on the device using the dialer interface and ISDN interfaces. A number of ISDN interfaces are aggregated together into a bundle and assigned a single dialer profile. Initially, only one ISDN link is active and all packets are sent through this interface. When a configured threshold is exceeded, the dialer interface activates another ISDN link and initiates a data connection. The threshold is specified as a percentage of the cumulative load of all_UP_links that are part of the bundle. When the cumulative load of all_UP_links, not counting the most recently activated link, is at or below the threshold, the most recently activated link is deactivated.

**Configuring Dialer Interfaces for Bandwidth on Demand**

To configure a dialer interface for bandwidth-on-demand:
1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 91 on page 333.
3. Go on to “Configuring an ISDN Interface for Bandwidth on Demand” on page 336.

### Table 91: Configuring a Dialer Interface for Bandwidth on Demand

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Interfaces level in the configuration hierarchy, and select a dialer interface—for example, dl0.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit interfaces dl0</td>
</tr>
<tr>
<td></td>
<td>2. Next to Interfaces, click Edit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Next to dl0, click Edit.</td>
<td></td>
</tr>
<tr>
<td>Configure multilink properties on the dialer interface.</td>
<td>1. Select multilink-ppp as the encapsulation type.</td>
<td>Enter set encapsulation multilink-ppp</td>
</tr>
<tr>
<td>Configure the dialer options.</td>
<td>2. In the Unit section, click Dialer options under Encapsulation.</td>
<td></td>
</tr>
<tr>
<td>■ Dial string—Telephone number for the interface to dial that establishes ISDN connectivity—for example, 4085550115. You can configure a maximum of 15 dial strings per dialer interface.</td>
<td>3. Next to Dial string, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td>■ Load interval—Interval of time used to calculate the average load on the dialer interface—for example, 90. Default value is 60 seconds with a range of 20-180 seconds. The value must be a multiple of 10.</td>
<td>4. In the Value box, type 4085550115 and click OK.</td>
<td></td>
</tr>
<tr>
<td>■ Load threshold—Threshold above which an additional ISDN interface is activated, specified as a percentage of the cumulative load of all UP links—for example 95. Default value is 100 with a range of 0–100.</td>
<td>5. In the Load interval box, type 90.</td>
<td></td>
</tr>
<tr>
<td>■ Pool—Name of a group of ISDN interfaces configured to use the dialer interface—for example, bw-pool.</td>
<td>6. In the Pool box, type bw-pool.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. Click OK.</td>
<td></td>
</tr>
</tbody>
</table>

- Enter
- edit unit 0
- edit dialer-options
- set dial-string 4085550115
- set load-interval 90
- set load-threshold 95
- set pool bw-pool
Table 91: Configuring a Dialer Interface for Bandwidth on Demand (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure unit properties. To configure multiple dialer interfaces for bandwidth-on-demand, increment the unit number—for example, dl0.1, dl0.2, and so on. <strong>F max period</strong>—Maximum number of compressed packets allowed between the transmission of full packets—for example, 100. The value can be between 1 and 65535.</td>
<td>1. Next to Compression, select Yes, and then click <strong>Configure</strong>. 2. Select <strong>Rtp</strong>, and then click <strong>Configure</strong>. 3. In the <strong>F max period</strong> box, type <strong>100</strong>. 4. Next to <strong>Queues</strong>, click <strong>Add new entry</strong>. 5. From the <strong>Value</strong> list, select <strong>q3</strong>. 6. Click <strong>OK</strong> until you return to the Unit page.</td>
<td>1. From the [edit] hierarchy level, enter <code>edit interfaces dl0 unit 0</code> 2. Enter <code>set compression rtp f-max-period 500</code> <code>queues q3</code></td>
</tr>
<tr>
<td>Configure logical properties. <strong>Fragment threshold</strong>—Maximum size, in bytes, for multilink packet fragments. The value can be between 128 and 16320 bytes, for example, 1024. The default is 0 bytes (no fragmentation). Any nonzero value must be a multiple of 64 bytes. <strong>Maximum received reconstructed unit (MRRU)</strong>—This value is expressed as a number between 1500 and 4500 bytes—for example, 1500</td>
<td>1. In the Fragment threshold box, type <strong>1024</strong>. 2. In the <strong>Mrru</strong> box, type <strong>1500</strong>. 3. Click <strong>OK</strong> until you return to the main Configuration page.</td>
<td>1. Enter <code>set fragment-threshold 1024</code> 2. Enter <code>set mrru 1500</code></td>
</tr>
<tr>
<td>Define a CHAP access profile with a client and a secret password. For example, define <strong>bw-profile</strong> with client 1 and password <strong>my-secret</strong>.</td>
<td>1. On the main Configuration page next to <strong>Access</strong>, click <strong>Configure</strong> or <strong>Edit</strong>. 2. Next to <strong>Profile</strong>, click <strong>Add new entry</strong>. 3. In the Profile name box, type <strong>bw-profile</strong>. 4. Next to <strong>Client</strong>, click <strong>Add new entry</strong>. 5. In the <strong>Name</strong> box, type <strong>client1</strong>. 6. In the Chap secret box, type <strong>my-secret</strong>. 7. Click <strong>OK</strong> until you return to the main Configuration page.</td>
<td>From the [edit] hierarchy level, enter <code>set access profile bw-profile client client1</code> <code>chap-secret my-secret</code></td>
</tr>
</tbody>
</table>
### Table 91: Configuring a Dialer Interface for Bandwidth on Demand (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Navigate to the appropriate dialer interface level in the configuration hierarchy—for example, dl0 unit 0. | 1. On the main Configuration page next to Interfaces, click **Configure** or **Edit**.  
2. In the interface name box, click **dl0**.  
3. In the Interface unit number box, click **0**. | From the [edit] hierarchy level, enter **edit interfaces dl0 unit 0** |
| Configure CHAP on the dialer interface and specify a unique profile name containing a client list and access parameters—for example, **bw-profile**. | 1. Next to Ppp options, click **Configure**.  
2. Next to Chap, click **Configure**.  
3. Next to Access data, select Access profile.  
4. In the Access profile box, type **bw-profile**.  
5. Click **OK**. | Enter **set ppp-options chap access-profile bw-profile** |
| Configure packet compression. You can configure the following compression types: | 1. Under Compression, select **Acfc**.  
2. Click **OK** until you return to the Unit page. | Enter **set ppp-options compression acfc** |

- **ACFC (address and control field compression)**—Conserves bandwidth by compressing the address and control fields of PPP-encapsulated packets.  
- **PFC (protocol field compression)**—Conserves bandwidth by compressing the protocol field of a PPP-encapsulated packet.
Table 91: Configuring a Dialer Interface for Bandwidth on Demand (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the dialer interface to be assigned an IP address in one of the following ways:</td>
<td>Do one of the following:</td>
<td></td>
</tr>
<tr>
<td>■ Assign source and destination IP addresses as described in Table 84 on page 324—for example, 172.20.10.2 and 172.20.10.1. (The destination IP address is optional.)</td>
<td>■ To assign source and destination IP addresses, enter set family inet address 172.20.10.2 destination 172.20.10.1</td>
<td></td>
</tr>
<tr>
<td>■ Obtain an IP address by negotiation with the remote end. This method might require the access concentrator to use a RADIUS authentication server.</td>
<td>■ To obtain an IP address from the remote end, enter set family inet negotiate-address</td>
<td></td>
</tr>
<tr>
<td>■ Derive the source address from a specified interface—for example, the loopback interface, lo0.0—and assign a destination address—for example, 192.168.1.2. The specified interface must include a logical unit number and have a configured IP address.</td>
<td>■ To derive the source address and assign the destination address, enter set family inet unnumbered-address lo0.0 destination 192.168.1.2</td>
<td></td>
</tr>
</tbody>
</table>

To assign source and destination IP addresses:
1. Next to Address, click Add new entry.
2. In the Source box, type 172.20.10.2.
3. In the Destination box, type 172.20.10.1.
4. Click OK.

To assign source and destination IP addresses (continued):

To obtain an IP address from the remote end:
1. Next to Negotiate address, select the Yes check box.
2. Click OK.

To derive the source address and assign the destination address:
1. Next to Unnumbered address, select the Yes check box and click Configure.
2. In the Destination box, type 192.168.1.2.
3. In the Source box, type lo0.0.
4. Click OK.

Configuring an ISDN Interface for Bandwidth on Demand

To configure bandwidth on demand on the ISDN interface:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 92 on page 337. Repeat these tasks for each ISDN interface participating in the aggregated link.
3. If you are finished configuring the device, commit the configuration.
4. To verify that the network interface is configured correctly, see “Verifying the ISDN Configuration” on page 343.
Table 92: Configuring an ISDN Interface for Bandwidth on Demand

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Interfaces level in the configuration hierarchy, and select an ISDN BRI physical interface—for example, br-1/0/3. For ISDN PRI, select a channelized T1/E1/ISDN PRI interface—for example, ct1-1/0/1.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level:</td>
</tr>
<tr>
<td></td>
<td>2. Next to Interfaces, click Edit.</td>
<td>■ For ISDN BRI, enter edit interfaces br-1/0/3</td>
</tr>
<tr>
<td></td>
<td>3. Under Interface name:</td>
<td>■ For ISDN PRI, enter edit interfaces ct1-1/0/1</td>
</tr>
<tr>
<td></td>
<td>■ For ISDN BRI, click br-1/0/3.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ For ISDN PRI, click ct1-1/0/1.</td>
<td></td>
</tr>
<tr>
<td>Because each ISDN interface must have the same pool identifier to participate in bandwidth on demand, use the dialer pool name bw-pool, the dialer interface configured in Table 91 on page 333, to configure the ISDN interfaces participating in the pool. For ISDN BRI, you can group up to four ISDN interfaces together when configuring bandwidth on demand, for a total of eight B-channels (two channels per interface) providing connectivity. For ISDN PRI, the pool limit is eight B-channels per channelized T1/E1/ISDN PRI port.</td>
<td>1. Next to Dialer options, click Dialer options.</td>
<td>Enter set dialer-options pool bw-pool</td>
</tr>
<tr>
<td></td>
<td>2. Next to Pool, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. In the Pool identifier box, type the name of the dialer pool—for example, bw-pool.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Click OK.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Dial-In and Callback (Optional)

If you are a service provider or a corporate data center into which a remote location dials in during an emergency, you can configure your Juniper Networks device to accept incoming ISDN calls originating from the remote location, or reject the incoming calls and call back the remote location. The callback feature lets you control access by allowing only specific remote locations to connect to the device. You can also configure the device to reject all incoming ISDN calls.

**NOTE:** Incoming voice calls are currently not supported.

When it receives an incoming ISDN call, the Juniper Networks device matches the incoming call’s caller ID against the caller IDs configured on its dialer interfaces. If an exact match is not found and the incoming call’s caller ID has more digits than the configured caller IDs, the device performs a right-to-left match of the incoming call’s caller ID with the configured caller IDs and accepts the incoming call if a match is found. For example, if the incoming call’s caller ID is 4085550115 and the caller ID configured on a dialer interface is 5550115, the incoming call is accepted. Each dialer interface accepts calls from only callers whose caller IDs are configured on it.

The dialer interface of the device and the dialer interface of the remote device must have the same encapsulation—PPP, Multilink PPP, or Cisco HDLC. If the encapsulation...
is different, the ISDN call is dropped. Table 93 on page 338 describes how the device performs encapsulation monitoring.

Table 93: Encapsulation Monitoring by Juniper Networks Devices

<table>
<thead>
<tr>
<th>Encapsulation on Juniper Networks Device’s Interface</th>
<th>Encapsulation on Remote Router’s Dialer Interface</th>
<th>Possible Action on Juniper Networks Device’s Dialer Interface</th>
<th>Encapsulation Monitoring and Call Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPP</td>
<td>PPP</td>
<td>■ Accepts an incoming call</td>
<td>Device performs encapsulation monitoring</td>
</tr>
<tr>
<td>Multilink PPP</td>
<td>Multilink PPP</td>
<td>■ Rejects an incoming call and calls back the incoming number when callback is enabled on the dialer interface</td>
<td>ISDN call is successful because encapsulation matches.</td>
</tr>
<tr>
<td>PPP</td>
<td>Multilink PPP or Cisco HDLC</td>
<td>■ Accepts an incoming call as a result of having originally dialed out, because the dialer interface of the remote device has callback enabled</td>
<td>Device performs encapsulation monitoring.</td>
</tr>
<tr>
<td>Multilink PPP</td>
<td>PPP or Cisco HDLC</td>
<td>■ Dials out</td>
<td>ISDN call is dropped because of encapsulation mismatch.</td>
</tr>
<tr>
<td>PPP or Multilink PPP</td>
<td>PPP, Multilink PPP, or Cisco HDLC</td>
<td>■ Accepts an incoming call as a result of having originally dialed out, because the dialer interface of the remote device has callback enabled</td>
<td>Device does not perform encapsulation monitoring.</td>
</tr>
<tr>
<td>Cisco HDLC</td>
<td>PPP, Multilink PPP, or Cisco HDLC</td>
<td>■ Dials out</td>
<td>Success of the ISDN call depends on the encapsulation monitoring capability of the remote device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Accepts an incoming call</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Accepts an incoming call as a result of having originally dialed out, because the dialer interface of the remote device has callback enabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Rejects an incoming call and calls back the incoming number when callback is enabled on the dialer interface</td>
<td></td>
</tr>
</tbody>
</table>

This section contains the following topics:

- Configuring Dialer Interfaces for Dial-In and Callback on page 339
- Configuring an ISDN Interface to Screen Incoming Calls on page 340
- Configuring the Device to Reject Incoming ISDN Calls on page 341
Configuring Dialer Interfaces for Dial-In and Callback

To configure a dialer interface for dial-in and callback:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 94 on page 339.
3. If you are finished configuring the device, commit the configuration.
4. To verify that the network interface is configured correctly, see “Verifying the ISDN Configuration” on page 345.

Table 94: Configuring the Dialer Interface for Dial-In and Callback

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Interfaces level in the configuration hierarchy, and select a dialer interface—for example, dl0.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit interfaces dl0.</td>
</tr>
<tr>
<td></td>
<td>2. Next to Interfaces, click Configure or Edit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Next to dl0, click Edit.</td>
<td></td>
</tr>
</tbody>
</table>

On a logical interface—for example, 0—configure the incoming map options for the dialer interface. To use dial-in, you must configure an incoming map on the dialer interface.

- **Accept all**—Dialer interface accepts all incoming calls.
  
  You can configure this option for only one of the dialer interfaces associated with an ISDN physical interface. The dialer interface configured to accept all calls is used only if the incoming call’s caller ID does not match the caller IDs configured on other dialer interfaces.

- **Caller**—Dialer interface accepts calls from a specific caller ID—for example, 4085550115. You can configure a maximum of 15 caller IDs per dialer interface.

  The same caller ID must not be configured on different dialer interfaces. However, you can configure caller IDs with more or fewer digits on different dialer interfaces. For example, you can configure the caller IDs 14085550115, 4085550115, and 5550115 on different dialer interfaces.
### Table 94: Configuring the Dialer Interface for Dial-In and Callback (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Configure callback options for the dialer interface | 1. Select **Callback**. 2. In the **Callback wait period** box, type 5. | 1. Enter **set callback**  
2. Enter **set callback-wait-period 5** |

- **Callback**—Enable this feature to allow the ISDN interface to reject incoming calls, wait for 5 seconds (the default callback wait period), and then call back the incoming number.

Before configuring callback on a dialer interface, ensure that the following conditions exist:

- The dialer interface is not configured as a backup for a primary interface.
- The dialer interface does not have a watch list configured.
- Only one dial string is configured for the dialer interface.
- Dial-in is configured on the dialer interface of the remote device that is dialing in.

- **Callback wait period**—Number of seconds to wait before redialing an incoming ISDN call.

## Configuring an ISDN Interface to Screen Incoming Calls

By default, an ISDN interface is configured to accept all incoming calls. If multiple devices are connected to the same ISDN line, you can configure an ISDN interface to screen incoming calls based on the incoming called number.

You can configure the incoming called numbers that you want an ISDN interface to accept. You can also use the reject option to configure a called number that you want an ISDN interface to ignore because the number belongs to another device connected to the same ISDN line. For example, if another device on the same ISDN line has the called number 4085551091, you can configure the called number 4085551091 with the reject option on the ISDN interface so that it does not accept calls with that number.

When it receives an incoming ISDN call, the device matches the incoming called number against the called numbers configured on its ISDN interfaces. If an exact match is not found, or if the called number is configured with the reject option, the incoming call is ignored. Each ISDN interface accepts only the calls whose called numbers are configured on it.

To configure an ISDN interface to screen incoming ISDN calls:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 95 on page 341.
3. If you are finished configuring the device, commit the configuration.

4. To verify that the network interface is configured correctly, see “Verifying the ISDN Configuration” on page 343.

Table 95: Configuring an ISDN Interface to Screen Incoming ISDN Calls

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Navigate to the Interfaces level in the configuration hierarchy, and select an ISDN physical interface—for example, br-1/0/3. For ISDN PRI, select a channelized T1/E1/ISDN PRI interface—for example, ct1-1/0/1. | 1. In the J-Web interface, select Configure > CLI Tools > Point and Click CLI.  
2. Next to Interfaces, click Configure or Edit.  
3. Under Interface name:  
   - For ISDN BRI, click br-1/0/3.  
   - For ISDN PRI, click ct1-1/0/1. | From the [edit] hierarchy level:  
   - For ISDN BRI, enter edit interfaces br-1/0/3  
   - For ISDN PRI, enter edit interfaces ct1-1/0/1 |
| Configure the incoming called number—for example, 4085550115—for the ISDN interface. To configure the ISDN interface to ignore the incoming called number, use the reject option. | 1. Next to Isdn options, click Edit.  
2. Next to Incoming called number, click Add new entry.  
3. In the Called number box, type 4085550115.  
4. Click OK. | Enter set isdn-options incoming-called-number 4085550115 |

Configuring the Device to Reject Incoming ISDN Calls

By default, the device is configured to accept incoming ISDN calls. The incoming calls are accepted if dial-in is configured on the device. You can configure the device to reject all incoming ISDN calls.

To configure the device to reject incoming ISDN calls:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.

2. Perform the configuration tasks described in Table 96 on page 342.

3. If you are finished configuring the device, commit the configuration.

4. To verify that the network interface is configured correctly, see “Verifying the ISDN Configuration” on page 343.
Table 96: Configuring the Device to Reject Incoming ISDN Calls

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Processes level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter set system processes isdn-signaling reject-incoming</td>
</tr>
<tr>
<td></td>
<td>2. Next to System, click Configure or Edit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Next to Processes, click Configure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Next to Isdn signaling, click Configure.</td>
<td></td>
</tr>
<tr>
<td>Configure the device to reject incoming calls.</td>
<td>1. Select the Reject Incoming check box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Click OK.</td>
<td></td>
</tr>
</tbody>
</table>

Disabling Dialing Out Through Dialer Interfaces

The JUNOS ISDN dialer services process manages dialing out through dialer interfaces. You can disable dialing out through all dialer interfaces by disabling the dialer services process.

**CAUTION:** Never disable a software processes unless instructed to do so by a Customer Support engineer.

To disable dialing out through dialer interfaces:
1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 97 on page 342.
3. If you are finished configuring the device, commit the configuration.

Table 97: Disabling Dialing Out Through Dialer Interfaces

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Processes level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter set system processes dialer-services disable</td>
</tr>
<tr>
<td></td>
<td>2. Next to System, click Configure or Edit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Next to Processes, click Configure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Next to Dialer services, click Configure.</td>
<td></td>
</tr>
<tr>
<td>Disable dialing out through dialer interfaces.</td>
<td>1. Select the Disable check box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Click OK.</td>
<td></td>
</tr>
</tbody>
</table>
Disabling ISDN Signaling

The JUNOS ISDN signaling process manages ISDN signaling by initializing ISDN connections. You can disable ISDN signaling by disabling the ISDN signaling process.

CAUTION: Never disable a software processes unless instructed to do so by a Customer Support engineer.

To disable ISDN signaling:
1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 98 on page 343.
3. If you are finished configuring the device, commit the configuration.

Table 98: Disabling ISDN Signaling

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Navigate to the Processes level in the configuration hierarchy. | 1. In the J-Web interface, select Configure > CLI Tools > Point and Click CLI.  
2. Next to System, click Configure or Edit.  
3. Next to Processes, click Configure. | From the [edit] hierarchy level, enter set system processes isdn-signaling disable |
| Disable ISDN signaling on the device. | 1. Select the Disable check box.  
2. Click OK. | |

Verifying the ISDN Configuration

To verify an ISDN configuration, perform the following tasks:
- Displaying the ISDN Status on page 344
- Verifying an ISDN BRI Interface on page 345
- Verifying an ISDN PRI Interface and Checking B-Channel Interface Statistics on page 346
- Checking D-Channel Interface Statistics on page 347
- Displaying the Status of ISDN Calls on page 349
- Verifying Dialer Interface Configuration on page 350
### Displaying the ISDN Status

**Purpose**
Display the status of ISDN service on the ISDN interface. For example, you can display ISDN BRI status on the `br-6/0/0` interface and ISDN PRI status on the `ct1-2/0/0` interface.

**Action**
From the operational mode in the CLI, enter `show isdn status`.

**Sample Output**
```
user@host> show isdn status
Interface: br-6/0/0
Layer 1 status: active
Layer 2 status:
   CES: 0, Q.921: up, TEI: 12
Layer 3 status: 1 Active calls
   Switch Type : ETSI
   Interface Type : USER
   T310 : 10 seconds
   Tei Option : Power Up

user@host> show isdn status
Interface: ct1-2/0/0
Layer 1 status: active
Layer 2 status:
   CES: 0, Q.921: up, TEI: 0
Layer 3 status: 8 Active calls
   Switch Type : NI2
   Interface Type : USER
   T310 : 10 seconds
   Tei Option : Power Up
```

**Meaning**
The output shows a summary of interface information. Verify the following information:

- **Interface**—ISDN interface currently active on the device. For ISDN BRI, the interface is a `br-pim/0/port` interface, as shown in the first example for `br-6/0/0`. For ISDN PRI, the interface displayed is a channelized T1 or channelized E1 interface, as shown in the second example for `ct1-2/0/0`.

- **Layer 1 status**—Indicates whether Layer 1 is active or inactive.

- **Layer 2 status**—Indicates whether Q.921 (the D-channel protocol) is up or down.

- **TEI**—Assigned terminal endpoint identifier (TEI) number.

- **Layer 3 status**—Number of active calls.

- **Switch Type**—Type of ISDN switch connected to the device interface.

- **Interface Type**—Default value for the local interface.

- **Calling number**—Telephone number configured for dial-out.

- **T310**—Q.931-specific timer.

- **TEI Option**—Indicates when TEI negotiations occur on the interface.
Verifying an ISDN BRI Interface

**Purpose**
Verify that the ISDN BRI interface is correctly configured.

**Action**
From the CLI, enter the `show interfaces extensive` command. Alternatively, from the J-Web interface select **Monitor > Interfaces > br-6/0/0**.

**Sample Output**

```
user@host> show interfaces br-6/0/0 extensive
Physical interface: br-6/0/0, Enabled, Physical link is Up
  Interface index: 143, SNMP ifIndex: 59, Generation: 24
  Type: BRI, Link-level type: Controller, MTU: 4092, Clocking: 1, Speed: 144kbps,
  Parent: None
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Link type      : Full-Duplex
  Link flags     : None
  Physical info  : S/T
  Hold-times     : Up 0 ms, Down 0 ms
  Last flapped   : 2005-12-07 12:21:11 UTC (04:07:26 ago)
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes : 0 0 bps
    Output bytes : 0 0 bps
    Input packets: 0 0 pps
    Output packets: 0 0 pps
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards: 0
    Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors: 0
```

**Meaning**
The output shows a summary of interface information. Verify the following information:

- The physical interface is **Enabled**. If the interface is shown as **Disabled**, do either of the following:
  - In the CLI configuration editor, delete the `disable` statement at the `[edit interfaces interface-name]` level of the configuration hierarchy.
  - In the J-Web configuration editor, clear the **Disable** check box on the **Interfaces > interface-name** page.

- The physical link is **Up**. A link state of **Down** indicates a problem with the interface module, interface port, or physical connection (link-layer errors).
The **Last Flapped** time is an expected value. The **Last Flapped** time indicates the last time the physical interface became unavailable and then available again. Unexpected flapping indicates likely link-layer errors.

The traffic statistics reflect expected input and output rates. Verify that the number of inbound and outbound bytes and packets matches expected throughput for the physical interface. To clear the statistics and see only new changes, use the `clear interfaces statistics interface-name` command.

**Related Topics** For a complete description of `show interfaces` (ISDN BRI) output, see the *Junos Interfaces Command Reference*.

### Verifying an ISDN PRI Interface and Checking B-Channel Interface Statistics

**Purpose** Verify that an ISDN B-channel interface is operating properly. For ISDN PRI, verify that a B-channel interface is configured correctly. (To display a list of B-channel interfaces, enter the `show isdn calls` command.)

**Action** From the CLI, enter the `show interfaces extensive` command. Alternatively, from the J-Web interface select **Monitor > Interfaces > bc-0/0/4:1**.

**Sample Output**

```
user@host> show interfaces bc-0/0/4:1 extensive
Physical interface: bc-0/0/4:1, Administratively down, Physical link is Up
Interface index: 145, SNMP ifIndex: 75, Generation: 26
Type: Serial, Link-level type: Multilink-PPP, MTU: 1510, Clocking: Internal,
Speed: 64kbps,
Parent: br-0/0/4 Interface index 143
Device flags   : Present Running
Interface flags: Admin-Test SNMP-Traps 16384
Link type      : Full-Duplex
Link flags     : None
Physical info  : Unspecified
Hold-times     : Up 0 ms, Down 0 ms
Current address: Unspecified, Hardware address: Unspecified
Alternate link address: Unspecified
CoS queues     : 8 supported, 8 maximum usable queues
Last flapped   : Never
Statistics last cleared: Never
Traffic statistics:
Input bytes : 5787 0 bps
Output bytes: 3816 0 bps
Input packets: 326 0 pps
Output packets: 264 0 pps
Input errors:
   Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards: 6,
   Resource errors: 0
Output errors:
   Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors: 0
  Queue counters Queued packets Transmitted Packets Dropped packets
  0 best-effort        314335        0          0
  1 best-effort            0          0          0
  2 best-effort              5          0          0
  3 best-effort           5624         5624        0
```

346  ■  Verifying an ISDN PRI Interface and Checking B-Channel Interface Statistics
Packet Forwarding Engine configuration:
Destination slot: 5, PLP byte: 1 (0x00)

<table>
<thead>
<tr>
<th>CoS transmit queue</th>
<th>Bandwidth</th>
<th>Buffer Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit</td>
<td>%</td>
<td>bps</td>
</tr>
<tr>
<td>0 best-effort</td>
<td>95</td>
<td>60800</td>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 network-control</td>
<td>5</td>
<td>3200</td>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Logical interface bc-0/0/4:1.0 (Index 71) (SNMP ifIndex 61) (Generation 33)
Flags: Device Down Point-To-Point SNMP-Traps Encapsulation: PPP
Protocol mlppp, Multilink bundle: dl0.0, MTU: 1506, Generation: 18, Route table: 0

**Meaning**
The output shows a summary of B-channel interface information. Verify the following information:

- The physical interface is **Enabled**. If the interface is shown as **Disabled**, do either of the following:
  - In the CLI configuration editor, delete the `disable` statement at the `[edit interfaces interface-name]` level of the configuration hierarchy.
  - In the J-Web configuration editor, clear the **Disable** check box on the **Interfaces > interface-name** page.

- The physical link is **Up**. A link state of **Down** indicates a problem with the interface module, interface port, or physical connection (link-layer errors).

- For ISDN BRI, the **Parent** interface is a `br-pim/0/port` interface—`br-0/0/4` in this example. For ISDN PRI, the **Parent** interface is a channelized T1 or channelized E1 interface—`ct1–pim/0/port` or `ce1–pim/0/port`.

- The **Last Flapped** time is an expected value. The **Last Flapped** time indicates the last time the physical interface became unavailable and then available again. Unexpected flapping indicates possible link-layer errors.

- The traffic statistics reflect expected input and output rates. Verify that the number of inbound and outbound bytes and packets matches expected throughput for the physical interface. To clear the statistics and see only new changes, use the `clear interfaces statistics interface-name` command.

**Related Topics**
For a complete description of `show interfaces` (ISDN B-channel) output, see the *Junos Interfaces Command Reference.*

### Checking D-Channel Interface Statistics

**Purpose**
Verify that the ISDN D-channel interface is operating properly. For ISDN PRI, verify that the D-channel interface is configured correctly.

**Action**
From the CLI, enter the `show interfaces extensive` command. Alternatively, from the J-Web interface select **Monitor > Interfaces > dc-0/0/4**.
Sample Output

```
user@host> show interfaces dc-0/0/4 extensive
Physical interface: dc-0/0/4, Enabled, Physical link is Up
    Interface index: 144, SNMP ifIndex: 60, Generation: 25
    Type: Serial, Link-level type: 55, MTU: 4092, Clocking: Internal, Speed: 16kbps,
    Parent: br-0/0/4 Interface index 143
    Device flags   : Present Running
    Interface flags: SNMP-Traps Internal: 0x4000
    Link type      : Full-Duplex
    Link flags     : None
    Physical info  : Unspecified
    Hold-times     : Up 0 ms, Down 0 ms
    Current address: Unspecified, Hardware address: Unspecified
    Alternate link address: Unspecified
    Last flapped   : 2005-12-07 12:21:12 UTC (05:46:00 ago)
    Statistics last cleared: Never
    Traffic statistics:
        Input bytes  : 13407 0 bps
        Output bytes : 16889 0 bps
        Input packets: 3262 0 pps
        Output packets: 3262 0 pps
    Input errors:
        Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards: 0,
        Resource errors: 0
    Output errors:
        Carrier transitions: 1, Errors: 0, Drops: 0, MTU errors: 0, Resource errors: 0
    ISDN alarms   : None
    ISDN media:
        LOF    Seconds  Count  State
        LOF    0        1      OK
        LOS    0        0      OK

Logical interface dc-0/0/4.32767 (Index 70) (SNMP ifIndex 72) (Generation 8)
    Flags: Point-To-Point SNMP-Traps Encapsulation: 60
    Traffic statistics:
        Input bytes  : 13407
        Output bytes : 82129
        Input packets: 3262
        Output packets: 3262
    Local statistics:
        Input bytes  : 13407
        Output bytes : 82129
        Input packets: 3262
        Output packets: 3262
```

Meaning

The output shows a summary of D-channel interface information. Verify the following information:

- The physical interface is **Enabled**. If the interface is shown as **Disabled**, do either of the following:
  - In the CLI configuration editor, delete the `disable` statement at the `[edit interfaces interface-name]` level of the configuration hierarchy.
In the J-Web configuration editor, clear the **Disable** check box on the **Interfaces > interface-name** page.

- The physical link is **Up**. A link state of **Down** indicates a problem with the interface module, interface port, or physical connection (link-layer errors).
- For ISDN BRI, the **Parent** interface is a `br-pim/0/port` interface—`br-0/0/4` in this example. For ISDN PRI, the **Parent** interface is a channelized T1 or channelized E1 interface—`ct1-pim/0/port` or `ce1-pim/0/port`.
- The **Last Flapped** time is an expected value. The **Last Flapped** time indicates the last time the physical interface became unavailable and then available again. Unexpected flapping indicates possible link-layer errors.
- The traffic statistics reflect expected input and output rates. Verify that the number of inbound and outbound bytes and packets matches expected throughput for the physical interface. To clear the statistics and see only new changes, use the `clear interfaces statistics interface-name` command.

**Related Topics**
For a complete description of `show interfaces` (ISDN D-channel) output, see the **Junos Interfaces Command Reference**.

### Displaying the Status of ISDN Calls

**Purpose**
Display the status of ISDN calls. This information helps you to verify the dialer interface configuration as described in “Verifying Dialer Interface Configuration” on page 350. The command also provides a list of the B-channels configured on an ISDN BRI or ISDN PRI interface.

**Action**
From the CLI, enter the `show isdn calls` command.

**Sample Output**

```bash
user@host> show isdn calls
Interface: bc-6/0/0:1
   Status: No call in progress
   Most recent error code: No error
Interface: bc-6/0/0:2
   Status: Connected to 384070
   Call Duration: 43 seconds
   Call Direction: Dialout
   Most recent error code: No error

user@host> show isdn calls
Interface: bc-2/0/0:1
   Status: Connected to 384010
   Call Duration: 49782 seconds
   Call Direction: Dialin
   Most recent error code: destination out of order
Interface: bc-2/0/0:2
   Status: Connected to 384011
   Call Duration: 49782 seconds
   Call Direction: Dialin
   Most recent error code: destination out of order
Interface: bc-2/0/0:3
   Status: Connected to 384020
```

Displaying the Status of ISDN Calls
Meaning

The output shows a summary of B-channel interfaces and the active ISDN calls on the interfaces. The first example shows the two B-channels on an ISDN BRI interface—bc-2/0/0:1 and bc-2/0/0:2. The second example indicates B-channels bc-2/0/0:1 through bc-2/0/0:23, the 23 B-channels on an ISDN PRI interface. Determine the following information:

- The interfaces on which ISDN calls are in progress
- Whether the call is a dial-in call, dial-out call, or a callback call

Related Topics

For a complete description of show isdn calls output, see the Junos Interfaces Command Reference.

Verifying Dialer Interface Configuration

Purpose

Verify that the dialer interface is correctly configured. To determine the ISDN interfaces on which calls are taking place, see “Displaying the Status of ISDN Calls” on page 349.

Action

From the CLI, enter the show interfaces dl0 extensive command. Alternatively, from the J-Web interface select Monitor > Interfaces > dl0.

Sample Output

user@host> show interfaces dl0 extensive
Physical interface: dl0, Enabled, Physical link is Up
  Interface index: 173, SNMP ifIndex: 26, Generation: 77
  Type: 27, Link-level type: PPP, MTU: 1504, Clocking: Unspecified, Speed: Unspecified
  Device flags : Present Running
  Interface flags: SNMP-Traps
  Link type : Full-Duplex
  Link flags : Keepalives
  Physical info : Unspecified
  Hold-times : Up 0 ms, Down 0 ms
  Current address: Unspecified, Hardware address: Unspecified
  Alternate link address: Unspecified
  Last flapped : Never
  Statistics last cleared: Never
### Traffic statistics:

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input bytes</td>
<td>13859</td>
<td>0 bps</td>
</tr>
<tr>
<td>Output bytes</td>
<td>0</td>
<td>0 bps</td>
</tr>
<tr>
<td>Input packets</td>
<td>317</td>
<td>0 pps</td>
</tr>
<tr>
<td>Output packets</td>
<td>0</td>
<td>0 pps</td>
</tr>
</tbody>
</table>

**Input errors:**
- Errors: 0
- Drops: 0
- Framing errors: 0
- Runts: 0
- Giants: 0
- Policed discards: 0
- Resource errors: 0

**Output errors:**
- Carrier transitions: 0
- Errors: 0
- Drops: 0
- MTU errors: 0
- Resource errors: 0

### Logical interface dl0.0 (Index 76) (SNMP ifIndex 28) (Generation 148)

- Flags: Point-To-Point SNMP-Traps 0x4000 LinkAddress 23-0 Encapsulation: PPP

**Dialer:**
- State: Active, Dial pool: 1
- Dial strings: 384070
- Subordinate interfaces: bc-6/0/0:2 (Index 172)
- Watch list: 11.12.13.14/32
- Activation delay: 0, Deactivation delay: 0
- Initial route check delay: 120
- Redial delay: 3
- Callback wait period: 5
- Load threshold: 0, Load interval: 60
- Bandwidth: 64kbps

**Traffic statistics:**
- Input bytes: 24839
- Output bytes: 17792
- Input packets: 489
- Output packets: 340

**Local statistics:**
- Input bytes: 10980
- Output bytes: 17792
- Input packets: 172
- Output packets: 340

**Transit statistics:**
- Input bytes: 13859
- Output bytes: 0
- Input packets: 317
- Output packets: 0

**Keepalive settings:** Interval 10 seconds, Up-count 1, Down-count 3

**Keepalive statistics:**
- Input: 0 (last seen: never)
- Output: 36 (last sent 00:00:09 ago)

**LCP state:** Opened

**NCP state:** inet: Opened, inet6: Not-configured, iso: Not-configured, mpls: Not-configured

**CHAP state:** Success

**Protocol inet, MTU: 1500, Generation: 74, Route table: 0**

**Flags:** Negotiate-Address

**Addresses, Flags:** Kernel Is-Preferred Is-Primary

**Destination: 43.1.1.2, Local: 43.1.1.19, Broadcast: Unspecified, Generation: 37**
Interface flags: Point-To-Point SNMP-Traps
Last flapped : 2007-02-27 01:50:38 PST (1d 15:48 ago)
Statistics last cleared: Never
Traffic statistics:

- Input bytes : 42980144 0 bps
- Output bytes : 504 0 bps
- Input packets: 934346 0 pps
- Output packets: 6 0 pps

Frame exceptions:
- Oversized frames 0
- Errored input frames 0
- Input on disabled link/bundle 0
- Output for disabled link/bundle 0
- Queuing drops 0

Buffering exceptions:
- Packet data buffer overflow 0
- Fragment data buffer overflow 0

Assembly exceptions:
- Fragment timeout 0
- Missing sequence number 0
- Out-of-order sequence number 0
- Out-of-range sequence number 0

Hardware errors (sticky):
- Data memory error 0
- Control memory error 0

Egress queues: 8 supported, 8 in use

<table>
<thead>
<tr>
<th>Queue counters</th>
<th>Queued packets</th>
<th>Transmitted packets</th>
<th>Dropped packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 q1</td>
<td>6</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>1 q2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 assured-forw</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3 q3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Logical interface d10.0 (Index 66) (SNMP ifIndex 36) (Generation 133)
Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: Multilink-PPP

Dialer:
- State: Active, Dial pool: 1
- Dial strings: 384010
- Subordinate interfaces: bc-2/0/0:8 (Index 161), bc-2/0/0:7 (Index 160),
  bc-2/0/0:6 (Index 159), bc-2/0/0:5 (Index 158), bc-2/0/0:4 (Index 157),
  bc-2/0/0:3 (Index 156), bc-2/0/0:2 (Index 155), bc-2/0/0:1 (Index 154)
- Activation delay: 0, Deactivation delay: 0
- Initial route check delay: 120
- Redial delay: 3
- Callback wait period: 5
- Load threshold: 100, Load interval: 60
- Bandwidth: 512kbps

Bundle options:
- MRRU 1504
- Remote MRRU 1504
- Drop timer period 0
- Inner PPP Protocol field compression enabled
- Sequence number format long (24 bits)
- Fragmentation threshold 0
- Links needed to sustain bundle 1
- Interleave fragments Disabled

Bundle errors:

---

JUNOS Software Interfaces and Routing Configuration Guide
Packet drops: 0 (0 bytes)
Fragment drops: 15827 (759696 bytes)
MRRU exceeded: 0
Exception events: 0

Statistics

<table>
<thead>
<tr>
<th>Frames</th>
<th>fps</th>
<th>Bytes</th>
<th>bps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bundle:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Link:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bc-2/0/0:1.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| NCP state:/inet: Opened, inet6: Not-configured, iso: Not-configured, mpls: Not-configured
Protocol inet, MTU: 1500, Generation: 138, Route table: 0
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
  Destination: 1.1.1.0/30, Local: 1.1.1.2, Broadcast: Unspecified, Generation: 134

Meaning

The output shows a summary of dialer interface information. The first example is for ISDN BRI service, and the second example is for ISDN PRI service. Verify the following information:

- The physical interface is Enabled. If the interface is shown as Disabled, do either of the following:
  - In the CLI configuration editor, delete the disable statement at the [edit interfaces interface-name] level of the configuration hierarchy.
  - In the J-Web configuration editor, clear the Disable check box on the Interfaces > interface-name page.

- The physical link is Up. A link state of Down indicates a problem with the interface module, interface port, or physical connection (link-layer errors).
- The **Last Flapped** time is an expected value. The **Last Flapped** time indicates the last time the physical interface became unavailable and then available again. Unexpected flapping indicates possible link-layer errors.

- **Subordinate interfaces** correctly lists the B-channel interface or interfaces associated with this dialer interface. The ISDN BRI output in the first example shows that `dl0` supports `bc-6/0/0:2`.

  The ISDN PRI output in the second example shows that `dl0` supports `bc-2/0/0:1` through `bc-2/0/0:8`.

- The traffic statistics reflect expected input and output rates. Verify that the number of inbound and outbound bytes and packets matches expected throughput for the physical interface. To clear the statistics and see only new changes, use the `clear interfaces statistics interface-name` command.

- The dialer state is **Active** when an ISDN call is in progress.

- The LCP state is **Opened** when an ISDN call is in progress. An LCP state of **Closed** or **Not Configured** indicates a problem with the dialer configuration that needs to be debugged with the `monitor traffic interface interface-name` command. For information about the `monitor traffic` command, see the Junos OS Administration Guide for Security Devices.
Chapter 12

Configuring 3G Wireless Modems for WAN Connections

3G refers to the third generation of mobile phone standards and technology based on the International Telecommunication Union (ITU) International Mobile Telecommunications-2000 (IMT-2000) global standard. 3G networks are wide area cellular telephone networks that have evolved to include high-data rate services of up to 3 Mbps. This increased bandwidth makes 3G networks a viable option as primary or backup wide area network (WAN) links for a branch office.

Juniper Networks supports 3G wireless modem cards that you can install into the ExpressCard slot in SRX210 devices. When used in a branch office, the SRX210 device can provide dial-out services to PC users and forward IP traffic through a service provider’s cellular network.

For information about which devices support the features documented in this chapter, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.

This chapter includes the following topics:

- 3G Wireless Modem Support on Different Device Types on page 356
- 3G Wireless Overview on page 356
- Understanding the 3G Wireless Modem Interface on page 359
- Understanding the Dialer Interface on page 360
- Understanding the GSM Profile on page 361
- 3G Wireless Modem Configuration Overview on page 362
- Configuring the 3G Wireless Modem Interface—Quick Configuration on page 363
- Configuring the Dialer Interface on page 365
- Configuring the 3G Wireless Modem Interface on page 367
- Configuring the GSM Profile on page 368
- Configuring PAP on the Dialer Interface on page 370
- Configuring CHAP on the Dialer Interface on page 371
- Configuring the Dialer Interface as a Backup WAN Connection on page 373
- Configuring Dialer Watch for the 3G Wireless Modem Interface on page 374
- Configuring Dialer Filter for the 3G Wireless Modem Interface on page 375
- Understanding Account Activation for CDMA EV-DO Cards on page 376
3G Wireless Modem Support on Different Device Types

The following table lists key 3G wireless modem features, specifies whether the features are supported on various device types, and indicates where you can find more information about each feature.

### Table 99: Support Information: 3G Wireless Modems

<table>
<thead>
<tr>
<th>Feature</th>
<th>J Series Devices</th>
<th>SRX210 Devices</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>3G Global System for Mobile Communications (GSM) High-SPEED Downlink Packet Access (HSDPA) wireless modem card</td>
<td>No</td>
<td>Yes</td>
<td>“3G Wireless Overview” on page 356</td>
</tr>
<tr>
<td>3G Code-Division Multiple Access (CDMA) Evolution-Data Optimized (EV-DO) wireless modem card</td>
<td>No</td>
<td>Yes</td>
<td>“3G Wireless Overview” on page 356</td>
</tr>
</tbody>
</table>

**3G Wireless Overview**

Figure 45 on page 357 illustrates a basic setup for 3G wireless connectivity for two branch offices. Branch Office A has a T1 leased line as the primary wide area network (WAN) link and a 3G wireless modem connection as the failover link. Branch Office B uses the 3G wireless modem connection as the primary WAN link.
**Supported Devices and 3G Wireless Modem Cards**

Juniper Networks supports 3G wireless modem cards that you can install into the ExpressCard slot in SRX210 devices. When used in a branch office, the SRX210 device can provide dial-out services to PC users as well as forward IP traffic onto the service provider’s cellular network.

Juniper Networks supports the following 3G wireless modem cards:

- Sierra Wireless AirCard Global System for Mobile Communications (GSM) High-Speed Downlink Packet Access (HSDPA) ExpressCard
- Sierra Wireless AirCard Code-Division Multiple Access (CDMA) 1xEvolution-Data Optimized (EV-DO) rev. A ExpressCard

GSM and CDMA are competing digital cellular phone technologies. GSM is used by AT&T, T-Mobile, and by cellular networks in countries other than the U.S., Japan, India, and Korea. CDMA is used by Sprint and Verizon.

**3G Terms**

Before configuring 3G wireless modems, become familiar with the terms defined in Table 100 on page 358.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access point name (APN)</td>
<td>Provides routing information for GPRS. The APN consists of two parts: the Network ID, which identifies the external service requested by a user of the GPRS service, and the Operator ID, which specifies routing information.</td>
</tr>
<tr>
<td>AT</td>
<td>A set of modem commands, preceded by AT, originally developed by Hayes, Inc. for their modems. The structure (but not the specific commands, which vary greatly from manufacturer to manufacturer) is a de facto industry standard for modems.</td>
</tr>
<tr>
<td>Base Transceiver Station (BTS)</td>
<td>Located at the cellular service provider network, BTS provides the radio or the Physical Layer connectivity between the mobile user and the mobile network.</td>
</tr>
<tr>
<td>Code-Division Multiple Access (CDMA)</td>
<td>Multiplexing protocols used in wireless communications. CDMA is used by Sprint and Verizon cellular networks.</td>
</tr>
<tr>
<td>Control and Status (CNS) message</td>
<td>These messages are used to:</td>
</tr>
<tr>
<td></td>
<td>■ Query 3G modem status</td>
</tr>
<tr>
<td></td>
<td>■ Set parameters and configuration of the 3G modem device</td>
</tr>
<tr>
<td></td>
<td>■ Control the traffic of event notifications from the 3G modem device</td>
</tr>
<tr>
<td></td>
<td>■ Receive event notification from modem device</td>
</tr>
<tr>
<td>Diagnostic Mode (DM)</td>
<td>Qualcomm Diagnostic Mode is the protocol specification and mechanism that is used to allow collection of debug logs from Sierra 3G wireless modem firmware.</td>
</tr>
<tr>
<td>dial backup</td>
<td>Feature that reestablishes network connectivity through one or more backup dialer interfaces after a primary interface fails. When the primary interface is reestablished, the backup is disconnected.</td>
</tr>
<tr>
<td>dialer interface</td>
<td>Logical interface for configuring properties for a 3G wireless modem connection.</td>
</tr>
<tr>
<td>dialer pool</td>
<td>One or more physical interfaces that are associated with a dialer profile.</td>
</tr>
<tr>
<td>dialer profile</td>
<td>Set of characteristics configured for the 3G wireless modem interface. Dialer profiles allow the configuration of physical interfaces to be separated from the logical configuration of dialer interfaces required for 3G wireless modem connectivity. This feature also allows physical and logical interfaces to be bound together dynamically on a per-connection basis.</td>
</tr>
<tr>
<td>Evolution Data Optimized (EV-DO)</td>
<td>Standard for transmitting data through radio signals.</td>
</tr>
<tr>
<td>Electronic Serial Number (ESN)</td>
<td>Number that is printed on the 3G wireless modem card itself. You can also use the show modem wireless interface firmware command to display this number.</td>
</tr>
<tr>
<td>Global System for Mobile Communications (GSM)</td>
<td>Standard used by AT&amp;T and T-Mobile cellular networks.</td>
</tr>
<tr>
<td>High Speed Downlink Packet Access (HSDPA)</td>
<td>3G mobile communications protocol.</td>
</tr>
<tr>
<td>Internet-based Over the Air (IOTA)</td>
<td>Activation method used by cellular network providers such as Sprint for CDMA EV-DO 3G wireless modem cards.</td>
</tr>
</tbody>
</table>
Table 100: 3G Terms (continued)

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over the Air Service Provisioning (OTASP)</td>
<td>Activation method used by cellular network providers such as Verizon for CDMA EV-DO 3G wireless modem cards.</td>
</tr>
<tr>
<td>Preferred Roaming List (PRL)</td>
<td>File that contains information for accessing the device’s home network, as well as the service provider’s roaming partners.</td>
</tr>
<tr>
<td>Subscriber Identity Module (SIM)</td>
<td>Detachable smart card on the GSM HSDPA 3G wireless modem.</td>
</tr>
</tbody>
</table>

Related Topics

- Understanding the 3G Wireless Modem Interface on page 359
- Understanding the Dialer Interface on page 360

Understanding the 3G Wireless Modem Interface

You configure two types of interfaces for 3G wireless modem connectivity—the physical interface and a logical dialer interface.

The physical interface for the 3G wireless modem uses the name cl-0/0/8. This interface is automatically created when a 3G wireless modem is installed in the device.

You configure the following for the physical interface:

- A dialer pool to which the physical interface belongs and the priority of the interface in the pool. A physical interface can belong to more than one dialer pool. The dialer pool priority has a range from 1 to 255, with 1 designating the lowest-priority interfaces and 255 designating the highest-priority interfaces.
- Modem initialization string (optional). These strings begin with AT and execute Hayes modem commands that specify modem operation.
- GSM profile for establishing a data call with a GSM cellular network. For more information, see “Understanding the GSM Profile” on page 361.

By default, the modem allows access to networks other than the home network.

Related Topics

- 3G Wireless Modem Configuration Overview on page 362
- Understanding the Dialer Interface on page 360
- Understanding the GSM Profile on page 361
Understanding the Dialer Interface

The dialer interface, `dln`, is a logical interface for configuring properties for modem connections. You can configure multiple dialer interfaces on an SRX Series device. A dialer interface and a dialer pool (which includes the physical interface) are bound together in a dialer profile.

The following rules apply when you configure dialer interfaces for 3G wireless modem connections:

- The dialer interface must be configured to use the default Point-to-Point Protocol (PPP) encapsulation. You cannot configure Cisco High-Level Data Link Control (HDLC) or Multilink PPP (MLPPP) encapsulation on dialer interfaces.
- You cannot configure the dialer interface as a constituent link in a multilink bundle.
- You cannot configure any dial-in options for the dialer interface.

You configure the following for a dialer interface:

- A dialer pool to which the physical interface belongs.
- Source IP address for the dialer interface.
- Dial string (optional) is the destination number to be dialed.
- Authentication, for GSM HSDPA 3G wireless modem cards.
- Watch list, if the dialer interface is a backup WAN link. See “Configuring Dialer Watch for the 3G Wireless Modem Interface” on page 374.

Authentication for GSM HSDPA 3G Wireless Modems

For GSM HSDPA 3G wireless modems, you configure a dialer interface to support authentication through Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).

CHAP is a server-driven, three-step authentication method that depends on a shared secret password that resides on both the server and the client. When you enable CHAP on a dialer interface, the device can authenticate its peer and be authenticated by its peer.

PAP allows a simple method for a peer to establish its identity using a two-way handshake during initial link establishment. After the link is established, an identification and password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated.

Backup, Dialer Filter, and Dialer Watch

The dialer interface can perform backup, dialer filter, and dialer watch functions, but these operations are mutually exclusive. You can configure a single dialer interface to operate in only one of the following ways:
As a backup interface for a single primary WAN connection. The dialer interfaces are activated only when the primary interface fails. The 3G wireless modem backup connectivity is supported on all interfaces except lsq-0/0/0.

As a dialer filter. Dialer filter enables the 3G wireless modem connection to be activated only when specific network traffic is sent on the backup WAN link. You configure a firewall rule with the dialer filter option, and then apply the dialer filter to the dialer interface.

As a dialer watch interface. With dialer watch, the SRX Series device monitors the status of a specified route and if the route disappears, the dialer interface initiates the 3G wireless modem connection as a backup connection. To configure dialer watch, you first add the routes to be monitored to a watch list in a dialer interface; specify a dialer pool for this configuration. Then configure the 3G wireless modem interface to use the dialer pool.

Operating Parameters

You can also specify optional operating parameters for the dialer interface:

- Activation delay—Number of seconds after the primary interface is down before the backup interface is activated. The default value is 0 seconds, and the maximum value is 60 seconds. Use this option only if dialer watch is configured.

- Deactivation delay—Number of seconds after the primary interface is up before the backup interface is deactivated. The default value is 0 seconds, and the maximum value is 60 seconds. Use this option only if dialer watch is configured.

- Idle timeout—Number of seconds the connection remains idle before disconnecting. The default value is 120 seconds, and the range is from 0 to 4294967295 seconds.

- Initial route check—Number of seconds before the primary interface is checked to see if it is up. The default value is 120 seconds, and the range is from 1 to 300 seconds.

Related Topics

- 3G Wireless Modem Configuration Overview on page 362
- Understanding the 3G Wireless Modem Interface on page 359

Understanding the GSM Profile

To allow data calls to a GSM network, you must obtain the following information from your service provider:

- Username and password
- Access point name (APN)
- Whether the authentication is CHAP or PAP
You configure this information in a GSM profile associated with the 3G wireless modem physical interface. You can configure up to 16 different GSM profiles, although only one profile can be active at a time.

**NOTE:** You also need to configure a CHAP or PAP profile with the specified username and password for the dialer interface.

Subscriber information is written to the Subscriber Identity Module (SIM) on the GSM HSDPA 3G wireless modem card. If the SIM is locked, you must unlock it before activation by using the master subsidy lock (MSL) value given by the service provider when you purchase the cellular network service. See “Unlocking the GSM 3G Wireless Modem” on page 381.

Some service providers may preload subscriber profile information on a SIM card. The assigned subscriber information is stored in profile 1, while profile 0 is a default profile created during manufacturing. If this is the case, specify profile 1 for the GSM profile associated with the 3G wireless modem physical interface.

**Related Topics**

- 3G Wireless Modem Configuration Overview on page 362

**3G Wireless Modem Configuration Overview**

### Before You Begin

1. Install your SRX Series device and establish basic connectivity for your device. For more information, see the Hardware Guide for your device.
2. Obtain a supported 3G wireless modem card for the device.
3. Establish an account with a cellular network service provider. Contact your service provider for more information.
4. With the services router powered off, insert the 3G wireless modem card into the ExpressCard slot. Power on the device. The PIM LED on the front panel of the device indicates the status of the 3G wireless modem interface.

**WARNING:** The device must be powered off before you insert the 3G wireless modem card in the ExpressCard slot. You cannot insert or remove the card when the device is powered on.

5. For background information, read the following:
   - 3G Wireless Overview on page 356
   - Understanding the 3G Wireless Modem Interface on page 359
   - Understanding the Dialer Interface on page 360
   - Understanding the GSM Profile on page 361

To configure and activate the 3G wireless modem card, perform the following tasks:
1. Configure a dialer interface.
2. Configure the 3G wireless modem interface.
3. Configure security zones and policies, as needed, to allow traffic through the WAN link.

**Related Topics**

- Configuring the Dialer Interface on page 365
- Configuring the 3G Wireless Modem Interface—Quick Configuration on page 363
- Configuring the 3G Wireless Modem Interface on page 367
- Configuring the GSM Profile on page 368

**Configuring the 3G Wireless Modem Interface—Quick Configuration**

The physical interface for the 3G wireless modem, cl-0/0/8, is automatically created when a 3G wireless modem is installed in the device. You can use J-Web Quick Configuration to configure the 3G wireless interface and activate a CDMA EV-DO 3G wireless modem card.

NOTE: The J-Web Quick Configuration does not support configuration of a GSM profile. Use the CLI configuration editor or the J-Web Edit Configuration page to configure a GSM profile.

**Before You Begin**

For background information, read “3G Wireless Modem Configuration Overview” on page 362.

To configure the 3G wireless interface with Quick Configuration:

1. In the J-Web user interface, select **Configure > Interfaces**.
   A list of network interfaces installed on the device is displayed.
2. Click the cl-0/0/0 interface name.
   The 3G Interface Configuration is displayed.
3. Enter information into the 3G Interface Configuration, as described in Table 101 on page 364.
4. To apply the configuration and return to the Quick Configuration Interfaces page, click **OK**. (To cancel your entries and return to the Quick Configuration Interfaces page, click **Cancel**.)
5. From the Interfaces Quick Configuration page, click **Apply** to apply the configuration.
# Table 101: 3G Wireless Interface Quick Configuration Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuring 3G Wireless Interfaces</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Adds supplemental information about the 3G wireless physical interface on the device.</td>
<td>Type a text description of the physical 3G wireless interface in the box to clearly identify the interface when viewing displays.</td>
</tr>
<tr>
<td>Modern Options: Init String</td>
<td>(Optional) Specifies modem operation.</td>
<td>Type a string that begins with AT and includes Hayes modem commands.</td>
</tr>
<tr>
<td><strong>Dialer Pool Options</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dialer Pools</td>
<td>Displays the list of configured dialer pools on the device.</td>
<td>To add a dialer pool to the interface, click Add.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To edit a dialer pool, select the name from the list. You can change the priority, but not the name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To delete a dialer pool, select the check box and click Delete.</td>
</tr>
<tr>
<td>Dialer Pool Name (required)</td>
<td>Specifies the group of physical interfaces to be used by the dialer interface.</td>
<td>Type the dialer pool name—for example, 1.</td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies the priority of this interface within the dialer pool. Interfaces with a higher priority are the first to interact with the dialer interface.</td>
<td>1. Type a priority value from 0 (lowest) to 255 (highest). The default is 0. 2. Click OK to return to the Quick Configuration Interfaces page.</td>
</tr>
<tr>
<td><strong>Card Activation Options</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card Activation</td>
<td>Enables the CDMA wireless modem card to connect to the service provider's cellular network.</td>
<td>1. Select the type of card activation:  ■ IOTA—Internet-based over the air provisioning.  ■ Manual Activation—Requires manual entry of the required information.  ■ OTASP—Over the air service provisioning. 2. Click Activate 3. If you selected Manual Activation or OTASP, you are prompted to enter information required for card activation. (No additional information is needed for IOTA card activation.) 4. Click OK.</td>
</tr>
<tr>
<td><strong>OTASP Activation Parameters</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dial String</td>
<td>Number that the modem uses to contact the service provider's network.</td>
<td>Enter the dial number supplied by the service provider.</td>
</tr>
<tr>
<td><strong>Manual Activation Parameters</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>International Mobile Station Identity</td>
<td>Mobile subscriber information</td>
<td>Enter the number supplied by the service provider.</td>
</tr>
</tbody>
</table>
Table 101: 3G Wireless Interface Quick Configuration Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Directory Number</td>
<td>10-digit user phone number</td>
<td>Enter the number supplied by the service provider.</td>
</tr>
<tr>
<td>Master Subsidy Lock</td>
<td>Activation code</td>
<td>Enter the code supplied by the service provider.</td>
</tr>
<tr>
<td>Network identification</td>
<td>Number between 0 and 65535</td>
<td>Enter the NID number displayed with the CLI show modem wireless interface cl-0/0/8 network command.</td>
</tr>
<tr>
<td>System identification</td>
<td>Number between 0 and 32767</td>
<td>Enter the SID number displayed with the CLI show modem wireless interface cl-0/0/8 network command.</td>
</tr>
<tr>
<td>Simple IP password</td>
<td>User name</td>
<td>Enter the user name supplied by the service provider.</td>
</tr>
<tr>
<td>Simple IP user ID</td>
<td>Password</td>
<td>Enter the password supplied by the service provider.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring the GSM Profile on page 368

Configuring the Dialer Interface

Before You Begin

For background information, read “Understanding the Dialer Interface” on page 360.

In this example, you configure the dialer interface dl0, specifying PPP encapsulation, dialer pool 1, dial string 14691, and the negotiate address option for the interface IP address.

You can use either J-Web or the CLI configuration editor to configure the dialer interface.

This topic covers:

- J-Web Configuration on page 365
- CLI Configuration on page 366
- Related Topics on page 366

J-Web Configuration

To configure a dialer interface:
1. Select **Configure > CLI Tools > Point and Click CLI**.
2. Next to Interfaces, click **Configure** or **Edit**.
3. Next to Interface, click **Add new entry**.
4. In the Interface name box, type `dl0`.
5. In the Description box, type `3g-wireless`.
6. Click **OK**.
7. Under Interface, click the Interface name **dl0**.
8. From the Encapsulation list, select **ppp**.
9. Next to Unit, click **Add new entry**.
10. In the Interface unit number box, type `0`.

**NOTE:** You can only specify `0` for the unit.

11. Next to Dialer options, select **Yes** and then click **Configure**.
12. In the Pool box, type `1`.
13. Next to Dial string, click **Add new entry**.
15. Click **OK** until you return to the Unit page.
16. Select **Inet** under Family, and click **Configure**.
17. Select **Yes** for Negotiate address.
18. Click **OK**.

### CLI Configuration

To configure a dialer interface:

```
user@host# set interfaces dl0 description 3g-wireless encapsulation ppp unit 0
dialer-options pool 1 dial-string 14691
user@host# set interfaces dl0 unit 0 family inet negotiate-address
```

### Related Topics

- Configuring the 3G Wireless Modem Interface—Quick Configuration on page 363
- Configuring the 3G Wireless Modem Interface on page 367
Configuring the 3G Wireless Modem Interface

Before You Begin

Configure a dialer interface, as described in “Configuring the Dialer Interface” on page 365.

In this example, you configure the physical interface for the 3G wireless modem to use the dialer pool 1 (previously configured for the dialer interface) and a priority for the dialer pool of 25. You also configure a modem initialization string to set the modem to autoanswer after two rings.

You can use either J-Web or the CLI configuration editor to configure the 3G wireless modem interface.

This topic covers:

- J-Web Configuration on page 367
- CLI Configuration on page 367
- Related Topics on page 368

J-Web Configuration

To configure the dialer pool for the 3G wireless modem interface:

1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Interfaces, click Configure or Edit.
3. In the Interface name column, click the cl-0/0/8 interface name.
4. Next to Dialer options, select Yes and then click Configure.
5. Next to Pool, click Add new entry.
6. In the Pool identifier box, type 1.
7. In the Priority box, type 25.
8. Click OK until you return to the Interface page.

To configure modem options for the 3G wireless modem interface:

1. On the Interface page, next to Modem options, click Configure.
2. In the Init command string box, type ATSO=2\n to configure the modem to autoanswer after two rings.
3. Click OK.

CLI Configuration

To configure the dialer pool for the 3G wireless modem interface:
user@host# set interfaces cl-0/0/8 dialer-options pool 1 priority 25

To configure modem options for the 3G wireless modem interface:

user@host# set interfaces cl-0/0/8 modem-options init-command-string “ATSO=2\n”

**Related Topics**

- (Optional) “Configuring CHAP on the Dialer Interface” on page 371
- (Optional) “Configuring PAP on the Dialer Interface” on page 370
- (Optional) “Configuring the Dialer Interface as a Backup WAN Connection” on page 373
- (Optional) “Configuring Dialer Watch for the 3G Wireless Modem Interface” on page 374
- (Optional) “Configuring Dialer Filter for the 3G Wireless Modem Interface” on page 375
- (Optional) “Configuring the GSM Profile” on page 368

**Configuring the GSM Profile**

This topic describes the configuration of the GSM profile for use with service provider networks such as AT&T and T-Mobile.

**Before You Begin**

For background information, read “Understanding the GSM Profile” on page 361 and “Configuring the 3G Wireless Modem Interface” on page 367.

In this example, the following information provided by the service provider is configured in a GSM profile `jnpr` that is associated with the 3G wireless modem physical interface `cl-0/0/8`:

- Username—juniper99
- Password—1@#6ahgf
- Access point name (APN)—apn.service.com
- Authentication method—CHAP

You also need to configure a CHAP profile with the specified username and password for the dialer interface. See “Configuring CHAP on the Dialer Interface” on page 371.

You can use either J-Web or the CLI configuration editor to configure the information required to activate the GSM 3G wireless modem card.
J-Web Configuration

To configure a GSM profile for the 3G wireless modem interface:
1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Interfaces, click Configure or Edit.
3. For cl-0/0/8, click Edit.
4. Next to Cellular options, click Yes and then click Configure.
5. Next to GSM options, click Yes and then click Configure.
6. Next to Profiles, click Add new entry.
7. In the Profile name box, type jnpr.
8. In the Access point name box, type apn.service.com.
9. In the Authentication method list, select chap.
10. In the Sip user id box, type juniper99.
11. In the Sip password box, type 1@#6ahgfh.
12. Click OK to return to the GSM options page.

To designate the GSM profile you just configured as the active profile:
1. On the GSM options page, in Select profile, select jnpr.
2. Click OK to return to the Cellular options page.
3. Click OK.

CLI Configuration

To configure a GSM profile for the 3G wireless modem interface:

```
user@host> request modem wireless gsm create-profile profile-id 1 sip-user-id juniper99 sip-password 16ahgfh access-point-name apn.service.com authentication-method chap
```

To designate the GSM profile you just configured as the active profile:

```
user@host# set interface cl-0/0/8 cellular-options gsm-options select-profile profile-id 1
```
Configuring PAP on the Dialer Interface

With GSM HSDPA 3G wireless modem cards, you may need to configure either Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) for authentication with the service provider network. The service provider must supply the username and password, which you configure in an access profile. You then specify this access profile in a dialer interface.

**Before You Begin**

Configure a dialer interface. See “Configuring the Dialer Interface” on page 365.

In this example, you configure the username and password in the PAP access profile `pap-1`, then associate the `pap-1` profile with the dialer interface `dl0`.

You can use either J-Web or the CLI configuration editor to configure the PAP access profile.

This topic covers:

- J-Web Configuration on page 370
- CLI Configuration on page 371
- Related Topics on page 371

**J-Web Configuration**

To configure a PAP access profile:

1. Select **Configure > CLI Tools > Point and Click CLI**.
2. Next to Access, click **Configure** or **Edit**.
3. Next to Profile, click **Add new entry**.
4. In the Profile name box, type `pap-1`.
5. Next to Client, click **Add new entry**.
6. In the Name box, type `clientX`.
7. In the Pap password box, type `\&7a^6b%5c`.
8. Click **OK** until you return to the main Configuration page.

To associate the PAP access profile with a dialer interface:
1. Select **Configure > CLI Tools > Point and Click CLI**.
2. Next to Interfaces, click **Configure** or **Edit**.
3. In the Interface name box, click **dl0**.
4. In the Interface unit number box, click **0**.
5. Next to Ppp options, click **Configure**.
6. Next to Pap, click **Configure**.
7. In the Access profile box, type **pap-1**.
8. Click **OK** until you return to the main Configuration page.

**CLI Configuration**

To configure a PAP access profile:

```bash
user@host# set access profile pap-1 client clientX pap-password &7a^6b%5c
```

To associate the PAP access profile with a dialer interface:

```bash
user@host# set interfaces dl0 unit 0 ppp-options pap access-profile pap-1
```

**Related Topics**

- Configuring CHAP on the Dialer Interface on page 371

**Configuring CHAP on the Dialer Interface**

With GSM HSDPA 3G wireless modem cards, you may need to configure either Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) for authentication with the service provider network. The service provider must supply the username and password, which you configure in an access profile. You then specify this access profile in a dialer interface.

**Before You Begin**

Configure a dialer interface. See “Configuring the Dialer Interface” on page 365.

In this example, you configure the username and password in the CHAP access profile **chap-1**, then associate the **chap-1** profile with the dialer interface **dl0**.

You can use either J-Web or the CLI configuration editor to configure the CHAP access profile.
This topic covers:
- J-Web Configuration on page 372
- CLI Configuration on page 372
- Related Topics on page 373

**J-Web Configuration**

To configure a CHAP access profile:
1. Select **Configure > CLI Tools > Point and Click CLI**.
2. Next to Access, click **Configure** or **Edit**.
3. Next to Profile, click **Add new entry**.
4. In the Profile name box, type **chap-1**.
5. Next to Client, click **Add new entry**.
6. In the Name box, type **clientX**.
7. In the Chap secret box, type `\&7a^6b%5c`.
8. Click **OK** until you return to the main Configuration page.

To associate the CHAP access profile with a dialer interface:
1. Select **Configure > CLI Tools > Point and Click CLI**.
2. Next to Interfaces, click **Configure** or **Edit**.
3. In the Interface name box, click **dl0**.
4. In the Interface unit number box, click **0**.
5. Next to Ppp options, click **Configure**.
6. Next to Chap, click **Configure**.
7. In the Access profile box, type **chap-1**.
8. Click **OK** until you return to the main Configuration page.

**CLI Configuration**

To configure a CHAP access profile:

```
user@host# set access profile chap-1 client clientX chap-secret &7a^6b%5c
```

To associate the CHAP access profile with a dialer interface:

```
user@host# set interfaces dl0 unit 0 ppp-options chap access-profile chap-1
```
Before You Begin

1. For background information, read “Understanding the Dialer Interface” on page 360.
2. Configure a dialer interface. See “Configuring the Dialer Interface” on page 365.

In this example, you configure the dialer interface dl0 as the backup WAN link for the ge-0/0/1.0 interface.

You can use either J-Web or the CLI configuration editor to configure the backup interface.

This topic covers:

- J-Web Configuration on page 373
- CLI Configuration on page 373
- Related Topics on page 374

J-Web Configuration

To configure a dialer interface as a backup to a primary interface:

1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Interfaces, click Configure or Edit.
3. In the Interface name column, click ge-0/0/1.
4. Under Unit, click the Interface unit number 0.
5. Next to Backup options, click Configure.
6. In the Interface box, type dl0.
7. Click OK until you return to the Interfaces page.

CLI Configuration

To configure a dialer interface as a backup to a primary interface:

```
user@host# set interfaces ge-0/0/1.0 unit 0 backup-options interface dl0
```
Related Topics

- Configuring Dialer Watch for the 3G Wireless Modem Interface on page 374
- Configuring Dialer Filter for the 3G Wireless Modem Interface on page 375

Configuring Dialer Watch for the 3G Wireless Modem Interface

Before You Begin

1. For background information, read “Understanding the Dialer Interface” on page 360.
2. Configure a dialer interface. See “Configuring the Dialer Interface” on page 365.

In this example, you configure dialer watch to enable the device to monitor the route to the head office router at 200.200.201.1/32.

You can use either J-Web or the CLI configuration editor to configure dialer watch.

This topic covers:

- J-Web Configuration on page 374
- CLI Configuration on page 374
- Related Topics on page 375

J-Web Configuration

To create a dialer watch list:

1. Select **Configure > CLI Tools > Point and Click CLI**.
2. Next to Interfaces, click **Configure** or **Edit**.
3. Next to Interface name, select **dl0**.
4. Under Unit, click the Interface unit number **0**.
5. Next to Dialer options, click **Yes**. Click **Configure**.
6. In the Pool box, type **dw-pool**.
7. Next to Watch list, click **Add new entry**.
8. In the Prefix box, type **200.200.201.1/32**.
9. Click **OK**.

CLI Configuration

To create a dialer watch list:
user@host# set interfaces dl0 description dialer-watch unit 0 dialer-options watch-list 200.200.201.1/32
user@host# set interfaces dl0 description dialer-watch unit 0 dialer-options pool dw-pool

**Related Topics**

- Configuring Dialer Filter for the 3G Wireless Modem Interface on page 375
- Configuring the Dialer Interface as a Backup WAN Connection on page 373

**Configuring Dialer Filter for the 3G Wireless Modem Interface**

**Before You Begin**

1. For background information, read “Understanding the Dialer Interface” on page 360.
2. Configure a dialer interface. See “Configuring the Dialer Interface” on page 365.

In this example, you configure a dialer filter firewall rule for traffic from the branch office to the main office router. In this example, the branch office router has the IP address 20.20.90.4/32 and the main office router has the IP address 200.200.201.1/32.

You can use either J-Web or the CLI configuration editor to configure dialer filter.

This topic covers:

- J-Web Configuration on page 375
- CLI Configuration on page 376
- Related Topics on page 376

**J-Web Configuration**

To create a dialer filter:

1. Select **Configure > CLI Tools > Point and Click CLI**.
2. Next to Firewall, click **Configure** or **Edit**.
3. Next to Inet, click **Configure**.
4. Next to Dialer filter, click **Add new entry**.
5. In the Filter name box, type corporate-traffic-only.
6. Next to Term, click **Add new entry**.
7. In the Rule name box, type term1.
8. Next to From, click **Configure**.
9. Next to Address, click **Add new entry**.
10. In the Address box, type 20.20.90.4/32.
11. Click OK.
12. Next to Destination address, click Add new entry.
13. In the Address box, type 200.200.201.1/32.
14. Click OK.
15. Click OK to return to the Firewall page.
16. Next to Then, click Configure.
17. From the Designation list, select Note.
18. Click OK.

To associate the dialer filter with a dialer interface:
1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Interfaces, click Configure or Edit.
3. In the Interface name column, click dl0.
4. Under Unit, click the Interface unit number 0.
5. In the Family section, next to Inet, click Edit.
6. Next to Filter, click Configure.
7. In the Dialer box, type corporate-traffic-only, the dialer filter configured previously.
8. Click OK.

**CLI Configuration**

To create a dialer filter:

```bash
user@host# set firewall family inet dialer-filter corporate-traffic-only term term1 from source-address 20.20.90.4/32 destination-address 200.200.201.1/32 then note
```

To associate the dialer filter with a dialer interface:

```bash
user@host# set interfaces dl0 unit 0 family inet filter dialer corporate-traffic-only
```

**Related Topics**

- Configuring Dialer Watch for the 3G Wireless Modem Interface on page 374
- Configuring the Dialer Interface as a Backup WAN Connection on page 373

**Understanding Account Activation for CDMA EV-DO Cards**

Account activation is the process of enabling the CDMA EV-DO wireless modem card to connect to your service provider's cellular network. This is a one-time process where your subscriber information is saved in nonvolatile memory on the card. The
procedure you use to perform account activation depends upon the service provider network.

Before activating an account, you can verify the signal strength on the 3G wireless modem interface by using the `show modem wireless interface cl-0/0/8 rssi` command. The signal strength should be at least -90 dB and preferably better than -80 dB (-125 dB indicates nil signal strength). If the signal strength is below -90 dB, activation may not be possible from that location. For example:

```
user@host> show modem wireless interface cl-0/0/8 rssi
Current Radio Signal Strength (RSSI) = -98 dBm
```

The service provider requires the electronic serial number (ESN) of the 3G wireless modem card to activate your account and to generate the necessary information you need to activate the card. You can obtain the ESN number of the modem card in the following ways:

- Inspect the modem card itself; the ESN is printed on the card.
- Use the CLI `show modem wireless interface cl-0/0/8 firmware` command, as shown in the following example, and note the value for the Electronic Serial Number (ESN) field:

```
user@host> show modem wireless interface cl-0/0/8 firmware
Modem Firmware Version : p2005600
Modem Firmware built date : 12-09-07
Card type : Aircard 597E - CDMA EV-DO revA
Manufacturer : Sierra Wireless, Inc.
Hardware Version : 1.0
Electronic Serial Number (ESN) : 0x6032688F
Preferred Roaming List (PRL) Version : 20224
Supported Mode : 1xev-do rev-a, 1x
Current Modem Temperature : 32 degrees Celsius
Modem Activated : YES
Activation Date: 2-06-08
Modem PIN Security : Unlocked
Power-up lock : Disabled
```

For the CDMA EV-DO 3G wireless modem card, account activation can be done through one or more of the following modes:

- Over the air service provisioning (OTASP)—protocol for programming phones over the air using Interim Standard 95 (IS-95) Data Burst Messages.

To activate the 3G wireless modem card with OTASP, you need to obtain from the service provider the dial number that the modem will use to contact the network. Typically, OTASP dial numbers begin with the feature code *228 to
indicate an activation call type to the cellular network’s base transceiver station, followed by additional digits specified by the service provider.

- Internet-based over the air (IOTA) provisioning—method for programming phones for voice and data services
- Manually providing the required information by entering in a CLI operational mode command

Sprint uses manual and IOTA activation, whereas Verizon uses only OTASP.

---

**NOTE:** The 3G wireless modem is set into Single-Carrier Radio Transmission Technology (1xRTT) mode automatically when it is activated for Verizon networks.

### Related Topics

- Activating the CDMA EV-DO Modem Card with OTASP Provisioning on page 378
- Activating the CDMA EV-DO Modem Card Manually on page 379
- Activating the CDMA EV-DO Modem Card with IOTA Provisioning on page 380

### Activating the CDMA EV-DO Modem Card with OTASP Provisioning

This topic describes the activation of the CDMA EV-DO 3G wireless modem card for use with service provider networks such as Verizon.

#### Before You Begin

Before you can activate the 3G wireless modem card, you need to obtain from the service provider the dial number that the modem will use to contact the network.

The service provider must activate your account before OTASP provisioning can proceed.

Use the CLI operational mode command to activate the 3G wireless modem card.

In this example, the dial number from the service provider is **22864**.

#### CLI Operational Mode Command

To activate the CDMA EV-DO 3G wireless modem card with OTASP provisioning:

```bash
user@host> request modem wireless interface cl-0/0/8 activate otasp dial-string
*22864
OTASP number *22286*, Selecting NAM 0
Beginning OTASP Activation. It can take up to 5 minutes
Please check the trace logs for details.
```

To check the trace log for account activation details:
Activating the CDMA EV-DO Modem Card Manually

Manual activation stores the supplied values into the 3G wireless modem card's nonvolatile memory. This topic describes the activation of the CDMA EV-DO 3G wireless modem card for use with service provider networks such as Sprint.

**Before You Begin**

The service provider must activate your account before you can activate the CDMA EV-DO 3G wireless modem card.

Using the electronic serial number (ESN) you provided and your account information, the service provider supplies you with the following information for manual activation of the 3G wireless modem card:

- Master subsidy lock (MSL)—activation code
- Mobile directory number (MDN)—10-digit user phone number
- International mobile station identify (IMSI)—Mobile subscriber information
- Simple IP user identification (SIP-ID)—Username
- Simple IP password (SIP-Password)—Password

You also need to obtain the following information from the 3G wireless modem card itself for the activation:

- System identification (SID)—Number between 0 and 32767
- Network identification (NID)—Number between 0 and 65535

Use the CLI `show modem wireless interface cl-0/0/8 network` command to display the SID and NID, as shown in the following example:

user@host> show modem wireless interface cl-0/0/8 network
Running Operating mode : 1xEV-DO (Rev A) and 1xRTT
Call Setup Mode : Mobile IP only
System Identifier (SID) : 3421
Network Identifier (NID) : 91
Roaming Status(1xRTT) : Home
Idle Digital Mode : HDR

Use the CLI `operational mode` command to manually activate the 3G wireless modem card.
This example uses the following values for manual activation:

- MSL (from service provider) — 43210
- MDN (from service provider) — 0123456789
- IMSI (from service provider) — 0123456789
- SIP-ID (from service provider) — jnpr
- SIP-Password (from service provider) — jn9rl
- SID (from modem card) — 12345
- NID (from modem card) — 12345

**CLI Operational Mode Command**

To activate the CDMA EV-DO 3G wireless modem card manually:

```
user@host> request modem wireless interface cl-0/0/8 activate manual msl 43210 mdn 0123456789 imsi 0123456789 sid 12345 nid 12345 sip-id jnpr sip-password jn9rl
```

Checking status...
Modem current activation status: Not Activated
Starting activation...
Performing account activation step 1/6 : [Unlock] Done
Performing account activation step 2/6 : [Set MDN] Done
Performing account activation step 3/6 : [Set SIP Info] Done
Performing account activation step 4/6 : [Set IMSI] Done
Performing account activation step 5/6 : [Set SID/NID] Done
Performing account activation step 6/6 : [Commit/Lock] Done
Configuration Commit Result: PASS
Resetting the modem ... Done
Account activation in progress. It can take up to 5 minutes
Please check the trace logs for details.

To check the trace log for account activation details:

```
user@host> tail -f /var/log/wwand.log
```

```
Jun 25 04:42:55: IOTA cl-0/0/8 Event: IOTA Start... Success
Jun 25 04:43:45: IOTA cl-0/0/8 OTA SPL unlock... Success
Jun 25 04:43:56: IOTA cl-0/0/8 Committing OTA Parameters to NVRAM... Success
Jun 25 04:44:02: IOTA cl-0/0/8 Over the air provisioning... Complete
Jun 25 04:44:04: IOTA cl-0/0/8 IOTA Event: IOTA End... Success
```

**Related Topics**

- Activating the CDMA EV-DO Modem Card with IOTA Provisioning on page 380

**Activating the CDMA EV-DO Modem Card with IOTA Provisioning**

Manual activation stores the supplied values in the 3G wireless modem card's nonvolatile memory. If the modem card is reset or you need to update Mobile IP
(MIP) parameters, use the CLI operational mode command to activate the modem card with IOTA.

### Before You Begin

Activate the CDMA EV-DO 3G wireless modem card. For information, see "Activating the CDMA EV-DO Modem Card Manually" on page 379.

### CLI Operational Mode Command

To activate the CDMA EV-DO 3G wireless modem card with IOTA:

```bash
user@host> request modem wireless interface cl-0/0/8 activate iota
Beginning IOTA Activation. It can take up to 5 minutes
Please check the trace logs for details.
```

To check the trace log for account activation details:

```bash
user@host> tail -f /var/log/wwand.log
Jun 25 04:42:55: IOTA cl-0/0/8 Event: IOTA Start... Success
Jun 25 04:43:45: IOTA cl-0/0/8 OTA SPL unlock... Success
Jun 25 04:43:56: IOTA cl-0/0/8 Committing OTA Parameters to NVRAM... Success
Jun 25 04:44:02: IOTA cl-0/0/8 Over the air provisioning... Complete
Jun 25 04:44:04: IOTA cl-0/0/8 IOTA Event: IOTA End... Success
```

### Unlocking the GSM 3G Wireless Modem

The subscriber identity module (SIM) in the GSM 3G wireless modem card is a detachable smart card. Swapping out the SIM allows you to change the service provider network, however some service providers lock the SIM to prevent unauthorized access to the service provider’s network. If this is the case, you will need to unlock the SIM by using an personal identification number (PIN), a four-digit number provided by the service provider.

### Before You Begin

Obtain the PIN from the service provider.

Use the CLI operational mode command to unlock the SIM on the GSM 3G wireless modem card.

This example uses the PIN 3210 from the service provider.

To unlock the SIM on the GSM 3G wireless modem card:

```bash
user@host> request modem wireless gsm sim-unlock cl-0/0/8 pin 3210
```

A SIM is blocked after three consecutive failed unlock attempts; this is a security feature to prevent brute force attempts to unlock the SIM. When the SIM is blocked,
you need to unblock the SIM with an eight-digit PIN unlocking key (PUK) obtained from the service provider.

Use the CLI operational mode command to unblock the SIM.

This example uses the PUK 76543210 from the service provider.

To unblock the SIM:

```
user@host> request modem wireless gsm sim-unblock cl-0/0/8 puk 76543210
```

**NOTE:** If you enter the PUK incorrectly ten times, you will need to return the SIM to the service provider for reactivation.
Chapter 13

Configuring USB Modems for Dial Backup

You can configure your device to “fail over” to a USB modem connection when the primary Internet connection experiences interruption.

**NOTE:** Low-latency traffic such as VoIP traffic is not supported over USB modem connections.

**NOTE:** We recommend using a US Robotics USB 56k V.92 Modem, model number USR Model 5637.

You use either the J-Web configuration editor or CLI configuration editor to configure the USB modem for dial backup.

For information about which devices support the features documented in this chapter, see the *Junos OS Feature Support Reference for SRX Series and J Series Devices*.

This chapter includes the following topics:

- USB Modem Terms on page 383
- USB Modem Interface Overview on page 384
- Before You Begin on page 385
- Connecting the USB Modem to the Device's USB Port on page 385
- Configuring USB Modems for Dial Backup with a Configuration Editor on page 386

**USB Modem Terms**

Before configuring USB modems and their supporting dialer interfaces, become familiar with the terms defined in Table 102 on page 384.
Table 102: USB Modem Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>caller ID</td>
<td>Telephone number of the caller on the remote end of a backup USB modem connection, used to dial in and also to identify the caller. Multiple caller IDs can be configured on a dialer interface. During dial-in, the device matches the incoming call's caller ID against the caller IDs configured on its dialer interfaces. Each dialer interface accepts calls from only callers whose caller IDs are configured on it.</td>
</tr>
<tr>
<td>dial backup</td>
<td>Feature that reestablishes network connectivity through one or more backup dialer interfaces after a primary interface fails. When the primary interface is reestablished, the USB modem backup is disconnected.</td>
</tr>
<tr>
<td>dialer interface</td>
<td>Logical interface for configuring dialing properties and the control interface for a backup USB modem connection.</td>
</tr>
<tr>
<td>dialer profile</td>
<td>Set of characteristics configured for the USB modem dialer interface. Dialer profiles allow the configuration of physical interfaces to be separated from the logical configuration of dialer interfaces required for USB modem connectivity. This feature also allows physical and logical interfaces to be bound together dynamically on a per-connection basis.</td>
</tr>
<tr>
<td>dial-in</td>
<td>Feature that enables devices to receive calls from the remote end of a backup USB modem connection. The remote end of the USB modem call might be a service provider, a corporate central location, or a customer premises equipment (CPE) branch office. All incoming calls can be verified against caller IDs configured on the device’s dialer interface.</td>
</tr>
</tbody>
</table>

USB Modem Interface Overview

You configure two types of interfaces for USB modem connectivity: a physical interface and a logical interface called the dialer interface:

- The USB modem physical interface uses the naming convention umd0. The device creates this interface when a USB modem is connected to the USB port.
- The dialer interface, dln, is a logical interface for configuring dialing properties for USB modem connections. The dialer interface can be configured using Point-to-Point Protocol (PPP) encapsulation. You can also configure the dialer interface to support authentication protocols—PPP Challenge Handshake (CHAP) or Password Authentication Protocol (PAP).

For information about interface names, see “Interface Naming Conventions” on page 9.

The USB modem provides a dial-in remote management interface, and supports dialer interface features by sharing the same dial pool as a dialer interface. The dial pool allows the logical dialer interface and the physical interface to be bound together dynamically on a per-call basis. You can configure the USB modem to operate either as a dial-in console for management or as a dial-in WAN backup interface.

The following rules apply when you configure dialer interfaces for USB modem connections:
The dialer interface must be configured to use PPP encapsulation. You cannot configure Cisco High-Level Data Link Control (HDLC) or Multilink PPP (MLPPP) encapsulation on dialer interfaces.

The dialer interface cannot be configured as a constituent link in a multilink bundle. For information about configuring multilink bundles, see “Configuring Link Services Interfaces” on page 399.

The dialer interface can perform backup, dialer filter, and dialer watch functions, but these operations are mutually exclusive. You can configure a single dialer interface to operate in only one of the following ways:
- As a backup interface—for one primary interface
- As a dialer filter
- As a dialer watch interface

Before You Begin

Before you configure USB modems, you need to perform the following tasks:
- Install device hardware. For more information, see the Getting Started Guide for your device.
- Establish basic connectivity. For more information, see the Getting Started Guide for your device.
- Order a US Robotics USB 56k V.92 Modem, model number USR Model 5637 from US Robotics (http://www.usr.com/).
- Order a public switched telephone network (PSTN) line from your telecommunications service provider. Contact your service provider for more information.
- If you do not already have a basic understanding of physical and logical interfaces and Juniper Networks interface conventions, read “Interfaces Overview” on page 3.

Connecting the USB Modem to the Device’s USB Port

NOTE: J Series devices have two USB ports. However, you can connect only one USB modem to the USB ports on these devices. If you connect USB modems to both ports, the device detects only the first modem connected.

NOTE: When you connect the USB modem to the USB port on the device, the USB modem is initialized with the modem initialization string configured for the USB modem interface on the device.

To connect the USB modem to the USB port on the device:
1. Plug the modem into the USB port.
2. Connect the modem to your telephone network.

## Configuring USB Modems for Dial Backup with a Configuration Editor

To configure USB modem interfaces, perform the following tasks.

- Configuring a USB Modem Interface for Dial Backup on page 386
- Configuring a Dialer Interface for USB Modem Dial Backup on page 387
- Configuring Dial-In for a USB Modem Connection on page 394
- Configuring PAP on Dialer Interfaces (Optional) on page 396
- Configuring CHAP on Dialer Interfaces (Optional) on page 397

### Configuring a USB Modem Interface for Dial Backup

To configure a USB modem interface for the device:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 103 on page 386.
3. Go on to “Configuring a Dialer Interface for USB Modem Dial Backup” on page 387.

### Table 103: Configuring a USB Modem Interface for Dial Backup

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Interfaces</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit interfaces umd0</td>
</tr>
<tr>
<td>level in the</td>
<td>2. Next to Interfaces, click Configure or Edit.</td>
<td></td>
</tr>
<tr>
<td>configuration hierarchy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create the new interface umd0</td>
<td>1. Next to Interface, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. In the Interface name box, type the name of the new interface, umd0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Click OK.</td>
<td></td>
</tr>
</tbody>
</table>
Table 103: Configuring a USB Modem Interface for Dial Backup (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure dialer options.</td>
<td>1. In the Encapsulation column, next to the new interface, click <strong>Edit</strong>.</td>
<td>Enter set dialer-options pool usb-modem-dialer-pool priority 25</td>
</tr>
<tr>
<td></td>
<td>2. Next to Dialer options, select <strong>Yes</strong>, and then click <strong>Configure</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Next to Pool, click <strong>Add new entry</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. In the Pool identifier box, type <strong>usb-modem-dialer-pool</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. In the Priority box, type <strong>25</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>OK</strong> until you return to the Interface page.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Configure dialer options.</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Name the dialer pool configured on the dialer interface you want to use for USB modem connectivity—for example, <strong>usb-modem-dialer-pool</strong>. For more information, see “Configuring a Dialer Interface for USB Modem Dial Backup” on page 387.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Set the dialer pool priority—for example, <strong>25</strong>.</td>
<td></td>
</tr>
<tr>
<td>Dialer pool priority has a range from <strong>1</strong> to <strong>255</strong>, with <strong>1</strong> designating lowest-priority interfaces and <strong>255</strong> designating the highest-priority interfaces.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the modem to automatically answer (autoanswer) calls after a specified number of rings.</td>
<td>1. Next to Modern options, click <strong>Configure</strong>.</td>
<td>Enter set modem-options init-command-string *ATS0=2 \n*</td>
</tr>
<tr>
<td></td>
<td>2. In the Init command string box, type <strong>ATS0=2 \n</strong> to configure the modem to autoanswer after two rings.</td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>The default modem initialization string is <strong>AT S7=45 S0=0 V1 X4 &amp;C1 E0 Q0 &amp;Q8 %C0</strong>. The modem command <strong>S0=0</strong> disables the modem from autoanswering calls.</td>
<td></td>
</tr>
<tr>
<td>Configure the modem to act as a dial-in WAN backup interface.</td>
<td>1. On the Modern options page, in the Dialin box, select <strong>routable</strong>.</td>
<td>Enter set modem-options dialin routable</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>OK</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring a Dialer Interface for USB Modem Dial Backup**

The dialer interface (dl) is a logical interface configured to establish USB modem connectivity. You can configure multiple dialer interfaces for different functions on the device.

After configuring the dialer interface, you must configure a backup method—either dialer backup, a dialer filter, or dialer watch.

For example, suppose you have a branch office router and a head office router each with a USB modem interface and a dialer interface. To establish a backup connection between the branch office and head office routers, you can configure them as described in Table 104 on page 388.
Table 104: Configuring Branch Office and Head Office Routers for USB Modem Backup Connectivity

<table>
<thead>
<tr>
<th>Router Location</th>
<th>Configuration Requirement</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch Office</td>
<td>1. Configure the logical dialer interface on the branch office router for USB modern dial backup.</td>
<td>To configure the logical dialer interface, see Table 105 on page 388.</td>
</tr>
<tr>
<td></td>
<td>2. Configure the dialer interface dl0 in one of the following ways on the branch office router:</td>
<td>To configure dl0 as a backup for t1-1/0/0 see “Configuring Dial Backup for a USB Modern Connection” on page 390.</td>
</tr>
<tr>
<td></td>
<td>■ Configure the dialer interface dl0 as the backup interface on the branch office router’s primary T1 interface t1-1/0/0.</td>
<td>To configure a dialer filter on dl0, see “Configuring a Dialer Filter for USB Modem Dial Backup” on page 391.</td>
</tr>
<tr>
<td></td>
<td>■ Configure a dialer filter on the branch office router’s dialer interface.</td>
<td>To configure a dialer watch on dl0, see “Configuring Dialer Watch for USB Modem Dial Backup” on page 393.</td>
</tr>
<tr>
<td></td>
<td>■ Configure a dialer watch on the branch office router’s dialer interface.</td>
<td></td>
</tr>
<tr>
<td>Head Office</td>
<td>Configure dial-in on the dialer interface dl0 on the head office router.</td>
<td>To configure dial-in on the head office router, see “Configuring Dial-In for a USB Modern Connection” on page 394.</td>
</tr>
</tbody>
</table>

To configure a logical dialer interface for USB modem dial backup:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 105 on page 388.
3. To configure a backup method, go on to one of the following tasks:
   ■ Configuring Dial Backup for a USB Modem Connection on page 390
   ■ Configuring a Dialer Filter for USB Modem Dial Backup on page 391
   ■ Configuring Dialer Watch for USB Modem Dial Backup on page 393

Table 105: Adding a Dialer Interface for USB Modem Dial Backup

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Interfaces level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit interfaces.</td>
</tr>
<tr>
<td></td>
<td>2. Next to Interfaces, click Configure or Edit.</td>
<td></td>
</tr>
</tbody>
</table>

JUNOS Software Interfaces and Routing Configuration Guide
### Table 105: Adding a Dialer Interface for USB Modem Dial Backup (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create the new interface—for example, dl0. Adding a description can differentiate between different dialer interfaces—for example, USB-modem-backup.</td>
<td>1. Next to Interface, click <strong>Add new entry</strong>&lt;br&gt;2. In the Interface name box, type dl0.&lt;br&gt;3. In the Description box, type USB-modem-backup. 4. Click <strong>OK</strong>.</td>
<td>Create and name the interface:&lt;br&gt;1. <code>edit dl0</code>&lt;br&gt;2. <code>set description USB-modem-backup</code></td>
</tr>
<tr>
<td>Configure Point-to-Point Protocol (PPP) encapsulation. <strong>NOTE:</strong> You cannot configure Cisco High-Level Data Link Control (HDLC) or Multilink PPP (MLPPP) encapsulation on dialer interfaces used in USB modem connections.</td>
<td>1. In the Encapsulation column, next to the new interface, click <strong>Edit</strong>&lt;br&gt;2. From the Encapsulation list, select <strong>ppp</strong>.</td>
<td>Enter&lt;br&gt;<code>set encapsulation ppp</code></td>
</tr>
<tr>
<td>Create the logical unit 0. <strong>NOTE:</strong> You can set the logical unit to 0 only.</td>
<td>1. Next to Unit, click <strong>Add new entry</strong>&lt;br&gt;2. In the Interface unit number box, type 0.&lt;br&gt;3. Next to Dialer options, select <strong>Yes</strong>, and then click <strong>Configure</strong>.</td>
<td>Enter&lt;br&gt;<code>set unit 0</code></td>
</tr>
</tbody>
</table>
Table 105: Adding a Dialer Interface for USB Modem Dial Backup (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure dialer options.</td>
<td>1. In the Activation delay box, type 60. 2. In the Deactivation delay box, type 30. 3. In the Idle timeout box, type 30. 4. In the Initial route check box, type 30. 5. In the Pool box, type usb-modem-dialer-pool.</td>
<td>1. Enter edit unit 0 dialer-options. 2. Enter set activation-delay 60. 3. Enter set deactivation-delay 30. 4. Enter set idle-timeout 30 initial-route-check 30 pool usb-modem-dialer-pool.</td>
</tr>
<tr>
<td><strong>Activation delay</strong>—Number of seconds to wait before activating the backup USB modem interface after the primary interface is down—for example, 30. The default value is 0 seconds, and the maximum value is 60 seconds. Use this option only for dialer backup and dialer watch.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Deactivation delay</strong>—Number of seconds to wait before deactivating the backup USB modem interface after the primary interface is up—for example, 30. The default value is 0 seconds, and the maximum value is 60 seconds. Use this option only for dialer backup and dialer watch.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Idle timeout</strong>—Number of seconds a connection is idle before disconnecting—for example, 30. The default value is 120 seconds, and the range is from 0 to 4294967295.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Initial route check</strong>—Number of seconds to wait before checking if the primary interface is up—for example, 30. The default value is 120 seconds, and the range is from 1 to 300 seconds.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Pool</strong>—Name of the dialer pool to use for USB modem connectivity—for example, usb-modem-dialer-pool.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Configure the telephone number of the remote destination to call if the primary interface goes down—for example, 5551212.

1. Next to Dial string, click Add new entry.
2. In the Dial string box, type 5551212.
3. Click OK until you return to the Unit page.

4. Enter set dial-string 5551212.

Configure source and destination IP addresses for the dialer interface—for example, 172.20.10.2 and 172.20.10.1.

**NOTE:** If you configure multiple dialer interfaces, ensure that the same IP subnet address is not configured on different dialer interfaces. Configuring the same IP subnet address on multiple dialer interfaces can result in inconsistency in the route and packet loss. Packets can be routed through any of the dialer interfaces with the IP subnet address, instead of being routed through the dialer interface to which the USB modem call is mapped.

1. Select Inet under Family, and click Edit.
2. Next to Address, click Add new entry.
3. In the Source box, type 172.20.10.2.
4. In the Destination box, type 172.20.10.1.
5. Click OK.

1. From the [edit] hierarchy level, enter edit interfaces dl0 unit 0.
2. Enter set family inet address 172.20.10.2 destination 172.20.10.1.

Configuring Dial Backup for a USB Modem Connection

Dial backup allows one or more dialer interfaces to be configured as the backup link for the primary serial interface. The backup dialer interfaces are activated only when
the primary interface fails. USB modem backup connectivity is supported on all interfaces except lsq-0/0/0.

To configure a primary interface for backup connectivity:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 106 on page 391.
3. If you are finished configuring the device, commit the configuration.

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Interfaces</strong> level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit interfaces t1-1/0/0 unit 0</td>
</tr>
<tr>
<td></td>
<td>2. Next to Interfaces, click <strong>Edit</strong>.</td>
<td></td>
</tr>
<tr>
<td>Select the physical interface for USB modem USB modem backup connectivity—for example, t1-1/0/0.</td>
<td>1. In the Interface name column, click the physical interface name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Under Unit, in the Interface unit number column, click <strong>0</strong>.</td>
<td></td>
</tr>
<tr>
<td>Configure the backup dialer interface—for instance, dl0.0.</td>
<td>1. Next to Backup options, click <strong>Configure</strong>.</td>
<td>Enter</td>
</tr>
<tr>
<td></td>
<td>2. In the Interface box, type <strong>dl0.0</strong>.</td>
<td>set backup-options interface dl0.0</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>OK</strong> until you return to the Interfaces page.</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring a Dialer Filter for USB Modem Dial Backup**

This dial-on-demand routing backup method allows a USB modem connection to be activated only when network traffic configured as an “interesting packet” arrives on the network. Once the network traffic is sent, an inactivity timer is triggered and the connection is closed.

You define an interesting packet using the dialer filter feature of the device.

To configure dial-on-demand routing backup using a dialer filter, you first configure the dialer filter and then apply the filter to the dialer interface.

To configure the dialer filter and apply it to the dialer interface:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 107 on page 392.
3. Go on to Table 108 on page 392.
4. When you are finished configuring the device, commit the configuration.

Table 107: Configuring a Dialer Filter for USB Modem Dial Backup

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Firewall level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI</td>
<td>From the [edit] hierarchy level, enter edit firewall</td>
</tr>
<tr>
<td></td>
<td>2. Next to Firewall, click Edit</td>
<td></td>
</tr>
<tr>
<td>Configure the dialer filter name—for example, interesting-traffic.</td>
<td>1. Next to Inet, click Configure or Edit</td>
<td>1. Enter edit family inet</td>
</tr>
<tr>
<td></td>
<td>2. Next to Dialer filter, click Add new entry</td>
<td>2. Then enter edit dialer-filter interesting-traffic</td>
</tr>
<tr>
<td></td>
<td>3. In the Filter name box, type interesting-traffic</td>
<td></td>
</tr>
<tr>
<td>Configure the dialer filter rule name—for example, term1.</td>
<td>1. Next to Term, click Add new entry</td>
<td>1. Enter edit term term1</td>
</tr>
<tr>
<td></td>
<td>2. In the Rule name box, type term1</td>
<td>2. Enter set from source-address 20.20.90.4/32</td>
</tr>
<tr>
<td></td>
<td>3. Next to From, click Configure</td>
<td>3. Enter set from destination-address 200.200.201.1/32</td>
</tr>
<tr>
<td></td>
<td>4. Next to Source address, click Add new entry</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. In the Address box, type 20.20.90.4/32</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Click OK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. Next to Destination address, click Add new entry</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. In the Address box, type 200.200.201.1/32</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9. Click OK until you return to the Term page</td>
<td></td>
</tr>
<tr>
<td>Configure the then part of the dialer filter to discard Telnet traffic between the branch office router and the head office router.</td>
<td>1. Next to Then, click Configure</td>
<td>Enter set then note</td>
</tr>
<tr>
<td></td>
<td>2. From the Designation list, select Note</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Click OK</td>
<td></td>
</tr>
</tbody>
</table>

Table 108: Applying the Dialer Filter to the Dialer Interface

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Interfaces level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI</td>
<td>From the [edit] hierarchy level, enter edit interfaces dl0 unit 0</td>
</tr>
<tr>
<td></td>
<td>2. Next to Interfaces, click Edit</td>
<td></td>
</tr>
</tbody>
</table>
Table 108: Applying the Dialer Filter to the Dialer Interface (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Select the dialer interface to apply the filter—for example, dl0. | 1. In the Interface name column, click dl0.  
2. Under Unit, in the Interface unit number column, click 0. | 1. Enter edit family inet filter  
2. Next to Filter, click Configure.  
3. In the Dialer box, type interesting-traffic, the dialer filter configured in “Configuring the Dialer Filter” on page 328.  
4. Click OK. |

Apply the dialer filter to the dialer interface.

1. In the Family section, next to Inet, click Edit.  
2. Next to Filter, click Configure.  
3. In the Dialer box, type interesting-traffic, the dialer filter configured in “Configuring the Dialer Filter” on page 328.  
4. Click OK.

Configuring Dialer Watch for USB Modem Dial Backup

Dialer watch is a backup method that integrates backup dialing with routing capabilities and provides reliable connectivity without relying on a dialer filter to trigger outgoing USB modem connections. With dialer watch, the device monitors the existence of a specified route and if the route disappears, the dialer interface initiates the USB modem connection as a backup connection.

In this example, you configure dialer watch to enable the device to monitor the existence of the route to the head office router and initiate USB modem backup connectivity if the route disappears.

To configure dialer watch, you first add a dialer watch interface and then configure the USB modem interface to participate as a dialer watch interface.

To configure a dialer watch:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 109 on page 393.
3. Go on to Table 110 on page 394.
4. When you are finished configuring the device, commit the configuration.

Table 109: Adding a Dialer Watch Interface

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Navigate to the Interfaces level in the configuration hierarchy. | 1. In the J-Web interface, select Configure > CLI Tools > Point and Click CLI  
2. Next to Interfaces, click Edit. | From the [edit] hierarchy level, enter edit interfaces |

Chapter 13: Configuring USB Modems for Dial Backup
### Table 109: Adding a Dialer Watch Interface (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a dialer interface—for example, dl0.</td>
<td>1. Under Interface name, select dl0.</td>
<td>1. Enter</td>
</tr>
<tr>
<td>Adding a description, such as dialer-watch, can help you identify one</td>
<td>2. In the Description box, type dialer-watch.</td>
<td>2. Enter</td>
</tr>
<tr>
<td>dialer interface from another.</td>
<td></td>
<td>set description dialer-watch</td>
</tr>
<tr>
<td>On a logical interface—for example, 0—configure the route to the</td>
<td>1. Under Unit, click the logical unit number 0.</td>
<td>1. Enter</td>
</tr>
<tr>
<td>head office router for dialer watch—for example, 200.200.201.1/32.</td>
<td>2. Next to Dialer options, click Edit.</td>
<td>edit unit 0 dialer-options</td>
</tr>
<tr>
<td>3. Next to Watch list, click Add new entry.</td>
<td></td>
<td>2. Enter</td>
</tr>
<tr>
<td>4. In the Prefix box, type 200.200.201.1/32.</td>
<td></td>
<td>set watch-list 200.200.201.1/32</td>
</tr>
<tr>
<td>5. Click OK.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the name of the dialer pool to use for dialer watch—for</td>
<td>1. In the Pool box, type dw-pool.</td>
<td>Enter</td>
</tr>
<tr>
<td>example, dw-pool.</td>
<td>2. Click OK.</td>
<td>set pool dw-pool</td>
</tr>
</tbody>
</table>

### Table 110: Configuring a USB Modem Interface for Dialer Watch

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Interfaces level in the configuration hierarchy, and</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI</td>
<td>From the [edit] hierarchy level, enter</td>
</tr>
<tr>
<td>select the USB modem physical interface umd0.</td>
<td>2. Next to Interfaces, click Edit.</td>
<td>edit interfaces umd0</td>
</tr>
<tr>
<td>3. Under Interface name, click umd0.</td>
<td></td>
<td>dialer-options pool</td>
</tr>
<tr>
<td>Configure dialer watch options for the USB modem interface</td>
<td>1. Next to Dialer options, click Edit.</td>
<td>dw-pool</td>
</tr>
<tr>
<td>participating in the dialer watch.</td>
<td>2. Next to Pool, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td>The USB modem interface must have the same pool identifier to</td>
<td>3. In the Pool identifier box, type dw-pool.</td>
<td></td>
</tr>
<tr>
<td>participate in dialer watch.</td>
<td>4. Click OK.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Dial-In for a USB Modem Connection

You can configure a dialer interface to accept all incoming calls or accept only calls from one or more caller IDs.
If the dialer interface is configured to accept only calls from a specific caller ID, the device matches the incoming call’s caller ID against the caller IDs configured on its dialer interfaces. If an exact match is not found and the incoming call’s caller ID has more digits than the configured caller IDs, the device performs a right-to-left match of the incoming call’s caller ID with the configured caller IDs and accepts the incoming call if a match is found. For example, if the incoming call’s caller ID is 4085521091 and the caller ID configured on a dialer interface is 5321091, the incoming call is accepted. Each dialer interface accepts calls from only callers whose caller IDs are configured on it.

To configure a dialer interface for USB modem dial-in:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 111 on page 395.
3. If you are finished configuring the device, commit the configuration.

### Table 111: Configuring the Dialer Interface for USB Modem Dial-In

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Navigate to the **Interfaces** level in the configuration hierarchy, and select a dialer interface—for example, dl0. | 1. In the J-Web interface, select **Configure > CLI Tools > Point and Click CLI**.  
2. Next to Interfaces, click **Edit**.  
3. Next to dl0, click **Edit**. | From the [edit] hierarchy level, enter **edit interfaces dl0** |

On logical interface 0, configure the incoming map options for the dialer interface.

- **accept-all**—Dialer interface accepts all incoming calls.
  
  You can configure the **accept-all** option for only one of the dialer interfaces associated with a USB modem physical interface. The dialer interface with the **accept-all** option configured is used only if the incoming call’s caller ID does not match the caller IDs configured on other dialer interfaces.

- **caller**—Dialer interface accepts calls from a specific caller ID—for example, **4085551515**. You can configure a maximum of 15 caller IDs per dialer interface.
  
  The same caller ID must not be configured on different dialer interfaces. However, you can configure caller IDs with more or fewer digits on different dialer interfaces. For example, you can configure the caller IDs 14085551515, 4085551515, and 5551515 on different dialer interfaces.

1. In the Unit section, for logical unit number 0, click **Dialer options** under Encapsulation.  
2. Next to Incoming map, click **Configure**.  
3. From the Caller type menu, select **Caller**.  
4. Next to Caller, click **Add new entry**.  
5. In the Caller id box, type **4085551515**.

1. Enter **edit unit 0**  
2. Enter **edit dialer-options**  
3. Enter **set incoming-map caller 4085551515**
**Configuring PAP on Dialer Interfaces (Optional)**

You can configure dialer interfaces to support the Password Authentication Protocol (PAP). PAP allows a simple method for a peer to establish its identity using a two-way handshake during initial link establishment. After the link is established, an ID and password pair is repeatedly sent by the peer to the authenticator until authentication is acknowledged or the connection is terminated.

For more information about PAP, see the *Junos Network Interfaces Configuration Guide*.

To configure PAP on the dialer interface, create an access profile and then configure the dialer interface:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 112 on page 396.
3. If you are finished configuring the device, commit the configuration.

**Table 112: Configuring PAP on Dialer Interfaces**

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Define a PAP access profile—for example, `pap-access-profile` with a client (username) named `pap-access-user` and the PAP password `my-pap`. | 1. On the main Configuration page next to Access, click **Configure** or **Edit**.  
2. Next to Profile, click **Add new entry**.  
3. In the Profile name box, type `pap-access-profile`.  
4. Next to Client, click **Add new entry**.  
5. In the Name box, type `pap-access-user`.  
6. In the Pap-password box, type `my-pap`.  
7. Click **OK** until you return to the main Configuration page. | From the [edit] hierarchy level, enter  
*set access-profile pap-access-profile client pap-access-user pap-password my-pap* |
| Navigate to the appropriate dialer interface level in the configuration hierarchy—for example, `dl0` unit 0. | 1. On the main Configuration page next to Interfaces, click **Configure** or **Edit**.  
2. In the interface name box, click `dl0`.  
3. In the Interface unit number box, click `0`. | From the [edit] hierarchy level, enter  
*edit interfaces dl0 unit 0* |
Table 112: Configuring PAP on Dialer Interfaces (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure PAP on the dialer interface and specify the local name and</td>
<td>1. Next to Ppp options, click <strong>Configure</strong></td>
<td>Enter set ppp-options pap local-name</td>
</tr>
<tr>
<td>password—for example, pap-access-profile and my-pap</td>
<td>2. Next to Pap, click <strong>Configure</strong></td>
<td>pap-access-user local-password my-pap</td>
</tr>
<tr>
<td></td>
<td>3. In the Local name box, type pap-access-profile.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. In the Local password box, type my-pap.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>OK</strong></td>
<td></td>
</tr>
</tbody>
</table>

Configuring CHAP on Dialer Interfaces (Optional)

You can optionally configure dialer interfaces to support the PPP Challenge Handshake Authentication Protocol (CHAP). CHAP is a server-driven, three-step authentication method that depends on a shared secret password residing on both the server and the client. When you enable CHAP on a dialer interface, the device can authenticate its peer and be authenticated by its peer.

For more information about CHAP, see the *Junos Network Interfaces Configuration Guide*.

To configure CHAP on the dialer interface:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 113 on page 398.
3. If you are finished configuring the device, commit the configuration.
### Table 113: Configuring CHAP on Dialer Interfaces

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Define a CHAP access profile—for example, `usb-modem-access-profile` with a client (username) named `usb-modem-user` and the secret (password) `my-secret`. | 1. On the main Configuration page next to Access, click **Configure** or **Edit**.  
2. Next to Profile, click **Add new entry**.  
3. In the Profile name box, type `usb-modem-access-profile`.  
4. Next to Client, click **Add new entry**.  
5. In the Name box, type `usb-modem-user`.  
6. In the Chap secret box, type `my-secret`.  
7. Click **OK** until you return to the main Configuration page. | From the [edit] hierarchy level, enter:  
- `set access profile usb-modem-access-profile client usb-modem-user chap-secret my-secret` |
| Navigate to the appropriate dialer interface level in the configuration hierarchy—for example, `di0 unit 0`. | 1. On the main Configuration page next to Interfaces, click **Configure** or **Edit**.  
2. In the interface name box, click `di0`.  
3. In the Interface unit number box, click `0`. | From the [edit] hierarchy level, enter:  
- `edit interfaces di0 unit 0` |
| Configure CHAP on the dialer interface and specify a unique profile name containing a client list and access parameters—for example, `usb-modem-access-profile`. | 1. Next to Ppp options, click **Configure**.  
2. Next to Chap, click **Configure**.  
3. In the Access profile box, type `usb-modem-access-profile`.  
4. Click **OK**. | Enter:  
- `set ppp-options chap access-profile usb-modem-access-profile` |
Chapter 14

Configuring Link Services Interfaces

Link services include the multilink services Multilink Point-to-Point Protocol (MLPPP), Multilink Frame Relay (MLFR), and Compressed Real-Time Transport Protocol (CRTP). J Series devices support link services on the lsq-0/0/0 link services interface.

You can use either J-Web Quick Configuration or a configuration editor to configure the link services interface.

For information about which devices support the features documented in this chapter, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.

This chapter contains the following topics:

- Link Services Terms on page 399
- Link Services Interfaces Overview on page 400
- Before You Begin on page 410
- Configuring the Link Services Interface with Quick Configuration on page 410
- Configuring the Link Services Interface with a Configuration Editor on page 413
- Verifying the Link Services intelligent queuing Interface Configuration on page 431
- Frequently Asked Questions About the Link Services Interface on page 439

Link Services Terms

Before configuring a link services interface, become familiar with the terms defined in Table 114 on page 399.

Table 114: Link Services Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compressed Real-Time Transport Protocol (CRTP)</td>
<td>Protocol defined in RFC 2508 that compresses the size of IP, UDP, and Real-Time Transport Protocol (RTP) headers and works with reliable and fast point-to-point links for voice over IP (VoIP) traffic.</td>
</tr>
<tr>
<td>data-link connection identifier (DLCI)</td>
<td>Identifier for a Frame Relay virtual connection, also called a logical interface.</td>
</tr>
</tbody>
</table>
Table 114: Link Services Terminology (continued)

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>link fragmentation and interleaving (LFI)</td>
<td>For MLFR with Frame Relay traffic or MLPPP with PPP traffic, a method of reducing excessive delays by fragmenting long packets into smaller packets and interleaving them with real-time frames. For example, short delay-sensitive packets, such as those of packetized voice, can race ahead of larger delay-insensitive packets, such as common data packets.</td>
</tr>
<tr>
<td>link services</td>
<td>Capabilities on an interface that use Multilink Frame Relay (MLFR) and Multilink Point-to-Point Protocol (MLPPP), link fragmentation and interleaving (LFI), Compressed Real-Time Transport Protocol (CRTP), and certain class-of-service (CoS) components to improve packet transmission, especially for time-sensitive voice packets.</td>
</tr>
<tr>
<td>Multilink Frame Relay (MLFR)</td>
<td>Protocol that allows multiple Frame Relay links to be aggregated by inverse multiplexing.</td>
</tr>
<tr>
<td>Multilink Point-to-Point Protocol (MLPPP)</td>
<td>Protocol that allows you to bundle multiple Point-to-Point Protocol (PPP) links into a single logical unit. MLPPP improves bandwidth efficiency and fault tolerance and reduces latency.</td>
</tr>
<tr>
<td>Point-to-Point Protocol (PPP)</td>
<td>Link-layer protocol defined in RFC 1661 that provides multiprotocol encapsulation. PPP is used for link-layer and network-layer configuration.</td>
</tr>
<tr>
<td>shaping rate</td>
<td>In class of service (CoS) classification, a method of controlling the maximum rate of traffic transmitted on an interface.</td>
</tr>
</tbody>
</table>

**Link Services Interfaces Overview**

You configure the link services queuing interface (lsq-0/0/0) on a J Series device to support multilink services and Compressed Real-Time Transport Protocol (CRTP).

The link services interface on a J Series device consists of services provided by the following interfaces on the Juniper Networks M Series and T Series routing platforms: multilink services interface (ml-fpc/pic/port), link services interface (ls-fpc/pic/port), and link services intelligent queuing interface (lsq-fpc/pic/port). Although the multilink services, link services, and link services intelligent queuing (IQ) interfaces on M Series and T Series routing platforms are installed on Physical Interface Cards (PICs), the link services interface on a J Series device is an internal interface only and is not associated with a physical medium or Physical Interface Module (PIM).

**NOTE:** (ls-fpc/pic/port) is not supported on J series and SRX platforms.

For information about interface names, see “Network Interface Naming” on page 9.

For more information about the link services interfaces, see the *Junos Services Interfaces Configuration Guide*. 
This section contains the following topics.

- Services Available on J Series Link Services Interface on page 401
- Link Services Exceptions on J Series Services Routers on page 402
- Multilink Bundles Overview on page 402
- Link Fragmentation and Interleaving Overview on page 403
- Compressed Real-Time Transport Protocol Overview on page 404
- Configuring Fragmentation by Forwarding Class on page 405
- Configuring Link-Layer Overhead on page 406
- Configuring Multiclass MLPPP on page 407
- Queuing with LFI on J Series Devices on page 409
- Configuring CoS Components with LFI on page 409

**Services Available on J Series Link Services Interface**

On a J Series device, the link services interface is a logical interface available by default. Table 115 on page 401 summarizes the services available on a J Series link services interface.

**Table 115: Services Available on J Series Link Services Interface**

<table>
<thead>
<tr>
<th>Services</th>
<th>Purpose</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multilink bundles by means of MLPPP and MLFR encapsulation</td>
<td>Aggregates multiple constituent links into one larger logical bundle to provide additional bandwidth, load balancing, and redundancy.</td>
<td>■ Configuring an MLPPP Bundle on page 414</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Configuring MLFR FRF.15 Bundles on page 424</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Configuring MLFR FRF.16 Bundles on page 427</td>
</tr>
<tr>
<td>Link fragmentation and interleaving (LFI)</td>
<td>Reduces delay and jitter on links by breaking up large data packets and interleaving delay-sensitive voice packets with the resulting smaller packets.</td>
<td>“Link Fragmentation and Interleaving Overview” on page 403</td>
</tr>
</tbody>
</table>
Table 115: Services Available on J Series Link Services Interface (continued)

<table>
<thead>
<tr>
<th>Services</th>
<th>Purpose</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class-of-service (CoS) classifiers, forwarding classes, scheduler maps,</td>
<td>Provide a higher priority to delay-sensitive packets—by configuring class of service (CoS) components, such as the following:</td>
<td>Defining Classifiers and Forwarding Classes on page 417</td>
</tr>
<tr>
<td>and shaping rates</td>
<td>- Classifiers—To classify different type of traffic, such as voice, data and network control packets</td>
<td>Defining and Applying Scheduler Maps on page 420</td>
</tr>
<tr>
<td></td>
<td>- Forwarding classes—To direct different types of traffic to different output queues</td>
<td>Applying Shaping Rates to Interfaces on page 423</td>
</tr>
<tr>
<td></td>
<td>- Fragmentation map—To define mapping between forwarding class and multilink class, forwarding class and fragment threshold. In forwarding class and multilink class mapping, drop timeout can be configured.</td>
<td>Configuring Fragmentation by Forwarding Class on page 405</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Junos OS Class of Service Configuration Guide for Security Devices</td>
</tr>
<tr>
<td></td>
<td>- Schedulers and scheduler maps—To define properties for the output queues such as delay-buffer, transmission rate, and transmission priority</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Shaping rate—To define certain bandwidth usage by an interface</td>
<td></td>
</tr>
</tbody>
</table>

Link Services Exceptions on J Series Services Routers

The link and multilink services implementation on a J Series Services Router is similar to the implementation on the M Series and T Series routing platforms, with the following exceptions:

- J Series devices support link and multilink services on the lsq-0/0/0 interface instead of the mlfpc/pic/port, lsq-fpc/pic/port, and ls-fpc/pic/port interfaces.

- When LFI is enabled, fragmented packets are queued in a round-robin fashion on the constituent links to enable per-packet and per-fragment load balancing. For more information, see “Queuing with LFI on J Series Devices” on page 409.

- J Series devices support per-unit scheduling on all types of constituent links (on all types of interfaces).

- J Series devices support Compressed Real-Time Transport Protocol (CRTP) with MLPPP as well as PPP.

Multilink Bundles Overview

The J Series device supports MLPPP and MLFR multilink encapsulations. MLPPP enables you to bundle multiple PPP links into a single multilink bundle, and MLFR enables you to bundle multiple Frame Relay data-link connection identifiers (DLCIs) into a single multilink bundle. Multilink bundles provide additional bandwidth, load balancing, and redundancy by aggregating low-speed links, such as T1, E1, and serial links.
You configure multilink bundles as logical units or channels on the link services interface lsq-0/0/0:

- With MLPPP and MLFR FRF.15, multilink bundles are configured as logical units on lsq-0/0/0—for example, lsq-0/0/0.0 and lsq-0/0/0.1.
- With MLFR FRF.16, multilink bundles are configured as channels on lsq-0/0/0—for example, lsq-0/0/0:0 and lsq-0/0/0:1.

After creating multilink bundles, you add constituent links to the bundle. The constituent links are the low-speed physical links that are to be aggregated. You can create 64 multilink bundles, and on each multilink bundle you can add up to 8 constituent links. The following rules apply when you add constituent links to a multilink bundle:

- On each multilink bundle, add only interfaces of the same type. For example, you can add either T1 or E1, but not both.
- Only interfaces with a PPP encapsulation can be added to an MLPPP bundle, and only interfaces with a Frame Relay encapsulation can be added to an MLFR bundle.
- If an interface is a member of an existing bundle and you add it to a new bundle, the interface is automatically deleted from the existing bundle and added to the new bundle.

For information about configuring MLPPP bundles, see “Configuring an MLPPP Bundle” on page 414. For information about configuring MLFR bundles, see “Configuring MLFR FRF.15 Bundles” on page 424 and “Configuring MLFR FRF.16 Bundles” on page 427.

### Link Fragmentation and Interleaving Overview

As it does on any other interface, priority scheduling on a multilink bundle determines the order in which an output interface transmits traffic from an output queue. The queues are serviced in a weighted round-robin fashion. But when a queue containing large packets starts using the multilink bundle, small and delay-sensitive packets must wait their turn for transmission. Because of this delay, some slow links, such as T1 and E1, can become useless for delay-sensitive traffic.

Link fragmentation and interleaving (LFI) solves this problem. It reduces delay and jitter on links by fragmenting large packets and interleaving delay-sensitive packets with the resulting smaller packets for simultaneous transmission across multiple links of a multilink bundle.

Figure 46 on page 404 illustrates how LFI works. In this figure, Device R0 and Device R1 have LFI enabled. When Device R0 receives large and small packets, such as data and voice packets, it divides them into two categories. All voice packets and any other packets configured to be treated as voice packets are categorized as LFI packets and transmitted without fragmentation or an MLPPP header. If CRTP is configured on the bundle, LFI packets are transmitted through CRTP processing. The remaining non-LFI (data) packets can be fragmented or unfragmented based on the configured fragmentation threshold. The packets larger than the fragmentation threshold are
fragmented. An MLPPP header (containing a multilink sequence number) is added to all non-LFI packets, fragmented and unfragmented.

The fragmentation is performed according to the fragmentation threshold that you configure. For example, if you configure a fragmentation threshold of 128 bytes, all packets larger than 128 bytes are fragmented. When Device R1 receives the packets, it sends the unfragmented voice packets immediately but buffers the packet fragments until it receives the last fragment for a packet. In this example, when Device R1 receives fragment 5, it reassembles the fragments and transmits the whole packet.

The unfragmented data packets are treated as a single fragment. Thus Device R1 does not buffer the unfragmented data packets and transmits them as it receives them.

For information about configuring LFI, see “Enabling Link Fragmentation and Interleaving” on page 416.

**Compressed Real-Time Transport Protocol Overview**

Real-Time Transport Protocol (RTP) can help achieve interoperability among different implementations of network audio and video applications. However, in some cases, the header, which includes the IP, UDP, and RTP headers, can be too large (around 40 bytes) on networks using low-speed lines such as dial-up modems. Compressed Real-Time Transport Protocol (CRTP) can be configured to reduce network overhead on low-speed links. CRTP replaces the IP, UDP, and RTP headers with a 2-byte context ID (CID), reducing the header overhead considerably.

Figure 47 on page 405 shows how CRTP compresses the RTP headers in a voice packet and reduces a 40-byte header to a 2-byte header.
On J Series devices, you can configure CRTP with MLPPP or PPP logical interface encapsulation on link services interfaces. For more information about configuring MLPPP, see “Configuring an MLPPP Bundle” on page 414.

Real-time and non-real-time data frames are carried together on lower-speed links without causing excessive delays to the real-time traffic. For more information about LFI, see “Link Fragmentation and Interleaving Overview” on page 403.

**Configuring Fragmentation by Forwarding Class**

For lsq-0/0/0 on SRX210, SRX240, SRX650, J2320, J2350, J4350, and J6350 devices, you can specify fragmentation properties for specific forwarding classes. Traffic on each forwarding class can be either multilink encapsulated (fragmented and sequenced) or nonencapsulated (hashed with no fragmentation). By default, traffic in all forwarding classes is multilink encapsulated.

When you do not configure fragmentation properties for the queues on MLPPP interfaces, the fragmentation threshold you set at the `[edit interfaces interface-name unit logical-unit-number fragment-threshold]` hierarchy level is the fragmentation threshold for all forwarding classes within the MLPPP interface. For MLFR FRF.16 interfaces, the fragmentation threshold you set at the `[edit interfaces interface-name mfr-uni-nni-bundle-options fragment-threshold]` hierarchy level is the fragmentation threshold for all forwarding classes within the MLFR FRF.16 interface.

If you do not set a maximum fragment size anywhere in the configuration, packets are still fragmented if they exceed the smallest maximum transmission unit (MTU) or maximum received reconstructed unit (MRRU) of all the links in the bundle. A nonencapsulated flow uses only one link. If the flow exceeds a single link, then the forwarding class must be multilink encapsulated, unless the packet size exceeds the MTU/MRRU.

Even if you do not set a maximum fragment size anywhere in the configuration, you can configure the MRRU by including the mrru statement at the `[edit interfaces lsq-0/0/0 unit logical-unit-number]` or `[edit interfaces interface-name mfr-uni-nni-bundle-options]` hierarchy level. The MRRU is similar to the MTU, but is specific to link services interfaces. By default the MRRU size is 1504 bytes, and you can configure it to be from 1500 through 4500 bytes.

To configure fragmentation properties on a queue, include the fragmentation-maps statement at the `[edit class-of-service]` hierarchy level:
To set a per-forwarding class fragmentation threshold, include the `fragment-threshold` statement in the fragmentation map. This statement sets the maximum size of each multilink fragment.

To set traffic on a queue to be nonencapsulated rather than multilink encapsulated, include the `no-fragmentation` statement in the fragmentation map. This statement specifies that an extra fragmentation header is not prepended to the packets received on this queue and that static link load balancing is used to ensure in-order packet delivery.

For a given forwarding class, you can include either the `fragment-threshold` or `no-fragmentation` statement; they are mutually exclusive.

You use the `multilink-class` statement to map a forwarding class into a multiclass MLPPP. For a given forwarding class, you can include either the `multilink-class` or `no-fragmentation` statement; they are mutually exclusive.

To associate a fragmentation map with a multilink PPP interface or MLFR FRF.16 DLCI, include the `fragmentation-map` statement at the `interfaces` hierarchy level:

```
[edit class-of-service interfaces]
lsq-0/0/0 {
    unit logical-unit-number { # Multilink PPP
        fragmentation-map map-name;
    }
}
lsq-0/0/0:channel { # MLFR FRF.16
    unit logical-unit-number
        fragmentation-map map-name;
}
```

**Configuring Link-Layer Overhead**

Link-layer overhead can cause packet drops on constituent links because of bit stuffing on serial links. Bit stuffing is used to prevent data from being interpreted as control information.
By default, 4 percent of the total bundle bandwidth is set aside for link-layer overhead. In most network environments, the average link-layer overhead is 1.6 percent. Therefore, we recommend 4 percent as a safeguard.

For **lsq-0/0/0** on SRX210, SRX240, SRX650, J2320, J2350, J4350, and J6350 devices, you can configure the percentage of bundle bandwidth to be set aside for link-layer overhead. To do this, include the link-layer-overhead statement:

```
link-layer-overhead percent;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces interface-name mfr-uni-nni-bundle-options]
- [edit interfaces interface-name unit logical-unit-number]
- [edit logical-routers logical-router-name interfaces interface-name unit logical-unit-number]

You can configure the value to be from 0 percent through 50 percent.

### Configuring Multiclass MLPPP

For **lsq-0/0/0** on SRX210, SRX240, SRX650, J2320, J2350, J4350, and J6350 devices, with MLPPP encapsulation, you can configure multiclass MLPPP. If you do not configure multiclass MLPPP, fragments from different classes cannot be interleaved. All fragments for a single packet must be sent before the fragments from another packet are sent. Nonfragmented packets can be interleaved between fragments of another packet to reduce latency seen by nonfragmented packets. In effect, latency-sensitive traffic is encapsulated as regular PPP traffic, and bulk traffic is encapsulated as multilink traffic. This model works as long as there is a single class of latency-sensitive traffic, and there is no high-priority traffic that takes precedence over latency-sensitive traffic. This approach to LFI, used on the Link Services PIC, supports only two levels of traffic priority, which is not sufficient to carry the four-to-eight forwarding classes that are supported by M series and T series routing platforms.

Multiclass MLPPP makes it possible to have multiple classes of latency-sensitive traffic that are carried over a single multilink bundle with bulk traffic. In effect, multiclass MLPPP allows different classes of traffic to have different latency guarantees. With multiclass MLPPP, you can map each forwarding class into a separate multilink class, thus preserving priority and latency guarantees.
NOTE: Configuring both LFI and multiclass MLPPP on the same bundle is not necessary, nor is it supported, because multiclass MLPPP represents a superset of functionality. When you configure multiclass MLPPP, LFI is automatically enabled.

The JUNOS Software PPP implementation does not support the negotiation of address field compression and protocol field compression PPP NCP options, which means that the software always sends a full 4-byte PPP header.

The JUNOS Software implementation of multiclass MLPPP does not support compression of common header bytes.

Multiclass MLPPP greatly simplifies packet ordering issues that occur when multiple links are used. Without multiclass MLPPP, all voice traffic belonging to a single flow is hashed to a single link to avoid packet ordering issues. With multiclass MLPPP, you can assign voice traffic to a high-priority class, and you can use multiple links.

For more information about voice services support on the lsq-0/0/0 interface, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.

To configure multiclass MLPPP on a link services IQ interface, you must specify how many multilink classes should be negotiated when a link joins the bundle, and you must specify the mapping of a forwarding class into a multiclass MLPPP class.

To specify how many multilink classes should be negotiated when a link joins the bundle, include the `multilink-max-classes` statement:

```
multilink-max-classes number;
```

You can include this statement at the following hierarchy levels:

- `[edit interfaces interface-name unit logical-unit-number]`
- `[edit logical-routers logical-router-name interfaces interface-name unit logical-unit-number]`

The number of multilink classes can be 1 through 8. The number of multilink classes for each forwarding class must not exceed the number of multilink classes to be negotiated.

To specify the mapping of a forwarding class into a multiclass MLPPP class, include the `multilink-class` statement at the `[edit class-of-service fragmentation-maps forwarding-class class-name]` hierarchy level:

```
[edit class-of-service fragmentation-maps forwarding-class class-name] multilink-class number;
```

The multilink class index number can be 0 through 7. The `multilink-class` statement and the `no-fragmentation` statement are mutually exclusive.

To view the number of multilink classes negotiated, issue the `show interfaces lsq-0/0/0.logical-unit-number detail` command.
Queuing with LFI on J Series Devices

LFI or non-LFI packets are placed into queues on constituent links based on the queues in which they arrive. No changes in the queue number occur while the fragmented, non-fragmented, or LFI packets are being queued.

For example, assume that Queue Q0 is configured with fragmentation threshold 128, Q1 is configured with no fragmentation, and Q2 is configured with fragmentation threshold 512. Q0 is receiving stream of traffic with packet size 512. Q1 is receiving voice traffic of 64 bytes, and Q2 is receiving stream of traffic with 128-byte packets. Next the stream on Q0 gets fragmented and queued up into Q0 of a constituent link. The stream on Q1 is considered to be LFI because no fragmentation is configured. Therefore, all packets on Q1 are queued up on Q1 on constituent link. Because the fragmentation threshold of Q2 is more than the packet size it is receiving, the packet is queued on Q2 of a constituent link without fragmenting, but with multilink header because it is a non-LFI packet.

Using lsq/0/0/0, Compressed Real-Time Transport Protocol (CRTP) can be applied on LFI and non-LFI packets. There will be no changes in their queue numbers because of CRTP.

Queuing on Q2s of Constituent Links

When using class of service on a multilink bundle, all Q2 traffic from the multilink bundle is queued to Q2 of constituent links based on a hash computed from the source address, destination address, and the IP protocol of the packet. If the IP payload is TCP or UDP traffic, the hash also includes the source port and destination port. As a result of this hash algorithm, all traffic belonging to one traffic flow is queued to Q2 of one constituent link. This method of traffic delivery to the constituent link is applied at all times, including when the bundle has not been set up with LFI.

Configuring CoS Components with LFI

If you configure CoS components with LFI on a J Series device, we recommend that you follow certain recommendations for shaping rate, scheduling priority, and buffer size. For configuration instructions, see “Configuring MLPPP Bundles and LFI on Serial Links” on page 413. For more information about other CoS components, see Junos OS Class of Service Configuration Guide for Security Devices.

Shaping Rate

When you configure LFI, we recommend that you configure the shaping rate on each constituent link of the multilink bundle. Shaping rate configuration on the constituent links is required to limit the jitter on the LFI queue. If you anticipate no delay-sensitive or jitter-sensitive traffic on the LFI queue, or if there is no LFI traffic at all, shaping rate configuration is optional.

For information about how to configure a shaping rate, see Junos OS Class of Service Configuration Guide for Security Devices.
Scheduling Priority

J Series devices support per-unit scheduling that allows you to configure scheduler maps on each MLPPP or MLFR multilink bundle. You can also configure scheduler maps on constituent links, but you must maintain the same relative priority on the constituent links and on the multilink bundle.

Table 116 on page 410 shows an example of correct and incorrect relative priorities on a multilink bundle and its constituent link. In this example, you have assigned a high priority to LFI packets and a low priority to data packets on the multilink bundle. To maintain the relative priority on the constituent links, you can assign a high priority to the LFI packets and a medium-high priority to the data packets, but you cannot assign a medium-high priority to LFI packets and a high priority to data packets.

<table>
<thead>
<tr>
<th>Multilink Bundle</th>
<th>Correct Constituent Link Priorities</th>
<th>Incorrect Constituent Link Priorities</th>
</tr>
</thead>
<tbody>
<tr>
<td>LFI packets—High priority</td>
<td>LFI packets—High priority</td>
<td>LFI packet—Medium-high priority</td>
</tr>
<tr>
<td>Data packets—Low priority</td>
<td>Data packets—Medium-high priority</td>
<td>Data packets—High priority</td>
</tr>
</tbody>
</table>

Before You Begin

Before you configure a link services interface, you need to perform the following tasks:

- Install device hardware. For more information, see the J Series Services Routers Hardware Guide.
- Establish basic connectivity. For more information, see the Getting Started Guide for your device.
- If you do not already have a basic understanding of physical and logical interfaces and Juniper Networks interface conventions, read “Interfaces Overview” on page 3.

Although it is not a requirement, you might also want to plan how you are going to use the link services interface on your network before you begin configuring it. Read “Link Services Interfaces Overview” on page 400 for a basic understanding of the link services interface implementation.

Configuring the Link Services Interface with Quick Configuration

You can use the services interfaces Quick Configuration pages to do the following:

- Configure the lsq-0/0/0 link services interface.
- Configure multilink logical interfaces on the lsq-0/0/0 interface. Multilink logical interfaces allow you to bundle multiple serial interfaces such as T1, T3, E1, E3, and serial interfaces into a single logical link as follows:
Bundle multiple Point-to-Point Protocol (PPP) links into a single Multilink Point-to-Point Protocol (MLPPP) logical link.

Bundle multiple Frame Relay data-link connection identifiers (DLCIs) into a single Multilink Frame Relay (MLFR) logical link.

To configure the link services interface:

1. From the Quick Configuration page, as shown in Figure 16 on page 82, select the link services interface—for example, lsq-0/0/0—you want to configure.
2. Enter information into the Quick Configuration page, as described in Table 117 on page 411.
3. Click one of the following buttons:
   - To apply the configuration and stay on the Quick Configuration page, click Apply.
   - To apply the configuration and return to the main configuration page, click OK.
   - To cancel your entries and return to the main page, click Cancel.

Table 117: Link Services Interface Quick Configuration Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Logical Interfaces</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add logical interfaces</td>
<td>Defines one or more logical units that you connect to this link services interface. You must define at least one logical unit for the link services interface.</td>
<td>Click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Logical Interface Description</td>
<td><strong>(Optional)</strong> Describes the logical interface.</td>
<td>Type a text description of the logical interface to more clearly identify it in monitoring displays.</td>
</tr>
</tbody>
</table>
| IPv4 Addresses and Prefixes   | Specifies one or more IPv4 addresses for the interface.                   | 1. Type one or more IPv4 addresses and prefixes. For example: 10.10.10.10/24  
|                               |                                                                          | 2. Click **Add**  
|                               |                                                                          | 3. Click **OK**  |
| Physical Interface Description| **(Optional)** Adds supplementary information about the physical link services interface. | Type a text description of the link services interface to more clearly identify it in monitoring displays. |
| Enable subunit queuing         | Enables or disables subunit queuing on Frame Relay or VLAN IQ interfaces. | To enable subunit queuing, select the check box.  
|                               |                                                                          | To disable subunit queuing, clear the check box.  |

**Multilink Bundle Options**
### Table 117: Link Services Interface Quick Configuration Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth</td>
<td>Specifies the informational-only bandwidth value for the logical interface.</td>
<td>Type the value.</td>
</tr>
<tr>
<td>Drop Timer Period</td>
<td>Specifies a drop timeout value (in milliseconds) to provide a recovery mechanism if individual links in the multilink bundle drop one or more packets.</td>
<td>Type a value between 0 and 2000.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Ensure that the value you specify is larger than the expected differential delay across the links, so that the timeout period does not elapse under normal jitter conditions, but only when there is actual packet loss.</td>
<td></td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Specifies the encapsulation type for which you want to create a multilink bundle.</td>
<td>From the list, select one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- multilink-ppp—Creates a Multilink Point-to-Point Protocol (MLPPP) bundle.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- multilink-frame-relay-end-to-end—Creates a Multilink Frame Relay (MLFR) bundle.</td>
</tr>
<tr>
<td>Fragmentation Threshold</td>
<td>Specifies the maximum size, in bytes, for multilink packet fragments.</td>
<td>Type a value that is a multiple of 64 bytes between 64 and 16320—for example, 1024.</td>
</tr>
<tr>
<td>Links needed to sustain bundle</td>
<td>Specifies the minimum number of links required to sustain the multilink bundle.</td>
<td>Type a value between 1 and 8.</td>
</tr>
<tr>
<td>MRRU</td>
<td>Specifies the maximum packet size, in bytes, that the multilink interface can process.</td>
<td>Type a value between 1500 and 4500.</td>
</tr>
<tr>
<td>Short Sequence</td>
<td>Sets the length of the packet sequence identification number to 12 bits.</td>
<td>Select this check box.</td>
</tr>
</tbody>
</table>
Table 117: Link Services Interface Quick Configuration Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member Interfaces</td>
<td>Specifies the interfaces that are members of the multilink bundle.</td>
<td>■ To add an interface in the multilink bundle, select the interface in the Logical Interfaces list and click the left arrow button to add it in the Member Interfaces list.</td>
</tr>
<tr>
<td></td>
<td>The Logical Interfaces list displays all the serial interfaces on the device. The Member Interfaces list displays the interfaces that are members of the multilink bundle.</td>
<td>■ To remove an interface from the multilink bundle, select the interface in the Member Interfaces list and click the right arrow button to remove it from the Member Interfaces list.</td>
</tr>
<tr>
<td></td>
<td>The following rules apply when you add interfaces to a multilink bundle:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Only interfaces of the same type can be added to a multilink bundle. For example, a T1 and an E1 interface cannot be added to the same bundle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Only interfaces with the PPP encapsulation can be added to an MLPPP bundle and interfaces with the Frame Relay encapsulation can be added to an MLFR bundle.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ If you add an interface that is a member of an existing bundle, the interface is deleted from the existing bundle and added to the new bundle.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring the Link Services Interface with a Configuration Editor

This section contains the following topics:

■ Configuring MLPPP Bundles and LFI on Serial Links on page 413
■ Configuring MLFR FRF.15 Bundles on page 424
■ Configuring MLFR FRF.16 Bundles on page 427
■ Configuring CRTP on page 430

Configuring MLPPP Bundles and LFI on Serial Links

Figure 48 on page 414 shows a network topology that is used as an example in this section. In this example, your company’s branch office is connected to its main branch using J Series devices R0 and R1. You transmit data and voice traffic on two low-speed 1-Mbps serial links. To increase bandwidth, you configure MLPPP and join the two serial links se-1/0/0 and se-1/0/1 into a multilink bundle lsq-0/0/0.0. Then you configure LFI and CoS on R0 and R1 to enable them to transmit voice packets ahead of data packets.
Configuring a multilink bundle on the two serial links increases the bandwidth by 70 percent from approximately 1 Mbps to 1.7 Mbps and prepends each packet with a multilink header as specified in the FRF.12 standard. To increase the bandwidth further, you can add up to 8 serial links to the bundle. In addition to a higher bandwidth, configuring the multilink bundle provides load balancing and redundancy. If one of the serial links fails, traffic continues to be transmitted on the other links without any interruption. In contrast, independent links require routing policies for load balancing and redundancy. Independent links also require IP addresses for each link as opposed to one IP address for the bundle. In the routing table, the multilink bundle is represented as a single interface.

This example uses MLPPP for providing multilink services. For information about configuring MLFR, see “Configuring MLFR FRF.15 Bundles” on page 424 and “Configuring MLFR FRF.16 Bundles” on page 427.

You can use the LFI and CoS configurations provided in this example with MLFR FRF.15 and MLFR FRF.16 bundles, too. You can also use the same LFI and CoS configurations for other interfaces, such as on T1 or E1.

To configure MLPPP bundles and LFI, perform the following tasks:

- Configuring an MLPPP Bundle on page 414
- Enabling Link Fragmentation and Interleaving on page 416
- Defining Classifiers and Forwarding Classes on page 417
- Defining and Applying Scheduler Maps on page 420
- Applying Shaping Rates to Interfaces on page 423

### Configuring an MLPPP Bundle

In this example, you create an MLPPP bundle (lsq-0/0/0.0) at the logical unit level of the link services interface (lsq-0/0/0) on J Series devices R0 and R1. Then you add the two serial interfaces se-1/0/0 and se-1/0/1 as constituent links to the multilink bundle. Adding multiple links does not require you to configure and manage more addresses.

To configure an MLPPP bundle on a J Series device:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 118 on page 415 on Device R0 and Device R1.
3. Go on to “Enabling Link Fragmentation and Interleaving” on page 416.
### Table 118: Configuring an MLPPP Bundle

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Navigate to the **Interfaces** level in the configuration hierarchy. Specify the link services interface to be configured. | - In the J-Web interface, select **Configure > CLI Tools > Point and Click CLI**.  
- Next to Interfaces, click **Configure** or **Edit**.  
- Next to Interface, click **Add new entry**.  
- In the Interface name box, type `lsq-0/0/0`.  
- Click **OK**. | - From the [edit] hierarchy level, enter **edit interfaces lsq-0/0/0**. |
| Configure a logical unit on the `lsq-0/0/0` interface and define the family type—for example, `Inet`.  
Configure an IP address for the multilink bundle at the unit level of the link services interface. | - Next to `lsq-0/0/0`, click **Edit**.  
- Next to Unit, click **Add new entry**.  
- In the Interface unit number box, type `0`.  
- Under Family, select **Inet** and click **Configure**.  
- Next to Address, click **Add new entry**.  
- In the Source box, type the appropriate source address:  
  - On R0—`10.0.0.10/24`  
  - On R1—`10.0.0.9/24`  
- Click **OK** until you return to the Interfaces page. | - Set the appropriate source address for the interface:  
  - On R0, enter `set unit 0 family inet address 10.0.0.10/24`  
  - On R1, enter `set unit 0 family inet address 10.0.0.9/24` |
| From the **Interfaces** level in the configuration hierarchy, specify the names of the constituent links to be added to the multilink bundle—for example, `se-1/0/0` and `se-1/0/1`. | - On the Interfaces page, Next to Interface, click **Add new entry**.  
- In the Interface name box, type the name of the interface to be added to the multilink bundle—for example `se-1/0/0` or `se-1/0/1`.  
- Click **OK**.  
- Click **Edit** next to the appropriate interface name—for example, `se-1/0/0` or `se-1/0/1`. | - From the [edit] hierarchy level, add the constituent links to the multilink bundle:  
  - To add `se-1/0/0` to the multilink bundle, enter **edit interfaces se-1/0/0**  
  - To add `se-1/0/1` to the multilink bundle, enter **edit interfaces se-1/0/1** |
Table 118: Configuring an MLPPP Bundle (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create the multilink bundle by specifying a logical unit on each constituent link and defining it as an MLPPP bundle—for example, lsq-0/0/0.0.</td>
<td></td>
<td>Enter set unit 0 family mlppp bundle lsq-0/0/0.0</td>
</tr>
<tr>
<td>1.</td>
<td>Next to Unit, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>In the Interface unit number box, type 0.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Under Family, select Mlppp and click Configure.</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>In the Bundle box, type lsq-0/0/0.0.</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Click OK until you return to the Interfaces page.</td>
<td></td>
</tr>
<tr>
<td>Set the serial options to the same values for both interfaces on R0—se-1/0/0 and se-1/0/1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For more information about serial options, see “Configuring Serial Interfaces with Quick Configuration” on page 104.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> In this example, R0 is set as a data circuit-terminating equipment (DCE) device. The serial options are not set for interfaces on R1. You can set the serial options according to your network setup.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>On the Interfaces page, click Edit.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Next to the interface that you want to configure (se-1/0/0 or se-1/0/1), click Edit.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Next to Serial options, click Configure.</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>From the Clocking mode list, select dce.</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>From the Clock rate list, select 2.0mhz.</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Click OK twice.</td>
<td></td>
</tr>
</tbody>
</table>

**Enabling Link Fragmentation and Interleaving**

To configure link fragmentation and interleaving (LFI), you define the MLPPP encapsulation type and enable fragmentation and interleaving of packets by specifying the following properties—the fragmentation threshold and fragmentation—maps with a no-fragmentation knob mapped to the forwarding class of choice. In this example, a fragmentation threshold of 128 bytes is set on the MLPPP bundle that applies to all traffic on both constituent links, so that any packet larger than 128 bytes transmitted on these links is fragmented.

For more information about LFI, see “Link Fragmentation and Interleaving Overview” on page 403.

To enable LFI:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 119 on page 417 on Device R0 and Device R1.
Table 119: Enabling LFI

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Interfaces</strong> level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select <code>Configure &gt; CLI Tools &gt; Point and Click CLI</code>.</td>
<td>From the [edit] hierarchy level, enter <code>edit interfaces lsq-0/0/0</code></td>
</tr>
<tr>
<td>Specify the link services intelligent queuing interface for fragmentation.</td>
<td>2. Next to Interfaces, click <strong>Edit</strong>.</td>
<td>Enter <code>set unit 0 encapsulation multilink-ppp fragment-threshold 128</code></td>
</tr>
<tr>
<td></td>
<td>3. Under Interface, next to lsq-0/0/0, click <strong>Edit</strong>.</td>
<td></td>
</tr>
<tr>
<td>Specify the multilink encapsulation type, enable LFI, and set the fragmentation threshold for the multilink interface.</td>
<td>1. Under Unit, next to 0, click <strong>Edit</strong>.</td>
<td></td>
</tr>
<tr>
<td>Fragment Threshold—Set the maximum size, in bytes, for multilink packet fragments—for example, 128. Any nonzero value must be a multiple of 64 bytes. The value can be between 128 and 16320. The default is 0 bytes (no fragmentation).</td>
<td>2. From the Encapsulation list, select <code>multilink-ppp</code> as the encapsulation type.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. In the Fragment threshold box, type <strong>128</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

**Defining Classifiers and Forwarding Classes**

By defining classifiers you associate incoming packets with a forwarding class and loss priority. Based on the associated forwarding class, you assign packets to output queues. To configure classifiers, you specify the bit pattern for the different types of traffic. The classifier takes this bit pattern and attempts to match it to the type of packet arriving on the interface. If the information in the packet’s header matches the specified pattern, the packet is sent to the appropriate queue, defined by the forwarding class associated with the classifier.

In this example, an IP precedence classifier, `classify_input`, is assigned to all incoming traffic. The precedence bit value in the type of service (ToS) field is assumed to be **000** for all incoming data traffic and **010** for all incoming voice traffic. This classifier assigns all data traffic to Q0 and all voice traffic to Q2, and fragmentation-map maps Q2 to no-fragmentation. On a J Series device, when LFI is enabled, all traffic assigned to Q2 is treated as LFI (voice) traffic. You do not need to assign network control traffic to a queue explicitly, because it is assigned to Q3 by default.

For more information about configuring CoS components, see *Junos OS Class of Service Configuration Guide for Security Devices*.

To define classifiers and forwarding classes:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 120 on page 418 on Device R0 and Device R1.
Table 120: Defining Classifiers and Forwarding Classes

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Navigate to the **Class of service** level in the configuration hierarchy. | 1. In the J-Web interface, select **Configure > CLI Tools > Point and Click CLI**.  
2. Next to Class of service, click **Configure or Edit**. | From the [edit] hierarchy level, enter **edit class-of-service** |
| Configure a behavior aggregate (BA) classifier for classifying packets. | 1. Next to Classifiers, click **Configure**.  
2. Next to Inet precedence, click **Add new entry**.  
3. In the Name box, type **classify_input**. | Enter **edit classifiers inet-precedence classify_input** |
| In this example, you specify the default IP precedence classifier, which maps IP precedence bits to forwarding classes and loss priorities. | | |
| Assign packets with IP precedence bits 000 to the **DATA** forwarding class, and specify a low loss priority. | 1. On the Inet precedence page, next to Forwarding class, click **Add new entry**.  
2. In the Class name box, type **DATA**.  
3. Next to Loss priority, click **Add new entry**.  
4. From the Loss val list, select **low**.  
5. Next to Code points, click **Add new entry**.  
6. In the Value box, type **000**.  
7. Click **OK** until you return to the Inet precedence page. | Enter **set forwarding-class DATA loss-priority low code-points 000** |
| Assign packets with IP precedence bits 010 to the **VOICE** forwarding class, and specify a low loss priority. | 1. Next to Forwarding class, click **Add new entry**.  
2. In the Class name box, type **VOICE**.  
3. Next to Loss priority, click **Add new entry**.  
4. From the Loss val list, select **low**.  
5. Next to Code points, click **Add new entry**.  
6. In the Value box, type **010**.  
7. Click **OK** until you return to the Class of service page. | Enter **set forwarding-class VOICE loss-priority low code-points 010** |
### Table 120: Defining Classifiers and Forwarding Classes (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Assign each forwarding class one-to-one with the output queues. | 1. On the Class of service page, next to Forwarding classes, click **Configure**.  
2. Next to Queue, click **Add new entry**.  
3. In the Queue num box, type 0.  
4. In the Class name box, type **DATA**.  
5. Click **OK**.  
6. Next to Queue, click **Add new entry**.  
7. In the Queue num box, type 2.  
8. In the Class name box, type **VOICE**.  
9. Click **OK**.  
10. Next to Queue, click **Add new entry**.  
11. In the Queue num box, type 3.  
12. In the Class name box, type **NC**.  
13. Click **OK** until you return to the Class of service page. | From the [edit class-of-service] hierarchy level, enter  
set forwarding-classes queue 0 **DATA**  
set forwarding-classes queue 2 **VOICE**  
set forwarding-classes queue 3 **NC** |
| Apply the behavior aggregate classifier to the incoming interface. | 1. On the Class of service page, next to Interfaces, click **Configure** or **Edit**.  
2. Next to Interface, click **Add new entry**.  
3. In the Interface name box, type **ge-0/0/1**.  
4. Next to Unit, click **Add new entry**.  
5. In the Unit number box, type 0.  
6. Next to Classifiers, click **Configure**.  
7. Under Inet precedence, in the Classifier name box, type **classify_input**.  
8. Click **OK**. | 1. From the [edit class-of-service] hierarchy level, enter  
edit interfaces ge-0/0/1  
2. Enter  
set unit 0 classifiers inet-precedence classify_input |
| Configure fragmentation-map | - | Enter  
set class-of-service fragmentation-maps  
FM forwarding-class **VOICE**  
no-fragmentation |
Defining and Applying Scheduler Maps

By defining schedulers you configure the properties of output queues that determine the transmission service level for each queue. These properties include the amount of interface bandwidth assigned to the queue, the size of the memory buffer allocated for storing packets, and the priority of the queue. After defining schedulers you associate them with forwarding classes by means of scheduler maps. You then associate each scheduler map with an interface, thereby configuring the hardware queues and packet schedulers that operate according to this mapping.

In this example, you define and apply scheduler maps as follows:

- Enable per-unit scheduling that allows configuration of scheduler maps on the bundle.
- Create three schedulers—DATA, VOICE, and NC. Define the VOICE and NC schedulers to have a high priority and the DATA scheduler to have the default priority (low). These priority assignments allow all voice and network control traffic to be transmitted ahead of data packets. For more information about scheduling priorities, see “Queuing with LFI on J Series Devices” on page 409.
- Create a scheduler map s_map that associates these schedulers with corresponding forwarding classes.
- Apply the scheduler map to the multilink bundle and the serial interfaces.

To define and apply scheduler maps:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 121 on page 420 on Device R0 and Device R1.
3. Go on to “Applying Shaping Rates to Interfaces” on page 423.

Table 121: Defining and Applying Scheduler Maps

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Interface level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI</td>
<td>From the [edit] hierarchy level, enter edit interfaces</td>
</tr>
<tr>
<td></td>
<td>2. Next to Interfaces, click Configure or Edit.</td>
<td></td>
</tr>
</tbody>
</table>

---

Table 120: Defining Classifiers and Forwarding Classes (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attach fragmentation-map to lsq</td>
<td>-</td>
<td>Enter set class-of-service interfaces lsq-0/0/0 unit unit fragmentation-map</td>
</tr>
</tbody>
</table>

---

JUNOS Software Interfaces and Routing Configuration Guide
Table 121: Defining and Applying Scheduler Maps (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| To configure CoS components for each multilink bundle, enable per-unit scheduling on the interface. | 1. Under Interfaces, select **lsq-0/0/0**.  
2. From the Scheduler type list, select **Per unit scheduler**.  
3. Click **OK**.  
4. Under Interfaces, select **se-1/0/0**.  
5. From the Scheduler type list, select **Per unit scheduler**.  
6. Click **OK**.  
7. Under Interfaces, select **se-1/0/1**.  
8. From the Scheduler type list, select **Per unit scheduler**.  
9. Click **OK** twice. | Enter  
set lsq-0/0/0 per-unit-scheduler  
set se-1/0/0 per-unit-scheduler  
set se-1/0/1 per-unit-scheduler |
| Navigate to the Interfaces level in the Class of Service configuration hierarchy and specify the link services intelligent queuing interface to be configured. | 1. On the Class of service page, next to Interfaces, click **Configure** or **Edit**.  
2. Next to Interface, click **Add new entry**.  
3. In the Interface name box, type **lsq-0/0/0**. | From the [edit class-of-service] hierarchy level, enter  
edit interfaces lsq-0/0/0 |
| Define a scheduler map—for example, **s_map**. | 1. Next to Unit, type **Add new entry**.  
2. In the Unit number box, type **0**.  
3. In the Scheduler map box, type **s_map**.  
4. Click **OK** twice. | Enter  
set unit 0 scheduler-map s_map |
| Apply the scheduler map to the constituent links of the multilink bundle—for example, **se-1/0/0** and **se-1/0/1**. | 1. On the Class of service page, next to Interfaces, click **Configure** or **Edit**.  
2. Next to Interface, click **Add new entry**.  
3. In the Interface name box, type the name of the interface on which scheduler map s_map is to be applied—for example, **se-1/0/0** or **se-1/0/1**.  
4. Next to Unit, type **Add new entry**.  
5. In the Unit number box, type **0**.  
6. In the Scheduler map box, type **s_map**.  
7. Click **OK** twice. | 1. From the [edit] hierarchy level, specify the interface to be configured:  
   - To apply the scheduler map to **se-1/0/0**, enter  
edit interfaces se-1/0/0  
   - To apply the scheduler map to **se-1/0/1**, enter  
edit interfaces se-1/0/1  
   2. Apply the scheduler map to the logical interface.  
   set unit 0 scheduler-map s_map |
Table 121: Defining and Applying Scheduler Maps (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associate a scheduler with each forwarding class.</td>
<td>1. On the Class of service page, next to Scheduler maps, click Add new entry.</td>
<td>From the [edit class-of-service] hierarchy level, enter</td>
</tr>
<tr>
<td>DATA—A scheduler associated with the DATA forwarding class.</td>
<td>2. In the Map box, type s_map.</td>
<td>set scheduler-maps s_map forwarding-class DATA scheduler DATA</td>
</tr>
<tr>
<td>VOICE—A scheduler associated with the VOICE forwarding class.</td>
<td>3. Next to Forwarding class, click Add new entry.</td>
<td>set scheduler-maps s_map forwarding-class VOICE scheduler VOICE</td>
</tr>
<tr>
<td>NC—A scheduler associated with the NC forwarding class.</td>
<td>4. In the Class name box, type DATA.</td>
<td>set scheduler-maps s_map forwarding-class NC scheduler NC</td>
</tr>
<tr>
<td>A scheduler receives the forwarding class and loss priority settings, and queues the outgoing packet based on those settings.</td>
<td>5. In the Scheduler box, type DATA.</td>
<td></td>
</tr>
<tr>
<td>6. Click OK.</td>
<td>7. Next to Forwarding class, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td>8. In the Class name box, type VOICE.</td>
<td>9. In the Scheduler box, type VOICE.</td>
<td></td>
</tr>
<tr>
<td>10. Click OK.</td>
<td>11. Next to Forwarding class, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td>12. In the Class name box, type NC.</td>
<td>13. In the Scheduler box, type NC.</td>
<td></td>
</tr>
<tr>
<td>14. Click OK until you return to the Class of service page.</td>
<td>Define the properties of output queues for the DATA scheduler:</td>
<td>For more information about transmit rate and buffer size, see Junos OS Class of Service Configuration Guide for Security Devices.</td>
</tr>
<tr>
<td>Transmit rate—Specify a percentage of transmission capacity—49.</td>
<td>1. On the Class of service page, next to Schedulers, click Add new entry.</td>
<td>Enter</td>
</tr>
<tr>
<td>Buffer size—Specify a percentage of total buffer—49.</td>
<td>2. In the Scheduler name box, type DATA.</td>
<td>set schedulers DATA transmit-rate percent 49</td>
</tr>
<tr>
<td>Priority—Do not specify the transmission priority for the DATA scheduler to apply the default setting—low.</td>
<td>3. Next to Transmit rate, click Configure.</td>
<td>set schedulers DATA buffer-size percent 49</td>
</tr>
<tr>
<td>For more information about transmit rate and buffer size, see Junos OS Class of Service Configuration Guide for Security Devices.</td>
<td>4. From the Transmit rate choice list, select Percent.</td>
<td></td>
</tr>
<tr>
<td>5. In the Percent box, type 49.</td>
<td>6. Click OK.</td>
<td></td>
</tr>
<tr>
<td>7. Next to Buffer size, click Configure.</td>
<td>8. From the Buffer size choice list, select Percent.</td>
<td></td>
</tr>
<tr>
<td>9. In the Percent box, type 49.</td>
<td>10. Click OK twice.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 121: Defining and Applying Scheduler Maps (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the properties of output queues for the VOICE scheduler:</td>
<td></td>
<td>Enter</td>
</tr>
<tr>
<td>■ Transmit rate—Specify a percentage of transmission capacity—50.</td>
<td>On the Class of service page, next to Schedulers, click Add new entry.</td>
<td>set schedulers VOICE transmit-rate percent 50</td>
</tr>
<tr>
<td>■ Buffer size—Specify a percentage of total buffer—5.</td>
<td>2. In the Scheduler name box, type VOICE.</td>
<td>set schedulers VOICE buffer-size percent 5</td>
</tr>
<tr>
<td>■ Priority—Specify a transmission priority—high.</td>
<td>3. Next to Transmit rate, click Configure.</td>
<td>set schedulers VOICE priority high</td>
</tr>
<tr>
<td></td>
<td>4. From the Transmit rate choice list, select Percent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. In the Percent box, type 50.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Click OK.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. Next to Buffer size, click Configure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. From the Buffer size choice list, select Percent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9. In the Percent box, type 5.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10. Click OK.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>11. In the Priority box, type high.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12. Click OK.</td>
<td></td>
</tr>
</tbody>
</table>

Define the properties of output queues for the NC scheduler:

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Transmit rate—Specify a percentage of transmission capacity—1.</td>
<td>On the Class of service page, next to Schedulers, click Add new entry.</td>
<td>Enter</td>
</tr>
<tr>
<td>■ Buffer size—Specify a percentage of total buffer—1.</td>
<td>2. In the Scheduler name box, type NC.</td>
<td>set schedulers NC transmit-rate percent 1</td>
</tr>
<tr>
<td>■ Priority—Specify a transmission priority—high.</td>
<td>3. Next to Transmit rate, click Configure.</td>
<td>set schedulers NC buffer-size percent 1</td>
</tr>
<tr>
<td></td>
<td>4. From the Transmit rate choice list, select Percent.</td>
<td>set schedulers NC priority high</td>
</tr>
<tr>
<td></td>
<td>5. In the Percent box, type 1.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Click OK.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. Next to Buffer size, click Configure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. From the Buffer size choice list, select Percent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9. In the Percent box, type 1.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10. Click OK.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>11. In the Priority box, type high.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12. Click OK.</td>
<td></td>
</tr>
</tbody>
</table>

### Applying Shaping Rates to Interfaces

To control the voice traffic latency within acceptable limits, you configure the shaping rate on constituent links of the MLPPP bundle. Shaping rate at the interface level is
required only when you enable LFI. To apply shaping rates to interfaces, you have to first enable per-unit scheduling. For information about shaping rates and LFI, see “Configuring CoS Components with LFI” on page 409.

You must configure the shaping rate to be equal to the combined physical interface bandwidth for the constituent links. In this example, the combined bandwidth capacity of the two constituent links—se-1/0/0 and se-1/0/1—is 2 Mbps. Hence, configure a shaping rate of 2 Mbps on each constituent link.

To apply a shaping rate to the constituent links of the multilink bundle:

1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 122 on page 424 on Device R0 and Device R1.
3. Go on to “Verifying the Link Services intelligent queuing Interface Configuration” on page 431, to verify your configuration.

Table 122: Applying Shaping Rate to Interfaces

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Class of service level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit class-of-service</td>
</tr>
<tr>
<td></td>
<td>2. Next to Class of service, click Edit.</td>
<td></td>
</tr>
</tbody>
</table>

Apply the shaping rate to the constituent links of the multilink bundle—for example, se-1/0/0 and se-1/0/1. The shaping rate specifies the amount of bandwidth to be allocated for this multilink bundle.

1. Under Interfaces, select the name of the interface on which you want to apply the shaping rate—se-1/0/0 or se-1/0/1.
2. Next to Unit 0, click Edit.
3. Select Shaping rate, and click Configure.
4. From the Shaping rate choice list, select Rate.
5. In the Rate box, type 2000000.
6. Click OK.

Configuring MLFR FRF.15 Bundles

J Series devices support Multilink Frame Relay end-to-end (MLFR FRF.15) on the link services intelligent queuing interface lsq-0/0/0.

With MLFR FRF.15, multilink bundles are configured as logical units on the link services intelligent queuing interface, such as lsq-0/0/0.0. MLFR FRF.15 bundles combine multiple permanent virtual circuits (PVCs) into one aggregated virtual circuit (AVC). This process provides fragmentation over multiple PVCs on one end and
reassembly of the AVC on the other end. For more information about multilink bundles, see “Multilink Bundles Overview” on page 402.

You can configure LFI and CoS with MLFR in the same way that you configure them with MLPPP. For information about configuring LFI and CoS, see “Configuring MLPPP Bundles and LFI on Serial Links” on page 413.

In this example, you aggregate two T1 links to create an MLFR FRF.15 bundle on two J Series devices—Device R0 and Device R1.

To configure an MLFR FRF.15 bundle:
1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor on Device R0 and Device R1.
2. Perform the configuration tasks described in Table 123 on page 425.
3. If you are finished configuring the device, commit the configuration.
4. Go on to “Verifying the Link Services intelligent queuing Interface Configuration” on page 431, to verify your configuration.

<table>
<thead>
<tr>
<th>Table 123: Configuring MLFR FRF.15 Bundles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Task</strong></td>
</tr>
<tr>
<td>Navigate to the Interfaces level in the configuration hierarchy. Specify the link services intelligent queuing interface as an interface to be configured.</td>
</tr>
</tbody>
</table>
Table 123: Configuring MLFR FRF.15 Bundles (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a logical unit on the lsq-0/0/0 interface, and define the family type—for example, Inet.</td>
<td>1. On the Interfaces page, next to lsq-0/0/0, click <strong>Edit</strong>.</td>
<td>Set the appropriate source address for the interface:</td>
</tr>
<tr>
<td></td>
<td>2. Next to Unit, click <strong>Add new entry</strong>.</td>
<td>■ On R0, enter set unit 0 family inet address 10.0.0.4/24</td>
</tr>
<tr>
<td></td>
<td>3. In the Interface unit number box, type 0.</td>
<td>■ On R1, enter set unit 0 family inet address 10.0.0.5/24</td>
</tr>
<tr>
<td></td>
<td>4. Under Family, select <strong>Inet</strong> and click <strong>Configure</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Next to Address, click <strong>Add new entry</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. In the Source box, type the appropriate source address:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ On R0—10.0.0.4/24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ On R1—10.0.0.5/24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>OK</strong> until you return to the Interfaces page.</td>
<td></td>
</tr>
<tr>
<td>Define the multilink bundle as an MLFR FRF.15 bundle by specifying the Multilink Frame Relay end-to-end encapsulation type.</td>
<td>1. On the Interfaces page, next to lsq-0/0/0, click <strong>Edit</strong>.</td>
<td>From the [edit interfaces lsq-0/0/0] hierarchy level, enter</td>
</tr>
<tr>
<td></td>
<td>2. Under Unit, next to 0, click <strong>Edit</strong>.</td>
<td>set unit 0 encapsulation frame-relay-end-to-end</td>
</tr>
<tr>
<td></td>
<td>3. From the Encapsulation list, select <strong>multilink-frame-relay-end-to-end</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong> until you return to the Interfaces page.</td>
<td></td>
</tr>
<tr>
<td>Specify the names of the constituent links to be added to the multilink bundle—for example, t1-2/0/0 and t1-2/0/1.</td>
<td>1. On the Interfaces page, next to Interface, click <strong>Add new entry</strong>.</td>
<td>1. From the [edit] hierarchy level, enter</td>
</tr>
<tr>
<td>Define the Frame Relay encapsulation type.</td>
<td>2. In the Interface name box, type the name of the interface:</td>
<td>■ For configuring t1-2/0/0</td>
</tr>
<tr>
<td></td>
<td>■ To configure t1-2/0/0, type t1-2/0/0.</td>
<td>edit interfaces t1-2/0/0</td>
</tr>
<tr>
<td></td>
<td>■ To configure t1-2/0/1, type t1-2/0/1.</td>
<td>■ For configuring t1-2/0/1</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>OK</strong>.</td>
<td>edit interfaces t1-2/0/1</td>
</tr>
<tr>
<td></td>
<td>4. Next to the interface you want to configure, click <strong>Edit</strong>.</td>
<td>2. Enter</td>
</tr>
</tbody>
</table>
|                                                                     | 5. From the Encapsulation list, select **frame-relay**.                                   |    set encapsulation frame-relay
Table 123: Configuring MLFR FRF.15 Bundles (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define R0 to be a data circuit-terminating equipment (DCE) device. R1 performs as a data terminal equipment (DTE) device, which is the default with Frame Relay encapsulation. For more information about DCE and DTE, see “Serial Interface Overview” on page 28.</td>
<td>On R0 only, select Dce.</td>
<td>On R0 only, enter set dce</td>
</tr>
</tbody>
</table>

On the logical unit level of the interface, specify the data-link connection identifier (DLCI). The DLCI field identifies which logical circuit the data travels over. DLCI is a value from 16 through 1022—for example, 100. (Numbers 1 through 15 are reserved for future use.) Specify the multilink bundle to which the interface is to be added as a constituent link—lsq-0/0/0.0. | 1. Next to Unit, click Add new entry. | Enter set unit 0 dlc 100 family mlfr-end-to-end bundle lsq-0/0/0.0 |
| | 2. In the Interface unit number box, type 0. | |
| | 3. In the Dlci box, type 100. | |
| | 4. Under Family, select mlfr-end-to-end and click Configure. | |
| | 5. In the Bundle box, type lsq-0/0/0.0. | |
| | 6. Click OK. | |

Configuring MLFR FRF.16 Bundles

J Series devices support Multilink Frame Relay (MLFR) user-to-network interface (UNI) network-to-network interface (NNI) (MLFR FRF.16) on the link services intelligent queuing interface lsq-0/0/0.

MLFR FRF.16 configures multilink bundles as channels on the link services intelligent queuing interface, such as lsq-0/0/0:0. A multilink bundle carries Frame Relay permanent virtual circuits (PVCs), identified by their data-link connection identifiers (DLCIs). Each DLCI is configured at the logical unit level of the link services intelligent queuing interface and is also referred as a logical interface. Packet fragmentation and reassembly occur on each virtual circuit. For more information about multilink bundles, see “Multilink Bundles Overview” on page 402.

You can configure LFI and CoS with MLFR in the same way that you configure them with MLPPP. For information about configuring LFI and CoS, see “Configuring MLPPP Bundles and LFI on Serial Links” on page 413.

In this example, you aggregate two T1 interfaces to create an MLFR FRF.16 bundle on two J Series devices—Device R0 and Device R1.

To configure an MLFR FRF.16 bundle:
1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor on Device R0 and Device R1.
2. Perform the configuration tasks described in Table 124 on page 428.
3. If you are finished configuring the device, commit the configuration.

4. Go on to “Verifying the Link Services intelligent queuing Interface Configuration” on page 431, to verify your configuration.

Table 124: Configuring MLFR FRF.16 Bundles

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Chassis level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter edit chassis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Next to Chassis, click Configure or Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td></td>
</tr>
<tr>
<td>Specify the number of multilink frame relay UNI NNI (FRF.16) bundles to be created on the interface. You can specify a number from 1 through 255.</td>
<td>Next to Fpc, click Add new entry.</td>
<td>Enter set fpc 0 pic 0 mlfr-uni-nni-bundles 1</td>
</tr>
<tr>
<td></td>
<td>In the Slot box, type 0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Next to Pic, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the Slot box, type 0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the Mlfr uni nni bundles box, type 1.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Click OK.</td>
<td></td>
</tr>
<tr>
<td>Specify the channel to be configured as a multilink bundle.</td>
<td>From the [edit] hierarchy level, enter edit interfaces lsq-0/0/0:0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Next to Interfaces, click Configure or Edit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Next to Interface, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the Interface name box, type lsq-0/0/0:0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Click OK.</td>
<td></td>
</tr>
<tr>
<td>Define the multilink bundle as an MLFR FRF.16 bundle by specifying the Multilink Frame Relay UNI NNI encapsulation type.</td>
<td>Enter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Next to lsq-0/0/0:0, click Edit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>From the Encapsulation list, select multilink-frame-relay-uni-nni.</td>
<td></td>
</tr>
<tr>
<td>Define R0 to be a data circuit-terminating equipment (DCE) device. R1 performs as a data terminal equipment (DTE) device, which is the default with Frame Relay encapsulation.</td>
<td>On R0 only, select Dce.</td>
<td>On R0 only, enter set dce</td>
</tr>
<tr>
<td>For more information about DCE and DTE, see “Serial Interface Overview” on page 28</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 124: Configuring MLFR FRF.16 Bundles (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a logical unit on the multilink bundle lsq-0/0/0:0, and define the family type—for example, inet.</td>
<td>1. Next to Unit, click <strong>Add new entry</strong>.</td>
<td>Set the appropriate address for the interface:</td>
</tr>
<tr>
<td>Assign a data link connection identifier (DLCI) to the multilink bundle. The DLCI field identifies which logical circuit the data travels over. DLCI is a value from 16 through 1022—for example, 400. (Numbers 1 through 15 are reserved for future use.)</td>
<td>2. In the Interface unit number box, type 0.</td>
<td>■ On R0, enter set unit 0 dlci 400 family inet address 10.0.0.10/24</td>
</tr>
<tr>
<td>Assign an IP address to the multilink bundle.</td>
<td>3. In the Dlci box, type 400.</td>
<td>■ On R1, enter set unit 0 dlci 400 family inet address 10.0.0.9/24</td>
</tr>
<tr>
<td>Create the T1 interfaces that are to be added as constituent links to the multilink bundle—t1-2/0/0 and t1-2/0/1.</td>
<td>4. Under Family, select <strong>Inet</strong> and click <strong>Configure</strong>.</td>
<td>5. Next to Address, click <strong>Add new entry</strong>.</td>
</tr>
<tr>
<td>Define the Frame Relay encapsulation type.</td>
<td>5. In the Source box, type the appropriate source address:</td>
<td>In the Source box, type the appropriate source address:</td>
</tr>
<tr>
<td></td>
<td>■ On R0—10.0.0.10/24</td>
<td>■ On R0—10.0.0.10/24</td>
</tr>
<tr>
<td>Specify the multilink bundle to which the interface is to be added as a constituent link—lsq-0/0/0:0.</td>
<td>6. In the Source box, type the appropriate source address:</td>
<td>■ On R1—10.0.0.9/24</td>
</tr>
<tr>
<td></td>
<td>■ On R1—10.0.0.9/24</td>
<td>7. Click <strong>OK</strong> until you return to the Interfaces page.</td>
</tr>
</tbody>
</table>
**Configuring CRTP**

Compressed Real-Time Transport Protocol (CRTP) is typically used for compressing voice and video packets. You can configure CRTP with LFI on the link services interface of a J Series device.

On the J Series device, CRTP can be configured as a compression device on a T1 or E1 interface with PPP encapsulation, using the link services interface.

For more information about configuring CRTP on a single link, see the *Junos Network Interfaces Configuration Guide* and the *Junos Services Interfaces Configuration Guide*.

To configure CRTP on the device:
1. Navigate to the top of the interfaces configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 125 on page 430.
3. If you are finished configuring the device, commit the configuration.

---

**Table 125: Adding CRTP to a T1 or E1 Interface**

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Interfaces</strong> level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select <strong>Configure &gt; CLI Tools &gt; Point and Click CLI</strong>&lt;br&gt;2. Next to Interfaces, click <strong>Configure</strong> or <strong>Edit</strong>.</td>
<td>From the [edit] hierarchy level, enter <strong>edit interfaces interface-name</strong></td>
</tr>
<tr>
<td>Select an E1 or T1 interface—for example, <strong>t1-1/0/0</strong>. <strong>Set PPP as the type of encapsulation for the physical interface.</strong></td>
<td>1. Next to a T1 or E1 interface, click <strong>Edit</strong>.&lt;br&gt;2. From the Encapsulation list, select <strong>ppp</strong> as the encapsulation type.&lt;br&gt;3. Next to Unit, click <strong>Add new entry</strong>&lt;br&gt;4. In the Interface unit number box, type <strong>0</strong>.</td>
<td>1. Enter <strong>set encapsulation ppp</strong>&lt;br&gt;2. Enter <strong>edit unit 0</strong></td>
</tr>
<tr>
<td>Add the link services intelligent queuing interface, <strong>lsq-0/0/0.0</strong>, to the physical interface.</td>
<td>1. In the Compression device box, enter <strong>lsq-0/0/0.0</strong>.&lt;br&gt;2. Click <strong>OK</strong> until you return to the Interfaces page.</td>
<td>Enter <strong>set compression-device lsq-0/0/0.0</strong></td>
</tr>
<tr>
<td>Add the link services intelligent queuing interface, <strong>lsq-0/0/0.0</strong>, to the device.</td>
<td>1. Next to Interface, click <strong>Add new entry</strong>.&lt;br&gt;2. In the Interface name box, type <strong>lsq-0/0/0.0</strong>.&lt;br&gt;3. Click <strong>OK</strong> to return to the Interfaces page.&lt;br&gt;4. On the main Interface page, next to lsq-0/0/0.0, click <strong>Edit</strong>&lt;br&gt;5. Next to Unit, click <strong>Add new entry</strong>&lt;br&gt;6. In the Interface unit number box, type <strong>0</strong>.</td>
<td>From the [edit interfaces] hierarchy level, enter <strong>edit interfaces lsq-0/0/0/0 unit 0</strong></td>
</tr>
</tbody>
</table>
Table 125: Adding CRTP to a T1 or E1 Interface (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the link services intelligent queuing interface, lsq-0/0/0, properties.</td>
<td>1. Next to Compression, select yes, and then click Configure.</td>
<td>Enter set compression rtp f-max-period 2500 port minimum 2000 maximum 64009</td>
</tr>
<tr>
<td>F-max period—Maximum number of compressed packets allowed between transmission of full headers. It has a range from 1 to 65535.</td>
<td>2. Select RTP, and then click Configure.</td>
<td></td>
</tr>
<tr>
<td>Maximum and Minimum—UDP port values from 1 to 65536 reserve these ports for RTP compression. CRTP is applied to network traffic on ports within this range. This feature is applicable only to voice services interfaces.</td>
<td>3. In the F-Max period box, type 2500.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Select Port, then click Configure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. In the Minimum value box, type 2000.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. In the Maximum value box, type 64009.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. Click OK.</td>
<td></td>
</tr>
</tbody>
</table>

Verifying the Link Services intelligent queuing Interface Configuration

To verify a link services configuration, perform the following tasks:

- Displaying Multilink Bundle Configurations on page 431
- Displaying Link Services CoS Configurations on page 432
- Verifying Link Services Interface Statistics on page 434
- Verifying Link Services CoS on page 437

**Displaying Multilink Bundle Configurations**

**Purpose**  Verify the multilink bundle configuration.

**Action**  From the J-Web interface, select Configure > CLI Tools > CLI Viewer. Alternatively, from configuration mode in the CLI, enter the show interfaces command.

The sample output in this section displays the multilink bundle configurations provided in “Configuring MLPPP Bundles and LFI on Serial Links” on page 413.

**NOTE:** The MLFR FRF.15 and MLFR FRF.16 configurations are not displayed in this section, but you can display MLFR configurations in the same manner.

```
[edit]
user@R0# show interfaces
interfaces {
    lsq-0/0/0 {
        per-unit-scheduler;
        unit 0 {
            encapsulation multilink-ppp;
            fragment-threshold 128;
            family inet {
```
address 10.0.0.10/24;
}
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 192.1.1.1/24;
        }
    }
}
se-1/0/0 {
    per-unit-scheduler;
    dce-options {
        clocking-mode dce;
        clocking-rate 2.0mhz;
    }
    unit 0 {
        family mlppp {
            bundle lsq-0/0/0.0;
        }
    }
}
se-1/0/1 {
    per-unit-scheduler;
    dce-options {
        clocking-mode dce;
        clocking-rate 2.0mhz;
    }
    unit 0 {
        family mlppp {
            bundle lsq-0/0/0.0;
        }
    }
}

**Meaning**  Verify that the output shows the intended multilink bundle configurations.

**Related Topics**  For more information about the format of a configuration file, see the *J-Web Interface User Guide* or the *Junos CLI User Guide*.

### Displaying Link Services CoS Configurations

**Purpose**  Displaying the CoS configurations on the link services interface.

**Action**  From the J-Web interface, select **Configure > CLI Tools > CLI Viewer**. Alternatively, from the configuration mode in the CLI, enter the `show class-of-service` command.

The sample output in this section displays the CoS configurations provided in “Configuring MLPPP Bundles and LFI on Serial Links” on page 413.
[edit]
user@R0# show class-of-service
classifiers {
  inet-precedence classify_input {
    forwarding-class DATA {
      loss-priority low code-points 000;
    }
    forwarding-class VOICE {
      loss-priority low code-points 010;
    }
  }
}
forwarding-classes {
  queue 0 DATA;
  queue 2 VOICE;
  queue 3 NC;
}
interfaces {
  ls-0/0/0 {
    unit 0 {
      scheduler-map s_map;
      fragmentation-maps fm;
    }
  }
  ge-0/0/1 {
    unit 0 {
      classifiers {
        inet-precedence classify_input
      }
    }
  }
  se-1/0/0 {
    unit 0 {
      scheduler-map s_map;
      shaping-rate 2000000;
    }
  }
  se-1/0/1 {
    unit 0 {
      scheduler-map s_map;
      shaping-rate 2000000;
    }
  }
}
scheduler-maps {
  s_map {
    forwarding-class DATA scheduler DATA;
    forwarding-class VOICE scheduler VOICE;
    forwarding-class NC scheduler NC;
  }
}
schedulers {
  DATA {
    transmit-rate percent 49;
    buffer-size percent 49;
  }
}
Meaning Verify that the output shows the intended CoS configurations.

Related Topics For more information about the format of a configuration file, see the J-Web Interface User Guide or the Junos CLI User Guide.

Verifying Link Services Interface Statistics

Purpose Verify the link services interface statistics.

Action The sample output provided in this section is based on the configurations provided in “Configuring MLPPP Bundles and LFI on Serial Links” on page 413. To verify that the constituent links are added to the bundle correctly and the packets are fragmented and transmitted correctly, take the following actions:

1. On Device R0 and Device R1, the two J Series devices used in this example, configure MLPPP and LFI as described in “Configuring MLPPP Bundles and LFI on Serial Links” on page 413.

2. From the CLI, enter the ping command to verify that a connection is established between R0 and R1.

3. Transmit 10 data packets, 200 bytes each, from R0 to R1.

4. On R0, from the CLI, enter the show interfaces interface-name statistics command.

Sample Output

user@R0> show interfaces lsq-0/0/0 statistics detail
Physical interface: lsq-0/0/0, Enabled, Physical link is Up
Interface index: 134, SNMP ifIndex: 29, Generation: 135
Link-level type: LinkService, MTU: 1504
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps
Last flapped : 2006-06-23 11:36:23 PDT (03:38:43 ago)
Statistics last cleared: 2006-06-23 15:13:12 PDT (00:01:54 ago)
Traffic statistics:

VOICE {
  transmit-rate percent 50;
  buffer-size percent 5;
  priority high;
}
NC {
  transmit-rate percent 1;
  buffer-size percent 1;
  priority high;
}
fragmentation-maps fm {
  forwarding-class {
    VOICE {
      no-fragmentation;
    }
  }
}
Meaning  This output shows a summary of interface information. Verify the following information:

- **Physical interface**—The physical interface is Enabled. If the interface is shown as Disabled, do either of the following:
  
  - In the CLI configuration editor, delete the disable statement at the [edit interfaces interface-name] level of the configuration hierarchy.
In the J-Web configuration editor, clear the Disable check box on the Interfaces > interface-name page.

- **Physical link**—The physical link is Up. A link state of Down indicates a problem with the interface module, interface port, or physical connection (link-layer errors).
- **Last flapped**—The Last Flapped time is an expected value. The Last Flapped time indicates the last time the physical interface became unavailable and then available again. Unexpected flapping indicates likely link-layer errors.
- **Traffic statistics**—Number and rate of bytes and packets received and transmitted on the interface. Verify that the number of inbound and outbound bytes and packets match the expected throughput for the physical interface. To clear the statistics and see only new changes, use the clear interfaces statistics interface-name command.
- **Queue counters**—Name and number of queues are as configured. This sample output shows that 10 data packets were transmitted and no packets were dropped.
- **Logical interface**—Name of the multilink bundle you configured—lsq-0/0/0.0.
- **Bundle options**—Fragmentation threshold is correctly configured, and fragment interleaving is enabled.
- **Bundle errors**—Any packets and fragments dropped by the bundle.
- **Statistics**—The fragments and packets are received and transmitted correctly by the device. All references to traffic direction (input or output) are defined with respect to the device. Input fragments received by the device are assembled into input packets. Output packets are segmented into output fragments for transmission out of the device.

In this example, 10 data packets of 200 bytes were transmitted. Because the fragmentation threshold is set to 128 bytes, all data packets were fragmented into two fragments. The sample output shows that 10 packets and 20 fragments were transmitted correctly.

- **Link**—The constituent links are added to this bundle and are receiving and transmitting fragments and packets correctly. The combined number of fragments transmitted on the constituent links must be equal to the number of fragments transmitted from the bundle. This sample output shows that the bundle transmitted 20 fragments and the two constituent links se-1/0/0.0 and se-1/0/1.0.0 correctly transmitted $10+10=20$ fragments.

- **Destination** and **Local**—IP address of the remote side of the multilink bundle and the local side of the multilink bundle. This sample output shows that the destination address is the address on R1 and the local address is the address on R0.

**Related Topics** For a complete description of show interfaces output, see the Junos Interfaces Command Reference.
Verifying Link Services CoS

Purpose
Verify CoS configurations on the link services interface.

Action
From the CLI, enter the following commands:

- show class-of-service interface interface-name
- show class-of-service classifier name classifier-name
- show class-of-service scheduler-map scheduler-map-name

The sample output provided in this section is based on the configurations provided in “Configuring MLPPP Bundles and LFI on Serial Links” on page 413.

Sample Output

user@R0> show class-of-service interface lsq-0/0/0
Physical interface: lsq-0/0/0, Index: 136
Queues supported: 8, Queues in use: 4
Scheduler map: [default], Index: 2
Input scheduler map: [default], Index: 3
Chassis scheduler map: [default-chassis], Index: 4
Logical interface: lsq-0/0/0.0, Index: 69

Object               Name                    Type              Index
Scheduler-map        s_map                   Output            16206
Classifier          ipprec-compatibility     ip                   12

user@R0> show class-of-service interface ge-0/0/1
Physical interface: ge-0/0/1, Index: 140
Queues supported: 8, Queues in use: 4
Scheduler map: [default], Index: 2
Input scheduler map: [default], Index: 3
Logical interface: ge-0/0/1.0, Index: 68

Object               Name                   Type         Index
Classifier         classfy_input            ip           4330

user@R0> show class-of-service classifier name classify_input
Classifier: classify_input, Code point type: inet-precedence, Index: 4330

Code point       Forwarding class            Loss priority
000                  DATA                       low
010                  VOICE                      low

user@R0> show class-of-service scheduler-map s_map
Scheduler map: s_map, Index: 16206
Scheduler: DATA, Forwarding class: DATA, Index: 3810
Transmit rate: 49 percent, Rate Limit: none, Buffer size: 49 percent, Priority:low

Drop profiles:
Loss priority     Protocol     Index     Name
Low               any          1        [default-drop-profile]
Medium low        any          1        [default-drop-profile]
Medium high       any          1        [default-drop-profile]
High              any          1        [default-drop-profile]
### Scheduler: VOICE, Forwarding class: VOICE, Index: 43363

Transmit rate: 50 percent, Rate Limit: none, Buffer size: 5 percent, Priority: high

#### Drop profiles:

<table>
<thead>
<tr>
<th>Loss priority</th>
<th>Protocol</th>
<th>Index</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>any</td>
<td>1</td>
<td>[default-drop-profile]</td>
</tr>
<tr>
<td>Medium low</td>
<td>any</td>
<td>1</td>
<td>[default-drop-profile]</td>
</tr>
<tr>
<td>Medium high</td>
<td>any</td>
<td>1</td>
<td>[default-drop-profile]</td>
</tr>
<tr>
<td>High</td>
<td>any</td>
<td>1</td>
<td>[default-drop-profile]</td>
</tr>
</tbody>
</table>

### Scheduler: NC, Forwarding class: NC, Index: 2435

Transmit rate: 1 percent, Rate Limit: none, Buffer size: 1 percent, Priority: high

#### Drop profiles:

<table>
<thead>
<tr>
<th>Loss priority</th>
<th>Protocol</th>
<th>Index</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>any</td>
<td>1</td>
<td>[default-drop-profile]</td>
</tr>
<tr>
<td>Medium low</td>
<td>any</td>
<td>1</td>
<td>[default-drop-profile]</td>
</tr>
<tr>
<td>Medium high</td>
<td>any</td>
<td>1</td>
<td>[default-drop-profile]</td>
</tr>
<tr>
<td>High</td>
<td>any</td>
<td>1</td>
<td>[default-drop-profile]</td>
</tr>
</tbody>
</table>

**Meaning**

These output examples show a summary of configured CoS components. Verify the following information:

- **Logical Interface**—Name of the multilink bundle and the CoS components applied to the bundle. The sample output shows that the multilink bundle is lsq 0/0/0.0, and the CoS scheduler-map s_map is applied to it.

- **Classifier**—Code points, forwarding classes, and loss priorities assigned to the classifier. The sample output shows that a default classifier, ipprec-compatibility, was applied to the lsq 0/0/0 interface and the classifier classify_input was applied to the ge 0/0/1 interface.

- **Scheduler**—Transmit rate, buffer size, priority, and loss priority assigned to each scheduler. The sample output displays the data, voice, and network control schedulers with all the configured values.

**Related Topics**

For complete descriptions of `show class-of-service` commands and output, see the *Junos System Basics and Services Command Reference*.
Frequently Asked Questions About the Link Services Interface

Use answers to the following questions to solve configuration problems on a link services interface:

- Which CoS Components Are Applied to the Constituent Links? on page 439
- What Causes Jitter and Latency on the Multilink Bundle? on page 440
- Are LFI and Load Balancing Working Correctly? on page 441
- Why Are Packets Dropped on a PVC Between a J Series Device and Another Vendor? on page 447

Which CoS Components Are Applied to the Constituent Links?

**Problem**—I have configured a multilink bundle, but I also have traffic without MLPPP encapsulation passing through constituent links of the multilink bundle. Do I apply all CoS components to the constituent links, or is applying them to the multilink bundle enough?

**Solution**—On a J Series device you can apply a scheduler map to the multilink bundle and its constituent links. Although you can apply several CoS components with the scheduler map, configure only the ones that are required. We recommend that you keep the configuration on the constituent links simple to avoid unnecessary delay in transmission.

Table 126 on page 439 shows the CoS components to be applied on a multilink bundle and its constituent links. For more information, see the *Junos Class of Service Configuration Guide*.

<table>
<thead>
<tr>
<th>Cos Component</th>
<th>Multilink Bundle</th>
<th>Constituent Links</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classifier</td>
<td>Yes</td>
<td>No</td>
<td>CoS classification takes place on the incoming side of the interface, not on the transmitting side, so no classifiers are needed on constituent links.</td>
</tr>
<tr>
<td>Forwarding class</td>
<td>Yes</td>
<td>No</td>
<td>Forwarding class is associated with a queue, and the queue is applied to the interface by a scheduler map. The queue assignment is predetermined on the constituent links. All packets from Q2 of the multilink bundle are assigned to Q2 of the constituent link, and packets from all the other queues are queued to Q0 of the constituent link.</td>
</tr>
</tbody>
</table>
Table 126: CoS Components Applied on Multilink Bundles and Constituent Links (continued)

<table>
<thead>
<tr>
<th>Cos Component</th>
<th>Multilink Bundle</th>
<th>Constituent Links</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduler map</td>
<td>Yes</td>
<td>Yes</td>
<td>Apply scheduler maps on the multilink bundle and the constituent links, as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ Transmit rate—Make sure that the relative order of the transmit rate configured on Q0 and Q2 is the same on the constituent links as on the multilink bundle.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ Scheduler priority—Make sure that the relative order of the scheduler priority configured on Q0 and Q2 is the same on the constituent links as on the multilink bundle.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ Buffer size—Because all non-LFI packets from the multilink bundle transit Q0 of constituent links, make sure that the buffer size on Q0 of the constituent links is large enough.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>■ RED drop profile—Configure a RED drop profile on the multilink bundle only. Configuring the RED drop profile on the constituent links applies a back pressure mechanism that changes the buffer size and introduces variation. Because this behavior might cause fragment drops on the constituent links, make sure to leave the RED drop profile at the default settings on the constituent links.</td>
</tr>
<tr>
<td>Shaping rate for a per-unit scheduler or an interface-level scheduler</td>
<td>No</td>
<td>Yes</td>
<td>Because per-unit scheduling is applied only at the end point, apply this shaping rate to the constituent links only. Any configuration applied earlier is overwritten by the constituent link configuration.</td>
</tr>
<tr>
<td>Transmit-rate exact or queue-level shaping</td>
<td>Yes</td>
<td>No</td>
<td>The interface-level shaping applied on the constituent links overrides any shaping on the queue. Thus apply transmit-rate exact shaping on the multilink bundle only.</td>
</tr>
<tr>
<td>Rewrite rules</td>
<td>Yes</td>
<td>No</td>
<td>Rewrite bits are copied from the packet into the fragments automatically during fragmentation. Thus what you configure on the multilink bundle is carried on the fragments to the constituent links.</td>
</tr>
<tr>
<td>Virtual channel group</td>
<td>Yes</td>
<td>No</td>
<td>Virtual channel groups are identified through firewall filter rules that are applied on packets only before the multilink bundle. Thus you do not need to apply the virtual channel group configuration to the constituent links.</td>
</tr>
</tbody>
</table>

What Causes Jitter and Latency on the Multilink Bundle?

**Problem**—To test jitter and latency on a J Series device, I sent three streams of IP packets. All packets have the same IP precedence settings. After I configured LFI and CRTP, the latency increased even over a non-congested link. How can I reduce jitter and latency?

**Solution**—To reduce jitter and latency, do the following:
1. Make sure that you have configured a shaping rate on each constituent link.

2. Make sure that you have not configured a shaping rate on the link services interface.

3. Make sure that the configured shaping rate value is equal to the physical interface bandwidth. For more information, see “Applying Shaping Rates to Interfaces” on page 423.

4. If shaping rates are configured correctly, and jitter still persists, contact the Juniper Networks Technical Assistance Center (JTAC). (See “Requesting Technical Support” on page xl.)

**Are LFI and Load Balancing Working Correctly?**

**Problem**—I have a single network that supports multiple services. My network transmits data and delay-sensitive voice traffic. I configured MLPPP and LFI to make sure that voice packets are transmitted across the network with very little delay and jitter. How can I find out if voice packets are being treated as LFI packets and load balancing is performed correctly?

**Solution**—When LFI is enabled, data (non-LFI) packets are encapsulated with an MLPPP header and fragmented to packets of a specified size. The delay-sensitive, voice (LFI) packets are PPP-encapsulated and interleaved between data packet fragments. Queuing and load balancing are performed differently for LFI and non-LFI packets.

To verify that LFI is performed correctly, determine that packets are fragmented and encapsulated as configured. After you know whether a packet is treated as an LFI packet or a non-LFI packet, you can confirm whether the load balancing is performed correctly.

**Solution Scenario**—Suppose two J Series devices R0 and R1 are connected by a multilink bundle lsq-0/0/0.0 that aggregates two serial links, se-1/0/0 and se-1/0/1. On R0 and R1, MLPPP and LFI are enabled on the link services interface and the fragmentation threshold is set to 128 bytes.

In this example, we used a packet generator to generate voice and data streams. You can use the packet capture feature to capture and analyze the packets on the incoming interface. For more information, see the *Junos OS Administration Guide for Security Devices*.

The following two data streams were sent on the multilink bundle:

- 100 data packets of 200 bytes (larger than the fragmentation threshold)
- 500 data packets of 60 bytes (smaller than the fragmentation threshold)

The following two voice streams were sent on the multilink bundle:

- 100 voice packets of 200 bytes from source port 100
- 300 voice packets of 200 bytes from source port 200
To confirm that LFI and load balancing are performed correctly, first verify that the link services interface is performing packet fragmentation as configured. Second, verify that the interface is encapsulating packets as configured. Finally, use the results to verify load balancing.

**NOTE:** Only the significant portions of command output are displayed and described in this example. For more information, see “Verifying the Link Services intelligent queuing Interface Configuration” on page 431.

---

**Step 1: Verifying Packet Fragmentation**

From the CLI, enter the `show interfaces lsq-0/0/0` command, to check that large packets are fragmented correctly.

```
user@R0#> show interfaces lsq-0/0/0

Physical interface: lsq-0/0/0, Enabled, Physical link is Up
Interface index: 136, SNMP ifIndex: 29
Link-level type: LinkService, MTU: 1504
Device flags   : Present Running
Interface flags: Point-To-Point SNMP-Traps
Last flapped   : 2006-08-01 10:45:13 PDT (2w0d 06:06 ago)
Input rate     : 0 bps (0 pps)
Output rate    : 0 bps (0 pps)
Logical interface lsq-0/0/0.0 (Index 69) (SNMP ifIndex 42)
Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: Multilink-PPP
Bandwidth: 16mbps
Statistics         Frames      fps       Bytes        bps
Bundle:            
Fragments:         
   Input :             0        0           0          0
   Output:          1100        0      118800          0
Packets:           
   Input :             0        0           0          0
   Output:          1000        0      112000          0
...
Protocol inet, MTU: 1500
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
Destination: 9.9.9/24, Local: 9.9.9.10
```

**What It Means**—The output shows a summary of packets transiting the device on the multilink bundle. Verify the following information on the multilink bundle:

- The total number of transiting packets = 1000
- The total number of transiting fragments = 1100
- The number of data packets that were fragmented = 100

The total number of packets sent (600 + 400) on the multilink bundle match the number of transiting packets (1000), indicating that no packets were dropped.

The number of transiting fragments exceeds the number of transiting packets by 100, indicating that 100 large data packets were correctly fragmented.
Corrective Action—If the packets are not fragmented correctly, check your fragmentation threshold configuration. Packets smaller than the specified fragmentation threshold are not fragmented. For information about configuring the fragmentation threshold, see “Configuring the Link Services Interface with a Configuration Editor” on page 413.

Step 2: Verifying Packet Encapsulation

To find out whether a packet is treated as an LFI or non-LFI packet, determine its encapsulation type. LFI packets are PPP encapsulated, and non-LFI packets are encapsulated with both PPP and MLPPP. PPP and MLPPP encodings have different overheads resulting in different-sized packets. You can compare packet sizes to determine the encapsulation type.

A small unfragmented data packet contains a PPP header and a single MLPPP header. In a large fragmented data packet, the first fragment contains a PPP header and an MLPPP header, but the consecutive fragments contain only an MLPPP header.

PPP and MLPPP encodings add the following number of bytes to a packet:

- PPP encapsulation adds 7 bytes:
  4 bytes of header + 2 bytes of frame check sequence (FCS) + 1 byte that is idle or contains a flag
- MLPPP encapsulation adds between 6 and 8 bytes:
  4 bytes of PPP header + 2 to 4 bytes of multilink header

Figure 49 on page 443 shows the overhead added to PPP and MLPPP headers.

Figure 49: PPP and MLPPP Headers

For CRTP packets, the encapsulation overhead and packet size are even smaller than for an LFI packet. For more information, see “Configuring CRTP” on page 450.

Table 127 on page 444 shows the encapsulation overhead for a data packet and a voice packet of 70 bytes each. After encapsulation, the size of the data packet is larger than the size of the voice packet.
Table 127: PPP and MLPPP Encapsulation Overhead

<table>
<thead>
<tr>
<th>Packet Type</th>
<th>Encapsulation</th>
<th>Initial Packet Size</th>
<th>Encapsulation Overhead</th>
<th>Packet Size after Encapsulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice packet (LFI)</td>
<td>PPP</td>
<td>70 bytes</td>
<td>4 + 2 + 1 = 7 bytes</td>
<td>77 bytes</td>
</tr>
<tr>
<td>Data fragment (non-LFI) with short sequence</td>
<td>MLPPP</td>
<td>70 bytes</td>
<td>4 + 2 + 1 + 4 = 13 bytes</td>
<td>83 bytes</td>
</tr>
<tr>
<td>Data fragment (non-LFI) with long sequence</td>
<td>MLPPP</td>
<td>70 bytes</td>
<td>4 + 2 + 1 + 4 + 4 = 15 bytes</td>
<td>85 bytes</td>
</tr>
</tbody>
</table>

From the CLI, enter the `show interfaces queue` command to display the size of transmitted packet on each queue. Divide the number of bytes transmitted by the number of packets to obtain the size of the packets and determine the encapsulation type.

**Step 3: Verifying Load Balancing**

From the CLI, enter the `show interfaces queue` command on the multilink bundle and its constituent links to confirm whether load balancing is performed accordingly on the packets.

```
user@RO> show interfaces queue lsq-0/0/0
Physical interface: lsq-0/0/0, Enabled, Physical link is Up
  Interface index: 136, SNMP ifIndex: 29
  Forwarding classes: 8 supported, 8 in use
  Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: DATA
  Queued:
    Packets : 600 0 pps
    Bytes : 44800 0 bps
  Transmitted:
    Packets : 600 0 pps
    Bytes : 44800 0 bps
    Tail-dropped packets : 0 0 pps
    RED-dropped packets : 0 0 pps

Queue: 1, Forwarding classes: expedited-forwarding
  Queued:
    Packets : 0 0 pps
    Bytes : 0 0 bps

Queue: 2, Forwarding classes: VOICE
  Queued:
    Packets : 400 0 pps
    Bytes : 61344 0 bps
  Transmitted:
    Packets : 400 0 pps
    Bytes : 61344 0 bps

Queue: 3, Forwarding classes: NC
  Queued:
    Packets : 0 0 pps
```
show interfaces queue se-1/0/0

Physical interface: se-1/0/0, Enabled, Physical link is Up
Interface index: 141, SNMP ifIndex: 35
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: DATA
  Queued:
  Packets: 350 0 pps
  Bytes: 24350 0 bps
  Transmitted:
  Packets: 350 0 pps
  Bytes: 24350 0 bps
...
Queue: 1, Forwarding classes: expedited-forwarding
  Queued:
  Packets: 0 0 pps
  Bytes: 0 0 bps
...
Queue: 2, Forwarding classes: VOICE
  Queued:
  Packets: 100 0 pps
  Bytes: 15272 0 bps
  Transmitted:
  Packets: 100 0 pps
  Bytes: 15272 0 bps
...
Queue: 3, Forwarding classes: NC
  Queued:
  Packets: 19 0 pps
  Bytes: 247 0 bps
  Transmitted:
  Packets: 19 0 pps
  Bytes: 247 0 bps
...
show interfaces queue se-1/0/1

Physical interface: se-1/0/1, Enabled, Physical link is Up
Interface index: 142, SNMP ifIndex: 38
Forwarding classes: 8 supported, 8 in use
Egress queues: 8 supported, 8 in use
Queue: 0, Forwarding classes: DATA
  Queued:
  Packets: 350 0 pps
  Bytes: 24350 0 bps
  Transmitted:
  Packets: 350 0 pps
  Bytes: 24350 0 bps
...
Queue: 1, Forwarding classes: expedited-forwarding
  Queued:
  Packets: 0 0 pps
  Bytes: 0 0 bps
...
Queue: 2, Forwarding classes: VOICE
  Queued:
  Packets: 300 0 pps
  Bytes: 45672 0 bps
  Transmitted:
Table 128: Number of Packets Transmitted on a Queue

<table>
<thead>
<tr>
<th>Packets Queued</th>
<th>Bundle lsq-0/0/0.0</th>
<th>Constituent Link se-1/0/0</th>
<th>Constituent Link se-1/0/1</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets on Q0</td>
<td>600</td>
<td>350</td>
<td>350</td>
<td>The total number of packets transiting the constituent links (350 + 350 = 700) exceeded the number of packets queued (600) on the multilink bundle.</td>
</tr>
<tr>
<td>Packets on Q2</td>
<td>400</td>
<td>100</td>
<td>300</td>
<td>The total number of packets transiting the constituent links equaled the number of packets on the bundle.</td>
</tr>
<tr>
<td>Packets on Q3</td>
<td>0</td>
<td>19</td>
<td>18</td>
<td>The packets transiting Q3 of the constituent links are for keepalive messages exchanged between constituent links. Thus, no packets were counted on Q3 of the bundle.</td>
</tr>
</tbody>
</table>

On the multilink bundle, verify the following:

- The number of packets queued matches the number transmitted. If the numbers match, no packets were dropped. If more packets were queued than were transmitted, packets were dropped because the buffer was too small. The buffer size on the constituent links controls congestion at the output stage. To correct this problem, increase the buffer size on the constituent links. For more information, see “Defining and Applying Scheduler Maps” on page 420.

- The number of packets transiting Q0 (600) matches the number of large and small data packets received (100 + 500) on the multilink bundle. If the numbers match, all data packets correctly transited Q0.

- The number of packets transiting Q2 on the multilink bundle (400) matches the number of voice packets received on the multilink bundle. If the numbers match, all voice LFI packets correctly transited Q2.
On the constituent links, verify the following:

- The total number of packets transiting Q0 (350 + 350) matches the number of data packets and data fragments (500 + 200). If the numbers match, all the data packets after fragmentation correctly transited Q0 of the constituent links.

  Packets transited both constituent links, indicating that load balancing was correctly performed on non-LFI packets.

- The total number of packets transiting Q2 (300 + 100) on constituent links matches the number of voice packets received (400) on the multilink bundle. If the numbers match, all voice LFI packets correctly transited Q2.

  LFI packets from source port 100 transited se-1/0/0, and LFI packets from source port 200 transited se-1/0/1. Thus all LFI (Q2) packets were hashed based on the source port and correctly transited both constituent links.

**Corrective Action**—If the packets transited only one link, take the following steps to resolve the problem:

1. Determine whether the physical link is up (operational) or down (unavailable). An unavailable link indicates a problem with the PIM, interface port, or physical connection (link-layer errors). If the link is operational, move to the next step.
2. Verify that the classifiers are correctly defined for non-LFI packets. Make sure that non-LFI packets are not configured to be queued to Q2. All packets queued to Q2 are treated as LFI packets.
3. Verify that at least one of the following values is different in the LFI packets: source address, destination address, IP protocol, source port, or destination port. If the same values are configured for all LFI packets, the packets are all hashed to the same flow and transit the same link.

---

**Why Are Packets Dropped on a PVC Between a J Series Device and Another Vendor?**

**Problem**—I configured a permanent virtual circuit (PVC) between T1, E1, T3, or E3 interfaces on my Juniper Networks device and another vendor's device, and packets are being dropped and ping fails.

**Solution**—If the other vendor’s device does not have the same FRF.12 support as the J Series device or supports FRF.12 in a different way, the J Series interface on the PVC might discard a fragmented packet containing FRF.12 headers and count it as a “Policed Discard.” As a workaround for this problem, configure multilink bundles on both peers, and configure fragmentation thresholds on the multilink bundles.
Chapter 15

Aggregated Ethernet

This chapter describes aggregated Ethernet and how to configure aggregated Ethernet interfaces. It also describes the Link Aggregation Control Protocol (LACP), which provides additional functionality for link aggregation groups (LAGs) and, in the case of chassis clusters, for redundant Ethernet interface LAGs.

**NOTE:** This chapter is specific to the SRX3000 and SRX5000 line devices. For information about link aggregation for other SRX Series devices and J Series devices, see the “Configuring Ethernet Ports for Switching” chapter in the *Junos OS Layer 2 Bridging and Switching Configuration Guide for Security Devices.*

For information about which devices support the features documented in this chapter, see the *Junos OS Feature Support Reference for SRX Series and J Series Devices.*

This chapter contains the following topics:

- Aggregated Ethernet Overview on page 449
- Configuring Aggregated Ethernet Interfaces on page 450
- Understanding Chassis Cluster Redundant Ethernet Interface Link Aggregation Groups on page 454
- Understanding the Link Aggregation Control Protocol on page 455
- Understanding LACP in Chassis Cluster Mode on page 456
- Configuring LACP on Stand-Alone Devices on page 457
- Configuring LACP on Chassis Clusters on page 458
- Verifying Aggregated Ethernet Interfaces on page 459

**Aggregated Ethernet Overview**

Link aggregation of Ethernet interfaces is defined in the IEEE 802.3ad standard. The JUNOS Software implementation of 802.3ad balances traffic across the member links within an aggregated Ethernet bundle based on Layer 3 or Layer 4 (or both) information carried in the packet or based on session ID data. (The session ID data has higher precedence than the Layer 3 or 4 information.) This implementation uses the same load-balancing algorithm used for per-packet load balancing.

You can combine multiple physical Ethernet ports to form a logical point-to-point link, known as a link aggregation group (LAG) or bundle. Support for LAGs based on...
IEEE 802.3ad makes it possible to aggregate physical interface links on your device. LAGs provide increased interface bandwidth and link availability by linking physical ports and load-balancing traffic crossing the combined interface.

In a chassis cluster configuration, link aggregation allows a redundant Ethernet interface to add multiple child interfaces from both nodes and thereby create a redundant Ethernet interface link aggregation group (LAG).

Link aggregation allows one or more links to be combined together to form a LAG, such that a media access control (MAC) client can treat the LAG as if it were a single link. For the LAG to operate correctly, it is necessary to coordinate the two end systems connected by the LAG, either manually or automatically.

Internally, a LAG is a virtual interface presented on SRX3000 and SRX5000 line devices or on any system (consisting of devices such as routers and switches) supporting 802.3ad link aggregation. Externally, a LAG corresponds to a bundle of physical Ethernet links connected between an SRX3000 or SRX5000 line device and another system capable of link aggregation. This bundle of physical links is a virtual link.

JUNOS Software supports the Link Aggregation Control Protocol (LACP), which is a subcomponent of IEEE 802.3ad. LACP provides additional functionality for LAGs.

LACP is supported in standalone (single chassis) deployments, where aggregated Ethernet interfaces are supported, and in chassis cluster deployments, where aggregated Ethernet interfaces and redundant Ethernet interfaces are supported simultaneously.

Aggregated Ethernet interfaces can be Layer 3 interfaces (VLAN-tagged or untagged) and Layer 2 interfaces. LACP is supported on Layer 3 only.

**Related Topics**

- Configuring Aggregated Ethernet Interfaces on page 450
- Understanding Chassis Cluster Redundant Ethernet Interface Link Aggregation Groups on page 454
- Understanding the Link Aggregation Control Protocol on page 455

**Configuring Aggregated Ethernet Interfaces**

You configure an aggregated Ethernet virtual link by specifying the link number as a physical device and then associating a set of ports that have the same speed and are in full-duplex mode. The physical ports can be 100-Megabit Ethernet, 1-Gigabit Ethernet, and 10-Gigabit Ethernet.

Note the following support details for the SRX3000 and SRX5000 lines:

- The devices support a maximum of 16 physical interfaces per single aggregated Ethernet bundle.
- Aggregated Ethernet interfaces can use interfaces from the same or different Flexible PIC Concentrators (FPCs) and PICs.
On the aggregated bundle, capabilities such as MAC accounting, VLAN rewrites, and VLAN queuing are available.

Aggregated Ethernet interfaces can be either VLAN-tagged or untagged, with LACP enabled or disabled. Aggregated Ethernet interfaces on the SRX3000 and SRX5000 lines support the configuration of `native-vlan-id`, which consists of the following configuration statements:

- inner-tag-protocol-id
- inner-vlan-id
- pop-pop
- pop-swap
- push-push
- swap-push
- swap-swap

**NOTE:** You can enable promiscuous mode on aggregated Ethernet interfaces. When promiscuous mode is enabled on a Layer 3 Ethernet interface, all packets received on the interface are sent to the central point or Services Processing Unit regardless of the destination MAC address of the packet. If you enable promiscuous mode on an aggregated Ethernet interface, promiscuous mode is then enabled on all member interfaces.

You must set the number of aggregated Ethernet interfaces on the chassis. You can also set the member link speed and the minimum links in a bundle.

**Configuring the Number of Aggregated Ethernet Interfaces on the Device**

By default, no aggregated Ethernet interfaces are created. You must set the number of aggregated Ethernet interfaces on the routing device before you can configure them.

Once the `device-count` statement is specified, the system creates that number of empty aggregated Ethernet interfaces. A globally unique MAC address is assigned to every aggregated Ethernet interface. More aggregated Ethernet interfaces can be created by increasing the parameter.

The maximum number of aggregated devices you can configure is 128. The aggregated interfaces are numbered from `ae0` through `ae127`.

To set the number of aggregated Ethernet interfaces to 2:

```
user@host# set chassis aggregated-devices ethernet device-count 2
```
**Associating Physical Interfaces with Aggregated Ethernet Interfaces**

You associate a physical interface with an aggregated Ethernet interface. Doing so associates the physical child links with the logical aggregated parent interface to form a link aggregation group (LAG). You must also specify the constituent physical links by including the `802.3ad` statement.

A physical interface can be added to any aggregated Ethernet interface as long as all member links have the same link speed and the maximum number of member links does not exceed 16. The aggregated Ethernet interface instance number aex can be from 0 through 127, for a total of 128 aggregated interfaces.

To associate physical interfaces with `ae0` and `ae1`, respectively:

```bash
user@host# set interfaces ge-1/0/0 gigether-options 802.3ad ae0
user@host# set interfaces ge-2/0/0 gigether-options 802.3ad ae0
user@host# set interfaces ge-3/0/0 gigether-options 802.3ad ae1
user@host# set interfaces ge-3/0/1 gigether-options 802.3ad ae1
user@host# set interfaces ge-4/0/0 gigether-options 802.3ad ae1
```

**NOTE:** If you specify (on purpose or accidentally) that a link already associated with an aggregated Ethernet interface be associated with another aggregated Ethernet interface, the link is removed from the previous interface (there is no need for you to explicitly delete it) and it is added to the other one.

**Configuring Aggregated Ethernet Link Speed**

On aggregated Ethernet interfaces, you can set the required link speed for all interfaces included in the bundle. All interfaces that make up a bundle must be the same speed. If you include in the aggregated Ethernet interface an individual link that has a speed different from the speed you specify in the `link-speed` parameter, an error message will be logged.

The speed value is specified in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).

Aggregated Ethernet interfaces on SRX3000 and SRX5000 line devices can have one of the following speed values:

- 100m—Links are 100 Mbps.
- 10g—Links are 10 Gbps.
- 1g—Links are 1 Gbps.

To set the required link speed for all interfaces included in the bundle to 10 Gbps:

```bash
user@host# set interfaces ae0 aggregated-ether-options link-speed 10g
```
**Configuring Aggregated Ethernet Minimum Links**

On aggregated Ethernet interfaces, you can configure the minimum number of links that must be up for the bundle as a whole to be labeled as up. By default, only one link must be up for the bundle to be labeled as up.

On SRX3000 and SRX5000 line devices, the valid range for the minimum links number is 1 through 16. When the maximum value (16) is specified, all configured links of a bundle must be up for the bundle to be labeled as up.

To set the minimum number of links to 8:

```
user@host# set interfaces ae0 aggregated-ether-options minimum-links 8
```

If the number of links configured in an aggregated Ethernet interface is less than the minimum-links value configured in the minimum-links statement, the configuration commit fails and an error message is displayed.

**Deleting Aggregated Ethernet Interfaces**

There are two approaches to deleting an aggregated Ethernet interface:

- You can delete an aggregated Ethernet interface from the interface configuration. The JUNOS Software removes the configuration statements related to aeX and sets this interface to the down state. The deleted aggregated Ethernet interface still exists, but it becomes an empty interface.

  To delete aggregated Ethernet interface ae4:

  ```
  user@host# delete interfaces ae4
  ```

- You can also permanently remove the aggregated Ethernet interface from the device configuration by deleting it from the device-count on the routing device.

  **WARNING:** Be aware that this approach deletes the aggregated Ethernet interface objects from the device configuration. The following command deletes all the interface objects.

  ```
  user@host# delete chassis aggregated-devices ethernet device-count
  ```

  If you reduce the device-count, only the aggregated Ethernet interface objects at the end of the list are removed, leaving the newly specified number of interfaces. That is, if you configure the device-count as 10 and then reduce it to 6, the system removes the last 4 interface objects from the list.

  To reduce the number of aggregated Ethernet interfaces to 6:

  ```
  user@host# delete chassis aggregated-devices ethernet device-count 6
  ```
Understanding Chassis Cluster Redundant Ethernet Interface Link Aggregation Groups

Link aggregation groups (LAGs) can be established across nodes in a chassis cluster. Link aggregation allows a redundant Ethernet interface (known as a reth interface in CLI commands) to add multiple child interfaces from both nodes and thereby create a redundant Ethernet interface LAG.

Instead of one active/standby link, you can configure up to 8 links per node. Having multiple active redundant Ethernet interface links reduces the possibility of failover. For example, when an active link is out of service, all traffic on this link is distributed to other active redundant Ethernet interface links, instead of triggering a redundant Ethernet active/standby failover.

Standalone link aggregation group interfaces (ae) are supported on clustered devices but cannot be added to redundant Ethernet interfaces. Likewise any child interface of an existing LAG cannot be added to a redundant Ethernet interface and vice versa. The maximum number of total combined standalone aggregate interfaces (ae) and redundant Ethernet interfaces (reth) per cluster is 128.

Redundant Ethernet interface configuration also includes a minimum-links setting that allows you to set a minimum number of physical child links in a redundant Ethernet interface LAG that must be working on the primary node for the interface to be up. The default minimum-links value is 1. When the number of physical links on the primary node in a redundant Ethernet interface falls below the minimum-links value, the interface will be down even if some links are still working.

For more information about Ethernet interface link aggregation with redundant Ethernet interfaces in a chassis cluster deployment, see the “Chassis Cluster Redundant Ethernet Interface Link Aggregation Groups” section of the JUNOS Software Security Configuration Guide.

Related Topics

- Aggregated Ethernet Overview on page 449
- Configuring Aggregated Ethernet Interfaces on page 450
- Understanding LACP in Chassis Cluster Mode on page 456
- Configuring LACP on Chassis Clusters on page 458
Understanding the Link Aggregation Control Protocol

JUNOS Software supports the Link Aggregation Control Protocol (LACP), which is a subcomponent of IEEE 802.3ad. LACP provides additional functionality for LAGs.

LACP provides a standardized means for exchanging information between partner systems on a link to allow their link aggregation control instances to reach agreement on the identity of the LAG to which the link belongs, and then to move the link to that LAG, and to enable the transmission and reception processes for the link to function in an orderly manner.

For example, when LACP is not enabled, a local LAG might attempt to transmit packets to a remote individual interface, which causes the communication to fail. (An individual interface is a non-aggregatable interface.) When LACP is enabled, a local LAG cannot transmit packets unless a LAG with LACP is also configured on the remote end of the link.

LACP does not support automatic configuration on SRX3000 and SRX5000 line devices, but partner systems are allowed to perform automatic configuration. When an SRX3000 or SRX5000 line device is connected to a fully 802.3ad-compliant partner system, static configuration of LAGs is initiated on the SRX3000 and SRX5000 line device side, and static configuration is not needed on the partner side.

**NOTE:** When an SRX3000 or SRX5000 line device is connected to a Juniper Networks MX Series router, static configuration of LAGs is needed at both the actor and partner systems.

LACP is supported in standalone deployments, where aggregated Ethernet interfaces are supported, and in chassis cluster deployments, where aggregated Ethernet interfaces and redundant Ethernet interfaces are supported simultaneously.

By default, aggregated and redundant Ethernet links do not exchange link aggregation control protocol data units (PDUs), which contain information about the state of the link. You can configure Ethernet links to actively transmit link aggregation control PDUs, or you can configure the links to passively transmit them, sending out link aggregation control PDUs only when they receive them from the remote end of the same link. The local end of a child link is known as the actor and the remote end of the link is known as the partner. That is, the actor sends link aggregation control PDUs to its protocol partner that convey what the actor knows about its own state and that of the partner’s state.

**NOTE:** Although the LACP functions on the SRX3000 and SRX5000 line devices are similar to the LACP features on Juniper Networks MX Series routers, the following LACP features on MX Series routers are not supported on SRX3000 and SRX5000 line devices: link protection, system priority, and port priority for aggregated Ethernet interfaces. Instead, SRX5000 and SRX5000 line devices provide active/standby support with redundant Ethernet interface LAGs in chassis cluster deployments.
Understanding LACP in Chassis Cluster Mode

In chassis cluster mode, aggregated Ethernet interfaces (ae) and redundant Ethernet interfaces (reth) coexist. Because the functionality of a redundant Ethernet interface relies on the JUNOS aggregated Ethernet framework, you can think of it as a special aggregated Ethernet interface.

A redundant Ethernet interface has active and standby links located on two nodes in a chassis cluster. All active links in a redundant Ethernet interface are located on a node, and all standby links are on the other node. The total number of active and standby links is limited to 16 (8 active and 8 standby).

LACP maintains a point-to-point LAG. Any port connected to the third point is denied. However, a redundant Ethernet interface does connect to two different systems or two remote aggregated Ethernet interfaces by design. To support LACP on both redundant Ethernet interface active and standby links, a redundant Ethernet interface can be modeled to consist of two sub-LAGs, where all active links form an active sub-LAG and all standby links form a standby sub-LAG. In this model, LACP selection logic is applied and limited to one sub-LAG at a time. In this way, two redundant Ethernet interface sub-LAGs are maintained simultaneously while all the LACP advantages are preserved for each sub-LAG.

It is necessary for the switches used to connect the nodes in the cluster to have a LAG link configured and 802.3ad enabled for each LAG on both nodes so that the aggregate links will be recognized as such and correctly pass traffic.

**NOTE:** The redundant Ethernet interface LAG child links from each node in the chassis cluster must be connected to a different LAG at the peer devices. If a single peer switch is used to terminate the redundant Ethernet interface LAG, two separate LAGs must be used in the switch.

With LACP, it is essential for the redundant Ethernet interface to support hitless failover between the active and standby links in normal operation. The term *hitless* means that the redundant Ethernet interface state remains up during failover.

The lacpd process manages both the active and standby links of the redundant Ethernet interfaces. A redundant Ethernet interface pseudolink is in the up condition when the number of active up links is not less than the number of minimum links configured. Therefore, to support hitless failover, the LACP state on the redundant
Ethernet interface standby links must be collecting and distributing before failover occurs.

**Related Topics**

- Aggregated Ethernet Overview on page 449
- Understanding Chassis Cluster Redundant Ethernet Interface Link Aggregation Groups on page 454
- Understanding the Link Aggregation Control Protocol on page 455
- Configuring LACP on Chassis Clusters on page 458

### Configuring LACP on Stand-Alone Devices

LACP is configured on aggregated Ethernet interfaces at the `[edit interfaces interface-name aggregated-ether-options]` hierarchy.

#### Configuring LACP

You configure LACP on an aggregated Ethernet interface by setting the LACP mode for the parent link with the `lacp` statement. The LACP mode can be off (the default), active, or passive.

LACP is enabled by setting the mode to either passive or active. If the actor and partner are both in passive mode, they do not exchange link aggregation control PDUs, which results in the aggregated Ethernet links not coming up. If either the actor or partner is active, they exchange link aggregation control PDUs. To initiate transmission of link aggregation control PDUs and response link aggregation control PDUs, you must enable LACP at both the local and remote ends of the links, and one end must be active.

To set the LACP mode to `passive` for `ae0`:

```
[edit interfaces]
user@host# set ae0 aggregated-ether-options lacp passive
```

To set the LACP mode to `active` for `ae0`:

```
[edit interfaces]
user@host# set ae0 aggregated-ether-options lacp active
```

#### Configuring the LinkAggregation Control PDU Transmit Interval

You configure the interval at which the interfaces on the remote side of the link transmit link aggregation control PDUs by configuring the `periodic` statement on the interfaces on the local side. It is the configuration on the local side that specifies the behavior of the remote side. That is, the remote side transmits link aggregation control PDUs at the specified interval. The interval can be `fast` (every second) or `slow` (every 30 seconds).
By default, the actor and partner transmit link aggregation control PDUs every second. You can configure different periodic rates on active and passive interfaces. When you configure the active and passive interfaces at different rates, the transmitter honors the receiver's rate.

To configure the interval to be every 30 seconds:

```
[edit interfaces]
user@host# set ae0 aggregated-ether-options lACP periodic slow
```

**Related Topics**

- Aggregated Ethernet Overview on page 449
- Configuring Aggregated Ethernet Interfaces on page 450
- Understanding the Link Aggregation Control Protocol on page 455
- Verifying Aggregated Ethernet Interfaces on page 459

**Configuring LACP on Chassis Clusters**

LACP is configured on redundant Ethernet interfaces at the [edit interfaces interface-name redundant-ether-options] hierarchy.

**Configuring LACP**

You configure LACP on a redundant Ethernet interface by setting the LACP mode for the parent link with the lACP statement. The LACP mode can be off (the default), active, or passive.

LACP is enabled by setting the mode to either passive or active. If the actor and partner are both in passive mode, they do not exchange link aggregation control PDUs, which results in the redundant Ethernet links not coming up. If either the actor or partner is active, they exchange link aggregation control PDUs. To initiate transmission of link aggregation control PDUs and response link aggregation control PDUs, you must enable LACP at both the local and remote ends of the links, and one end must be active.

To set the LACP mode to passive for reth0:

```
[primary:node1] [edit interfaces]
set reth0 redundant-ether-options lACP passive
```

To set the LACP mode to active for reth0:

```
[primary:node1] [edit interfaces]
set reth0 redundant-ether-options lACP active
```

**Configuring the Link Aggregation Control PDU Transmit Interval**

You configure the interval at which the interfaces on the remote side of the link transmit link aggregation control PDUs by configuring the periodic statement on the
interfaces on the local side. It is the configuration on the local side that specifies the behavior of the remote side. That is, the remote side transmits link aggregation control PDUs at the specified interval. The interval can be fast (every second) or slow (every 30 seconds).

By default, the actor and partner transmit link aggregation control PDUs every second. You can configure different periodic rates on active and passive interfaces. When you configure the active and passive interfaces at different rates, the transmitter honors the receiver’s rate.

To configure the interval to be every 30 seconds:

```
[edit interfaces]
user@host# set reth0 redundant-ether-options lACP periodic slow
```

**Related Topics**

- Aggregated Ethernet Overview on page 449
- Understanding Chassis Cluster Redundant Ethernet Interface Link Aggregation Groups on page 454
- Understanding the Link Aggregation Control Protocol on page 455
- Understanding LACP in Chassis Cluster Mode on page 456
- Verifying Aggregated Ethernet Interfaces on page 459

**Verifying Aggregated Ethernet Interfaces**

To verify an aggregated Ethernet interface configuration, perform these tasks:

- Verifying Aggregated Ethernet Interfaces (terse) on page 459
- Verifying Aggregated Ethernet Interfaces (extensive) on page 460
- Verifying LACP Statistics on page 461
- Verifying LACP Aggregated Ethernet Interfaces on page 461
- Verifying LACP Redundant Ethernet Interfaces on page 462

**Verifying Aggregated Ethernet Interfaces (terse)**

**Purpose**

Display status information in terse (concise) format for aggregated Ethernet interfaces.

**Action**

From the CLI, enter the `show interfaces ae0 terse` command.

**Sample Output**

```
user@host> show interfaces ae0 terse
ge-2/0/0.0              up    up   aenet    --> ae0.0
ge-2/0/0.32767          up    up   aenet    --> ae0.32767
ge-2/0/1.0              up    up   aenet    --> ae0.0
ge-2/0/1.32767          up    up   aenet    --> ae0.32767
ae0                     up    up
ae0.0                   up    up   bridge
ae0.32767               up    up   multiservice
```
Meaning  The output shows the bundle relationship for the aggregated Ethernet interface and the overall status of the interface, including information such as the following:

- The link aggregation control PDUs run on the .0 child logical interfaces for the untagged aggregated Ethernet interface.
- The link aggregation control PDUs run on the .32767 child logical interfaces for the VLAN-tagged aggregated Ethernet interface.
- The .32767 logical interface is created for the parent link and all child links.

Related Topics  For a complete description of show interfaces output, see the Junos OS CLI Reference.

Verifying Aggregated Ethernet Interfaces (extensive)

Purpose  Display status information and statistics in extensive format for aggregated Ethernet interfaces.

Action  From the CLI, enter the show interfaces ae0 extensive command.

Sample Output

user@host> show interfaces ae0 extensive
Physical interface: ae0, Enabled, Physical link is Up

Logical interface ae0.0 (Index 67) (SNMP ifIndex 628) (Generation 134)

<table>
<thead>
<tr>
<th>LACP info:</th>
<th>Role</th>
<th>System</th>
<th>System</th>
<th>Port</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>priority</td>
<td>identifier</td>
<td>priority</td>
<td>number</td>
<td>key</td>
<td></td>
</tr>
<tr>
<td>ge-5/0/0.0</td>
<td>Actor</td>
<td>127</td>
<td>00:1f:12:8c:af:c0</td>
<td>127</td>
<td>832</td>
<td>1</td>
</tr>
<tr>
<td>ge-5/0/0.0</td>
<td>Partner</td>
<td>127</td>
<td>00:1f:12:8f:d7:c0</td>
<td>127</td>
<td>640</td>
<td>1</td>
</tr>
<tr>
<td>ge-5/0/1.0</td>
<td>Actor</td>
<td>127</td>
<td>00:1f:12:8c:af:c0</td>
<td>127</td>
<td>833</td>
<td>1</td>
</tr>
<tr>
<td>ge-5/0/1.0</td>
<td>Partner</td>
<td>127</td>
<td>00:1f:12:8f:d7:c0</td>
<td>127</td>
<td>641</td>
<td>1</td>
</tr>
</tbody>
</table>

LACP Statistics: LACP Rx | LACP Tx | Unknown Rx | Illegal Rx
| ge-5/0/0.0 | 12830 | 7090 | 0 | 0 |
| ge-5/0/1.0 | 10304 | 4786 | 0 | 0 |

Logical interface ae0.32767 (Index 70) (SNMP ifIndex 630) (Generation 135)

<table>
<thead>
<tr>
<th>LACP info:</th>
<th>Role</th>
<th>System</th>
<th>System</th>
<th>Port</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>priority</td>
<td>identifier</td>
<td>priority</td>
<td>number</td>
<td>key</td>
<td></td>
</tr>
<tr>
<td>ge-5/0/0.32767</td>
<td>Actor</td>
<td>127</td>
<td>00:1f:12:8c:af:c0</td>
<td>127</td>
<td>832</td>
<td>1</td>
</tr>
<tr>
<td>ge-5/0/0.32767</td>
<td>Partner</td>
<td>127</td>
<td>00:1f:12:8f:d7:c0</td>
<td>127</td>
<td>640</td>
<td>1</td>
</tr>
<tr>
<td>ge-5/0/1.32767</td>
<td>Actor</td>
<td>127</td>
<td>00:1f:12:8c:af:c0</td>
<td>127</td>
<td>833</td>
<td>1</td>
</tr>
<tr>
<td>ge-5/0/1.32767</td>
<td>Partner</td>
<td>127</td>
<td>00:1f:12:8f:d7:c0</td>
<td>127</td>
<td>641</td>
<td>1</td>
</tr>
</tbody>
</table>

LACP Statistics: LACP Rx | LACP Tx | Unknown Rx | Illegal Rx
| ge-5/0/1.0 | 10304 | 4786 | 0 | 0 |
Meaning  The output shows detailed aggregated Ethernet interface information. This portion of the output shows LACP information and LACP statistics for each logical aggregated Ethernet interface.

Related Topics  For a complete description of show interfaces output, see the Junos OS CLI Reference.

### Verifying LACP Statistics

**Purpose**  Display LACP statistics for aggregated Ethernet interfaces.

**Action**  From the CLI, enter the `show lacp statistics interfaces ae0` command.

**Sample Output**

```
user@host> show lacp statistics interfaces ae0
Aggregated interface: ae0
LACP Statistics:       LACP Rx     LACP Tx   Unknown Rx   Illegal Rx
ge-2/0/0                1352        2035            0            0
ge-2/0/1                1352        2056            0            0
ge-2/2/0                1352        2045            0            0
ge-2/2/1                1352        2043            0            0
```

**Meaning**  The output shows LACP statistics for each physical interface associated with the aggregated Ethernet interface, such as the following:

- The LACP received counter that increments for each normal hello
- The number of LACP transmit packet errors logged
- The number of unrecognized packet errors logged
- The number of invalid packets received

Use the following command to clear the statistics and see only new changes:

```
user@host# clear lacp statistics interfaces ae0
```

**Related Topics**  For a complete description of show lacp statistics interfaces output, see the Junos OS CLI Reference.

### Verifying LACP Aggregated Ethernet Interfaces

**Purpose**  Display LACP status information for aggregated Ethernet interfaces.

**Action**  From the CLI, enter the `show lacp interfaces ae0` command.
Meaning

The output shows aggregated Ethernet interface information, such as the following:

- The LACP state—Indicates whether the link in the bundle is an actor (local or near-end of the link) or partner (remote or far-end of the link).
- The LACP mode—Indicates whether both ends of the aggregated Ethernet interface are enabled (active or passive)—at least one end of the bundle must be active.
- The periodic link aggregation control PDU transmit rate.
- The LACP protocol state—When the link is up, it is collecting and distributing packets.

Related Topics

For a complete description of `show lacp interfaces` output, see the Junos OS CLI Reference.

Verifying LACP Redundant Ethernet Interfaces

Purpose

Display LACP status information for redundant Ethernet interfaces.

Action

From the CLI, enter the `show lacp interfaces reth0` command.

Sample Output

```
user@host> show lacp interfaces reth0
Aggregated interface: reth0

LACP state:       Role   Exp   Def  Dist  Col  Syn  Aggr  Timeout  Activity
ge-11/0/0      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
ge-11/0/0    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
ge-11/0/1      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
ge-11/0/1    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
ge-11/0/2      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
ge-11/0/2    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
ge-11/0/3      Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
ge-11/0/3    Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
ge-3/0/0       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
ge-3/0/0     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
ge-3/0/1       Actor    No    No   Yes  Yes  Yes   Yes     Fast    Active
ge-3/0/1     Partner    No    No   Yes  Yes  Yes   Yes     Fast    Active
```

Verifying LACP Redundant Ethernet Interfaces
The output shows redundant Ethernet interface information, such as the following:

- **The LACP state**—Indicates whether the link in the bundle is an actor (local or near-end of the link) or partner (remote or far-end of the link).
- **The LACP mode**—Indicates whether both ends of the aggregated Ethernet interface are enabled (active or passive)—at least one end of the bundle must be active.
- **The periodic link aggregation control PDU transmit rate.**
- **The LACP protocol state**—When the link is up, it is collecting and distributing packets.

For a complete description of `show lacp interfaces` output, see the *Junos OS CLI Reference*. 

### Meaning

<table>
<thead>
<tr>
<th>Interface</th>
<th>Actor</th>
<th>Partner</th>
<th>LACP State</th>
<th>Transmit State</th>
<th>Mux State</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-3/0/2</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ge-3/0/2</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ge-3/0/3</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ge-3/0/3</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Verifying LACP Redundant Ethernet Interfaces

Chapter 15: Aggregated Ethernet
Part 2

Routing Protocols

- Routing Overview on page 467
- Static Routing on page 475
- RIP on page 485
- OSPF on page 503
- IS-IS on page 525
- BGP on page 535
- Multicast on page 559
Chapter 16
Routing Overview

Routing is the transmission of data packets from a source to a destination address. It involves delivering a message across a network or networks. This process has two primary components: the exchange of routing information to forward packets accurately from source to destination and the packet-forwarding procedure.


For packets to be correctly forwarded to the appropriate host address, the host must have a unique numeric identifier or IP address. The unique IP address of the destination host forms entries in the routing table. These entries are primarily responsible for determining the path that a packet traverses when transmitted from source to destination.

To use the routing capabilities of a Juniper Networks device, you must understand the fundamentals of IP routing and the routing protocols that are primarily responsible for the transmission of unicast traffic. To understand this topic, you need a basic understanding of IP addressing and TCP/IP.

NOTE: When configuring IPv6 addressing and routing on a J Series device, you must enable IPv6 in secure context.

This topic contains the following sections:

- Networks and Subnetworks on page 468
- Autonomous Systems on page 468
- Interior and Exterior Gateway Protocols on page 468
- Routing Tables on page 468
- Forwarding Tables on page 469
- Dynamic and Static Routing on page 470
Networks and Subnetworks

Large groups of machines that are interconnected and can communicate with one another form networks. Typically, networks identify large systems of computers and devices that are owned or operated by a single entity. Traffic is routed between or through the networks as data is passed from host to host.

As networks grow large, the ability to maintain the network and effectively route traffic between hosts within the network becomes increasingly difficult. To accommodate growth, networks are divided into subnetworks. Fundamentally, subnetworks behave exactly like networks, except that they are identified by a more specific network address and subnet mask (destination prefix). Subnetworks have routing gateways and share routing information in exactly the same way as large networks.

Autonomous Systems

A large network or collection of routers under a single administrative authority is termed an autonomous system (AS). Autonomous systems are identified by a unique numeric identifier that is assigned by the Internet Assigned Numbers Authority (IANA). Typically, the hosts within an AS are treated as internal peers, and hosts in a peer AS are treated as external peers. The status of the relationship between hosts—internal or external—governs the protocol used to exchange routing information.

Interior and Exterior Gateway Protocols

Routing information that is shared within an AS is transmitted by an interior gateway protocol (IGP). Of the different IGPs, the most common are RIP, OSPF, and IS-IS. IGPs are designed to be fast acting and light duty. They typically incorporate only a moderate security system, because trusted internal peers do not require the stringent security measures that untrusted peers require. As a result, you can usually begin routing within an AS by enabling the IGP on all internal interfaces and performing minimal additional configuration. You do not need to establish individual adjacencies.

Routing information that is shared with a peer AS is transmitted by an exterior gateway protocol (EGP). The primary EGP in use in almost all networks is the Border Gateway Protocol (BGP). BGP is designed to be very secure. Individual connections must be explicitly configured on each side of the link. As a result, although large numbers of connections are difficult to configure and maintain, each connection is secure.

Routing Tables

To route traffic from a source host to a destination host, the devices through which the traffic will pass must learn the path that the packet is to take. Once learned, the information is stored in routing tables. The routing table maintains a list of all the possible paths from point A to point B. Figure 50 on page 469 shows a simple network of routers.
This simple network provides multiple ways to get from host San Francisco to host Miami. The packet can follow the path through Denver and Cleveland. Alternatively, the packet can be routed through Phoenix and directly to Miami. The routing table includes all the possible paths and combinations—an exhaustive list of all the ways to get from the source to the destination.

The routing table must include every possible path from a source to a destination. Routing tables for the network in Figure 50 on page 469 must include entries for San Francisco-Denver, San Francisco-Cleveland, San Francisco-Miami, Denver-Cleveland, and so on. As the number of sources and destinations increases, the routing table quickly becomes large. The unwieldy size of routing tables is the primary reason for the division of networks into subnetworks.

**Forwarding Tables**

If the routing table is a list of all the possible paths a packet can take, the forwarding table is a list of only the best routes to a particular destination. The best path is determined according to the particular routing protocol being used, but generally the number of hops between the source and destination determines the best possible route.

In the network shown in Figure 50 on page 469, because the path with the fewest number of hops from San Francisco to Miami is through Phoenix, the forwarding table distills all the possible San Francisco-Miami routes into the single route through Phoenix. All traffic with a destination address of Miami is sent directly to the next hop, Phoenix.

After it receives a packet, the Phoenix router performs another route lookup, using the same destination address. The Phoenix router then routes the packet appropriately. Although it considers the entire path, the router at any individual hop along the way is responsible only for transmitting the packet to the next hop in the path. If the Phoenix router is managing its traffic in a particular way, it might send the packet through Houston on its route to Miami. This scenario is likely if specific
customer traffic is treated as priority traffic and routed through a faster or more direct route, while all other traffic is treated as nonpriority traffic.

Dynamic and Static Routing

Entries are imported into a router’s routing table from dynamic routing protocols or by manual inclusion as static routes. Dynamic routing protocols allow routers to learn the network topology from the network. The routers within the network send out routing information in the form of route advertisements. These advertisements establish and communicate active destinations, which are then shared with other routers in the network.

Although dynamic routing protocols are extremely useful, they have associated costs. Because they use the network to advertise routes, dynamic routing protocols consume bandwidth. Additionally, because they rely on the transmission and receipt of route advertisements to build a routing table, dynamic routing protocols create a delay (latency) between the time a router is powered on and the time during which routes are imported into the routing table. Some routes are therefore effectively unavailable until the routing table is completely updated, when the router first comes online or when routes change within the network (due to a host going offline, for example).

Static routing avoids the bandwidth cost and route import latency of dynamic routing. Static routes are manually included in the routing table, and never change unless you explicitly update them. Static routes are automatically imported into the routing table when a router first comes online. Additionally, all traffic destined for a static address is routed through the same router. This feature is particularly useful for networks with customers whose traffic must always flow through the same routers. Figure 51 on page 470 shows a network that uses static routes.

Figure 51: Static Routing Example

In Figure 51 on page 470, the customer routes in the 192.176.14/24 subnetwork are static routes. These are hard links to specific customer hosts that never change. Because all traffic destined for any of these routes is forwarded through Router A, these routes are included as static routes in Router A’s routing table. Router A then advertises these routes to other hosts so that traffic can be routed to and from them.

Route Advertisements

The routing table and forwarding table contain the routes for the routers within a network. These routes are learned through the exchange of route advertisements. Route advertisements are exchanged according to the particular protocol being employed within the network.
Generally, a router transmits hello packets out each of its interfaces. Neighboring routers detect these packets and establish adjacencies with the router. The adjacencies are then shared with other neighboring routers, which allows the routers to build up the entire network topology in a topology database, as shown in Figure 52 on page 471.

**Figure 52: Route Advertisement**

In Figure 52 on page 471, Router A sends out hello packets to each of its neighbors. Routers B and C detect these packets and establish an adjacent relationship with Router A. Router B and C then share this information with their neighbors, Routers D and E, respectively. By sharing information throughout the network, the routers create a network topology, which they use to determine the paths to all possible destinations within the network. The routes are then distilled into the forwarding table of best routes according to the route selection criteria of the protocol in use.

**Route Aggregation**

As the number of hosts in a network increases, the routing and forwarding tables must establish and maintain more routes. As these tables become larger, the time routers require to look up particular routes so that packets can be forwarded becomes prohibitive. The solution to the problem of growing routing tables is to group (aggregate) the routers by subnetwork, as shown in Figure 53 on page 472.
Figure 53 on page 472 shows three different ASs. Each AS contains multiple subnetworks with thousands of host addresses. To allow traffic to be sent from any host to any host, the routing tables for each host must include a route for each destination. For the routing tables to include every combination of hosts, the flooding of route advertisements for each possible route becomes prohibitive. In a network of hosts numbering in the thousands or even millions, simple route advertisement is not only impractical but impossible.

By employing route aggregation, instead of advertising a route for each host in AS 3, the gateway router advertises only a single route that includes all the routes to all the hosts within the AS. For example, instead of advertising the particular route 170.16.124.17, the AS 3 gateway router advertises only 170.16/16. This single route advertisement encompasses all the hosts within the 170.16/16 subnetwork, which reduces the number of routes in the routing table from $2^{16}$ (one for every possible IP address within the subnetwork) to 1. Any traffic destined for a host within the AS is forwarded to the gateway router, which is then responsible for forwarding the packet to the appropriate host.

Similarly, in this example, the gateway router is responsible for maintaining $2^{16}$ routes within the AS (in addition to any external routes). The division of this AS into subnetworks allows for further route aggregation to reduce this number. In the
subnetwork in the example, the subnetwork gateway router advertises only a single route (170.16.124/24), which reduces the number of routes from $2^8$ to 1.

**Related Topics**

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- RIP Overview on page 485
- OSPF Overview on page 503
- IS-IS Overview on page 525
- BGP Overview on page 535
- Multicast Overview on page 559
- Routing Policies Overview on page 581
- IPv6 Overview in the *Junos Routing Protocols Configuration Guide*
Chapter 17
Static Routing

Static Routing Configuration Overview on page 475
Basic Static Routes on page 476
Static Route Selection on page 477
Static Route Control in Routing and Forwarding Tables on page 480
Default Static Route Behavior on page 482
Verifying the Static Route Configuration on page 483

Static Routing Configuration Overview

To configure static routing:
3. Configure the static routes and define their next hop addresses. See “Example: Configuring a Basic Set of Static Routes (CLI)” on page 476.
4. (Optional) Specify how traffic should be routed to a destination if multiple next hops exist for a single static route. See “Example: Controlling Static Route Selection (CLI)” on page 478.
5. (Optional) Determine how static routes are inserted and maintained in the routing and forwarding tables. See “Example: Controlling Static Routes in the Routing and Forwarding Tables (CLI)” on page 481.
6. (Optional) Define the static routes’ default properties. See “Example: Defining Default Behavior for All Static Routes (CLI)” on page 483.

Related Topics
Junos OS Feature Support Reference for SRX Series and J Series Devices
Routing Overview on page 467
Verifying the Static Route Configuration on page 483
Understanding Basic Static Routing on page 476
Understanding Static Route Preferences and Qualified Next Hops on page 477
Basic Static Routes

- Understanding Basic Static Routing on page 476
- Example: Configuring a Basic Set of Static Routes (CLI) on page 476

**Understanding Basic Static Routing**

Routes that are permanent fixtures in the routing and forwarding tables are often configured as static routes. These routes generally do not change, and often include only one or very few paths to the destination.

To create a static route in the routing table, you must, at minimum, define the route as static and associate a next-hop address with it. The static route in the routing table is inserted into the forwarding table when the next-hop address is reachable. All traffic destined for the static route is transmitted to the next-hop address for transit.

**Example: Configuring a Basic Set of Static Routes (CLI)**

Customer routes that are connected to stub networks are often configured as static routes. Figure 54 on page 476 shows a sample network.

**Figure 54: Customer Routes Connected to a Stub Network**
To configure customer routes as static routes, like the ones in Figure 54 on page 476, follow these steps on the device to which the customer routes are connected:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 129 on page 477.
3. If you are finished configuring the router, commit the configuration.
4. Go on to one of the following procedures:
   - To manually control static route selection, see “Example: Controlling Static Route Selection (CLI)” on page 478.
   - To determine how static routes are imported into the routing and forwarding tables, see “Example: Controlling Static Routes in the Routing and Forwarding Tables (CLI)” on page 481.
   - To define default properties for static routes, see “Example: Defining Default Behavior for All Static Routes (CLI)” on page 483.
   - To check the configuration, see “Verifying the Static Route Configuration” on page 483.

### Table 129: Configuring Basic Static Routes

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Static level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter edit routing-options static</td>
</tr>
<tr>
<td>Add the static route 192.168.47.5/32, and define the next-hop address 10.10.10.10.</td>
<td>Define the static route and set the next-hop address: set route 192.168.47.5 next-hop 10.10.10.10</td>
</tr>
</tbody>
</table>

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding Basic Static Routing on page 476
- Static Routing Configuration Overview on page 475

### Static Route Selection

- Understanding Static Route Preferences and Qualified Next Hops on page 477
- Example: Controlling Static Route Selection (CLI) on page 478

**Understanding Static Route Preferences and Qualified Next Hops**

A static route destination address can have multiple next hops associated with it. In this case, multiple routes are inserted into the routing table, and route selection must occur. Because the primary criterion for route selection is the route preference, you can control the routes that are used as the primary route for a particular destination...
by setting the route preference associated with a particular next hop. The routes with a higher preference are always used to route traffic. When you do not set a preferred route, traffic is alternated between routes in round-robin fashion.

In general, the default properties assigned to a static route apply to all the next-hop addresses configured for the static route. If, however, you want to configure two possible next-hop addresses for a particular route and have them treated differently, you can define one as a qualified next hop.

Qualified next hops allow you to associate one or more properties with a particular next-hop address. You can set an overall preference for a particular static route and then specify a different preference for the qualified next hop. For example, suppose two next-hop addresses (10.10.10.10 and 10.10.10.7) are associated with the static route 192.168.47.5/32. A general preference is assigned to the entire static route, and then a different preference is assigned to only the qualified next-hop address 10.10.10.7. For example:

```plaintext
route 192.168.47.5/32 {
    next-hop 10.10.10.10;
    qualified-next-hop 10.10.10.7 {
        preference 2;
    }
    preference 6;
}
```

In this example, the qualified next hop 10.10.10.7 is assigned the preference 2, and the next-hop 10.10.10.10 is assigned the preference 6.

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Example: Controlling Static Route Selection (CLI) on page 478

**Example: Controlling Static Route Selection (CLI)**

When multiple next hops exist for a single static route (see Figure 55 on page 479), you can specify how traffic is to be routed to the destination.
In this example, the static route 192.168.47.5/32 has two possible next hops. Because of the links between those next-hop hosts, host 10.10.10.7 is the preferred path. To configure the static route 192.168.47.5/32 with two next hops and give preference to host 10.10.10.7, follow these steps:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 130 on page 479.
3. If you are finished configuring the router, commit the configuration.
4. Go on to one of the following procedures:
   - To determine how static routes are imported into the routing and forwarding tables, see “Example: Controlling Static Routes in the Routing and Forwarding Tables (CLI)” on page 481.
   - To define default properties for static routes, see “Example: Defining Default Behavior for All Static Routes (CLI)” on page 483.
   - To check the configuration, see “Verifying the Static Route Configuration” on page 483.

### Table 130: Controlling Static Route Selection

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Static level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter</td>
</tr>
<tr>
<td></td>
<td>edit routing-options static</td>
</tr>
<tr>
<td>Add the static route 192.168.47.5/32, and define the next-hop address 10.10.10.10.</td>
<td>Define the static route and set the next-hop address:</td>
</tr>
<tr>
<td></td>
<td>set route 192.168.47.5 next-hop 10.10.10.10</td>
</tr>
<tr>
<td>Set the preference for the 10.10.10.10 next hop to 7</td>
<td>Set the preference to 7:</td>
</tr>
<tr>
<td></td>
<td>set route 192.168.47.5 next-hop 10.10.10.10 preference 7</td>
</tr>
</tbody>
</table>
### Table 130: Controlling Static Route Selection (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the qualified next-hop address <strong>10.10.10.7</strong>.</td>
<td>Set the qualified-next-hop address:</td>
</tr>
<tr>
<td></td>
<td><code>set route 192.168.47.5 qualified-next-hop 10.10.10.7</code></td>
</tr>
<tr>
<td>Set the preference for the <strong>10.10.10.7</strong> qualified next hop to 6.</td>
<td>Set the preference to 6:</td>
</tr>
<tr>
<td></td>
<td><code>set route 192.168.47.5 qualified-next-hop 10.10.10.7 preference 6</code></td>
</tr>
</tbody>
</table>

### Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding Static Route Preferences and Qualified Next Hops on page 477
- Static Routing Configuration Overview on page 475

### Static Route Control in Routing and Forwarding Tables

- Understanding Static Route Control in Routing and Forwarding Tables on page 480
- Example: Controlling Static Routes in the Routing and Forwarding Tables (CLI) on page 481

### Understanding Static Route Control in Routing and Forwarding Tables

You can control the importation of static routes into the routing and forwarding tables in a number of ways. Primary ways include assigning one or more of the following attributes to the route:

- **retain**—Keeps the route in the forwarding table after the routing process shuts down or the device reboots.
- **no-readvertise**—Prevents the route from being readvertised to other routing protocols.
- **passive**—Rejects traffic destined for the route.

This topic includes the following sections:

- Route Retention on page 480
- Readvertisement Prevention on page 481
- Forced Rejection of Passive Route Traffic on page 481

### Route Retention

By default, static routes are not retained in the forwarding table when the routing process shuts down. When the routing process starts up again, any routes configured as static routes must be added to the forwarding table again. To avoid this latency, routes can be flagged as **retain**, so that they are kept in the forwarding table even
after the routing process shuts down. Retention ensures that the routes are always in the forwarding table, even immediately after a system reboot.

**Readvertisement Prevention**

Static routes are eligible for readvertisement by other routing protocols by default. In a stub area where you might not want to readvertise these static routes under any circumstances, you can flag the static routes as `no-readvertise`.

**Forced Rejection of Passive Route Traffic**

Generally, only active routes are included in the routing and forwarding tables. If a static route’s next-hop address is unreachable, the route is marked `passive`, and it is not included in the routing or forwarding tables. To force a route to be included in the routing tables regardless of next-hop reachability, you can flag the route as `passive`. If a route is flagged `passive` and its next-hop address is unreachable, the route is included in the routing table and all traffic destined for the route is rejected.

**Related Topics**

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Example: Controlling Static Routes in the Routing and Forwarding Tables (CLI) on page 481

**Example: Controlling Static Routes in the Routing and Forwarding Tables (CLI)**

Static routes have a number of attributes that define how they are inserted and maintained in the routing and forwarding tables. To customize this behavior for the static route `192.168.47.5/32`, perform these steps:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 131 on page 481.
3. If you are finished configuring the router, commit the configuration.
4. Go on to one of the following procedures:
   - To define default properties for static routes, see “Example: Defining Default Behavior for All Static Routes (CLI)” on page 483.
   - To check the configuration, see “Verifying the Static Route Configuration” on page 483.

**Table 131: Controlling Static Routes in the Routing and Forwarding Tables**

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <code>192.168.47.5/32</code> level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter <code>edit routing-options static route 192.168.47.5/32</code></td>
</tr>
</tbody>
</table>
Table 131: Controlling Static Routes in the Routing and Forwarding Tables (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify that the route is to be retained in the forwarding table after the routing process shuts down. By default, static routes are not retained.</td>
<td>Set the retain attribute: set retain</td>
</tr>
<tr>
<td>Specify that the static route is not to be readvertised. By default, static routes are eligible to be readvertised.</td>
<td>Set the no-readvertise attribute: set no-readvertise</td>
</tr>
<tr>
<td>Specify that the static route is to be included in the routing table whether the route is active or not. By default, passive routes are not included in the routing table.</td>
<td>Set the passive attribute: set passive</td>
</tr>
</tbody>
</table>

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding Static Route Control in Routing and Forwarding Tables on page 480
- Static Routing Configuration Overview on page 475

Default Static Route Behavior

- Understanding Static Routing Default Properties on page 482
- Example: Defining Default Behavior for All Static Routes (CLI) on page 483

Understanding Static Routing Default Properties

The basic configuration of static routes defines properties for a particular route. To define a set of properties to be used as defaults on all static routes, set those properties as default values. For example:

```plaintext
defaults {
    retain;
    no-readvertise;
    passive;
}
route 0.0.0.0/0 next-hop 192.168.1.1;
route 192.168.47.5/32 {
    next-hop 10.10.10.10;
    qualified-next-hop 10.10.10.7 {
        preference 6;
    }
    preference 2;
}
```

In this example, the retain, no-readvertise, and passive attributes are set as defaults for all static routes. If any local setting for a particular route conflicts with the default values, the local setting supersedes the default.
Attributes that define static route behavior can be configured either at the individual route level or as a default behavior that applies to all static routes. In the case of conflicting configuration, the configuration at the individual route level overrides static route defaults.

**Example: Defining Default Behavior for All Static Routes (CLI)**

To configure static route defaults, perform these steps:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 132 on page 483.
3. If you are finished configuring the router, commit the configuration.
4. To check the configuration, see “Verifying the Static Route Configuration” on page 483.

**Table 132: Defining Static Route Defaults**

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Defaults</strong> level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter</td>
</tr>
<tr>
<td></td>
<td><code>edit routing-options static defaults</code></td>
</tr>
<tr>
<td>Specify that the route is to be retained in the forwarding table after the routing process shuts down. By default, static routes are not retained.</td>
<td>Set the <code>retain</code> attribute:</td>
</tr>
<tr>
<td></td>
<td><code>set retain</code></td>
</tr>
<tr>
<td>Specify that the static route is not to be readvertised. By default, static routes are eligible to be readvertised.</td>
<td>Set the <code>no-readvertise</code> attribute:</td>
</tr>
<tr>
<td></td>
<td><code>set no-readvertise</code></td>
</tr>
<tr>
<td>Specify that the static route is to be included in the routing table whether the route is active or not. By default, passive routes are not included in the routing table.</td>
<td>Set the <code>passive</code> attribute:</td>
</tr>
<tr>
<td></td>
<td><code>set passive</code></td>
</tr>
</tbody>
</table>

**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding Static Routing Default Properties on page 482
- Static Routing Configuration Overview on page 475

**Verifying the Static Route Configuration**

**Purpose**

Verify that the static routes are in the routing table and that those routes are active.
**Action**  
From the CLI, enter the `show route terse` command.

**Sample Output**  
```plaintext
user@host> show route terse  
inet.0: 20 destinations, 20 routes (20 active, 0 holddown, 0 hidden)  
+ = Active Route, - = Last Active, * = Both  
A Destination        P Prf   Metric 1   Metric 2  Next hop        AS path  
* 192.168.47.5/32        S   5                        Reject  
* 172.16.0.0/12      S   5                       >192.168.71.254  
* 192.168.0.0/18     S   5                       >192.168.71.254  
* 192.168.40.0/22    S   5                       >192.168.71.254  
* 192.168.64.0/18    S   5                       >192.168.71.254  
* 192.168.64.0/21    D   0                       >fxp0.0  
* 192.168.71.246/32  L   0                        Local  
* 192.168.220.4/30    D   0                       >ge-0/0/1.0  
* 192.168.220.5/32    L   0                        Local  
* 192.168.220.8/30    D   0                       >ge-0/0/2.0  
* 192.168.220.9/32    L   0                        Local  
* 192.168.220.12/30   D   0                       >ge-0/0/3.0  
* 192.168.220.13/32   L   0                        Local  
* 192.168.220.17/32   L   0                        Reject  
* 192.168.220.21/32   L   0                        Reject  
* 192.168.220.24/30   D   0                       >at-1/0/0.0  
* 192.168.220.25/32   L   0                        Local  
* 192.168.220.28/30   D   0                       >at-1/0/1.0  
* 192.168.220.29/32   L   0                        Local  
* 224.0.0.9/32       R 100          1             MultiRecv  
```

**Meaning**  
The output shows a list of the routes that are currently in the inet.0 routing table. Verify the following information:

- Each configured static route is present. Routes are listed in ascending order by IP address. Static routes are identified with an *S* in the protocol (P) column of the output.

- Each static route is active. Routes that are active show the next-hop IP address in the **Next hop** column. If a route’s next-hop address is unreachable, the next-hop address is identified as **Reject**. These routes are not active routes, but they appear in the routing table because the **passive** attribute is set.

- The preference for each static route is correct. The preference for a particular route is listed in the **Prf** column of the output.

**Related Topics**  
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Static Routing Configuration Overview on page 475
- `show route terse` in the *Junos Routing Protocols and Policies Command Reference*
Chapter 18
RIP

RIP Overview

In a RIP network, each router's forwarding table is distributed among the nodes through the flooding of routing table information. Because topology changes are flooded throughout the network, every node maintains the same list of destinations. Packets are then routed to these destinations based on path-cost calculations done at each node in the network.

NOTE: In general, the term RIP refers to RIP version 1 and RIP version 2.

This topic contains the following sections:
- Distance-Vector Routing Protocols on page 485
- Maximizing Hop Count on page 486
- RIP Packets on page 486
- Split Horizon and Poison Reverse Efficiency Techniques on page 487
- Limitations of Unidirectional Connectivity on page 488

Distance-Vector Routing Protocols

Distance-vector routing protocols transmit routing information that includes a distance vector, typically expressed as the number of hops to the destination. This information is flooded out all protocol-enabled interfaces at regular intervals (every 30 seconds in the case of RIP) to create a network map that is stored in each node’s local topology database. Figure 56 on page 486 shows how distance-vector routing works.
In Figure 56 on page 486, Routers A and B have RIP enabled on adjacent interfaces. Router A has known RIP neighbors Routers C, D, and E, which are 1, 2, and 3 hops away, respectively. Router B has known RIP neighbors Routers X, Y, and Z, which are 1, 2, and 3 hops away, respectively. Every 30 seconds, each router floods its entire routing table information out all RIP-enabled interfaces. In this case, flooding exchanges routing table information across the RIP link.

When Router A receives routing information from Router B, it adds 1 to the hop count to determine the new hop count. For example, Router X has a hop count of 1, but when Router A imports the route to X, the new hop count is 2. The imported route also includes information about where the route was learned, so that the original route is imported as a route to Router X through Router B with a hop count of 2.

When multiple routes to the same host are received, RIP uses the distance-vector algorithm to determine which path to import into the forwarding table. The route with the smallest hop count is imported. If there are multiple routes with the same hop count, all are imported into the forwarding table, and traffic is sent along the paths in round-robin fashion.

**Maximizing Hop Count**

The successful routing of traffic across a RIP network requires that every node in the network maintain the same view of the topology. Topology information is broadcast between RIP neighbors every 30 seconds. If Router A is many hops away from a new host, Router B, the route to B might take significant time to propagate through the network and be imported into Router A’s routing table. If the two routers are 5 hops away from each other, Router A cannot import the route to Router B until 2.5 minutes after Router B is online. For large numbers of hops, the delay becomes prohibitive. To help prevent this delay from growing arbitrarily large, RIP enforces a maximum hop count of 15 hops. Any prefix that is more than 15 hops away is treated as unreachable and assigned a hop count equal to infinity. This maximum hop count is called the network diameter.

**RIP Packets**

Routing information is exchanged in a RIP network by RIP request and RIP response packets. A router that has just booted can broadcast a RIP request on all RIP-enabled interfaces. Any routers running RIP on those links receive the request and respond.
by sending a RIP response packet immediately to the router. The response packet contains the routing table information required to build the local copy of the network topology map.

In the absence of RIP request packets, all RIP routers broadcast a RIP response packet every 30 seconds on all RIP-enabled interfaces. The RIP broadcast is the primary way in which topology information is flooded throughout the network.

Once a router learns about a particular destination through RIP, it starts a timer. Every time it receives a new response packet with information about the destination, the router resets the timer to zero. However, if the router receives no updates about a particular destination for 180 seconds, it removes the destination from its RIP routing table.

In addition to the regular transmission of RIP packets every 30 seconds, if a router detects a new neighbor or detects that an interface is unavailable, it generates a triggered update. The new routing information is immediately broadcast out all RIP-enabled interfaces, and the change is reflected in all subsequent RIP response packets.

### Split Horizon and Poison Reverse Efficiency Techniques

Because RIP functions by periodically flooding the entire routing table out to the network, it generates a lot of traffic. The split horizon and poison reverse techniques can help reduce the amount of network traffic originated by RIP hosts and make the transmission of routing information more efficient.

If a router receives a set of route advertisements on a particular interface, RIP determines that those advertisements do not need to be retransmitted out the same interface. This technique, known as split horizon, helps limit the amount of RIP routing traffic by eliminating information that other neighbors on that interface have already learned. Figure 57 on page 487 shows an example of the split horizon technique.

---

**Figure 57: Split Horizon Example**

In Figure 57 on page 487, Router A advertises routes to Routers C, D, and E to Router B. In this example, Router A can reach Router C in 2 hops. When Router A advertises the route to Router B, B imports it as a route to Router C through Router A in 3 hops. If Router B then readvertised this route to Router A, A would import it as a route to Router C through Router B in 4 hops. However, the advertisement from Router B to Router A is unnecessary, because Router A can already reach the route in 2 hops.
The split horizon technique helps reduce extra traffic by eliminating this type of route advertisement.

Similarly, the poison reverse technique helps to optimize the transmission of routing information and improve the time to reach network convergence. If Router A learns about unreachable routes through one of its interfaces, it advertises those routes as unreachable (hop count of 16) out the same interface. Figure 58 on page 488 shows an example of the poison reverse technique.

**Figure 58: Poison Reverse Example**

In Figure 58 on page 488, Router A learns through one of its interfaces that routes to Routers C, D, and E are unreachable. Router A readvertises those routes out the same interface as unreachable. The advertisement informs Router B that Hosts C, D, and E are definitely not reachable through Router A.

**Limitations of Unidirectional Connectivity**

Because RIP processes routing information based solely on the receipt of routing table updates, it cannot ensure bidirectional connectivity. As Figure 59 on page 488 shows, RIP networks are limited by their unidirectional connectivity.

**Figure 59: Limitations of Unidirectional Connectivity**

In Figure 59 on page 488, Routers A and D flood their routing table information to Router B. Because the path to Router E has the fewest hops when routed through
Router A, that route is imported into Router B’s forwarding table. However, suppose that Router A can transmit traffic but is not receiving traffic from Router B because of an unavailable link or invalid routing policy. If the only route to Router E is through Router A, any traffic destined for Router A is lost, because bidirectional connectivity was never established.

OSPF establishes bidirectional connectivity with a three-way handshake.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Routing Overview on page 467
- RIP Configuration Overview on page 491
- Understanding Basic RIP Routing on page 492
- Understanding RIP Traffic Control with Metrics on page 493
- Understanding RIP Authentication on page 497
- RIPng Overview on page 489
- OSPF Overview on page 503

RIPng Overview

The Routing Information Protocol next generation (RIPng) is an interior gateway protocol (IGP) that uses a distance-vector algorithm to determine the best route to a destination, using hop count as the metric. RIPng exchanges routing information used to compute routes and is intended for IP version 6 (IPv6)-based networks. RIPng is disabled by default.

On devices in secure context, IPv6 is disabled. You must enable IPv6 to use RIPng. For instructions, see the Junos OS Interfaces Configuration Guide for Security Devices.

This topic contains the following sections:

- RIPng Protocol Overview on page 489
- RIPng Standards on page 490
- RIPng Packets on page 490

RIPng Protocol Overview

The RIPng IGP uses the Bellman-Ford distance-vector algorithm to determine the best route to a destination, using hop count as the metric. RIPng allows hosts and routers to exchange information for computing routes through an IP-based network. RIPng is intended to act as an IGP for moderately-sized autonomous systems.

RIPng is a distinct routing protocol from RIPv2. The JUNOS Software implementation of RIPng is similar to RIPv2, but has the following differences:

- RIPng does not need to implement authentication on packets.
- JUNOS Software does not support multiple instances of RIPng.
JUNOS Software does not support RIPng routing table groups.

RIPng is a UDP-based protocol and uses UDP port 521.

RIPng has the following architectural limitations:

- The longest network path cannot exceed 15 hops (assuming that each network, or hop, has a cost of 1).
- RIPng is prone to routing loops when the routing tables are reconstructed. Especially when RIPng is implemented in large networks that consist of several hundred routers, RIPng might take an extremely long time to resolve routing loops.
- RIPng uses only a fixed metric to select a route. Other IGPs use additional parameters, such as measured delay, reliability, and load.

**RIPng Standards**

RIPng is defined in the following documents:

- RFC 2080, *RIPng for IPv6*
- RFC 2081, *RIPng Protocol Applicability Statement*

To access Internet Requests for Comments (RFCs) and drafts, see the Internet Engineering Task Force (IETF) website at [http://www.ietf.org](http://www.ietf.org).

**RIPng Packets**

A RIPng packet header contains the following fields:

- **Command**—Indicates whether the packet is a request or response message. Request messages seek information for the router’s routing table. Response messages are sent periodically or when a request message is received. Periodic response messages are called update messages. Update messages contain the command and version fields and a set of destinations and metrics.
- **Version number**—Specifies the version of RIPng that the originating router is running. This is currently set to Version 1.

The rest of the RIPng packet contains a list of routing table entries consisting of the following fields:

- **Destination prefix**—128-bit IPv6 address prefix for the destination.
- **Prefix length**—Number of significant bits in the prefix.
- **Metric**—Value of the metric advertised for the address.
- **Route tag**—A route attribute that must be advertised and redistributed with the route. Primarily, the route tag distinguishes external RIPng routes from internal RIPng routes when routes must be redistributed across an exterior gateway protocol (EGP).
Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Routing Overview on page 467
- RIP Overview on page 485
- Configuring RIPng in the Junos Routing Protocols Configuration Guide
- Minimum RIPng Configuration in the Junos Routing Protocols Configuration Guide

RIP Configuration Overview

To achieve basic connectivity between all RIP hosts in a RIP network, you enable RIP on every interface that is expected to transmit and receive RIP traffic, as described in the steps that follow.

To configure a RIP network:

3. Define RIP groups, which are logical groupings of interfaces, and add interfaces to the groups. Then, configure a routing policy to export directly connected routes and routes learned through RIP routing exchanges. See “Example: Configuring a Basic RIP Network (CLI)” on page 492.
4. (Optional) Configure metrics to control traffic through the RIP network. See “Example: Controlling Traffic with the Incoming Metric (CLI)” on page 494 and “Example: Controlling Traffic with the Outgoing Metric (CLI)” on page 496.
5. (Optional) Configure authentication to ensure that only trusted routers participate in the autonomous system’s routing. See “Enabling Authentication with Plain-Text Passwords (CLI Procedure)” on page 498 and “Enabling Authentication with MD5 Authentication (CLI Procedure)” on page 498.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- RIP Overview on page 485
- Verifying a RIP Configuration on page 499
- Configuring RIP in the Junos Routing Protocols Configuration Guide
- Minimum RIP Configuration in the Junos Routing Protocols Configuration Guide

Basic RIP Routing

- Understanding Basic RIP Routing on page 492
- Example: Configuring a Basic RIP Network (CLI) on page 492
Understanding Basic RIP Routing

RIP is an interior gateway protocol (IGP) that routes packets within a single autonomous system (AS). By default, RIP does not advertise the subnets that are directly connected through the device's interfaces. For traffic to pass through a RIP network, you must create a routing policy to export these routes. Advertising only the direct routes propagates the routes to the immediately adjacent RIP-enabled router only. To propagate all routes through the entire RIP network, you must configure the routing policy to export the routes learned through RIP.

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- RIP Overview on page 485
- Example: Configuring a Basic RIP Network (CLI) on page 492

Example: Configuring a Basic RIP Network (CLI)

To use RIP on the device, you must configure RIP on all the RIP interfaces within a network like the one shown in Figure 60 on page 492.

Figure 60: Typical RIP Network Topology

To configure a RIP network like the one in Figure 60 on page 492, with a routing policy, perform these steps on each device in the network:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 133 on page 493.
3. If you are finished configuring the router, commit the configuration.

After you add the appropriate interfaces to the RIP group, RIP begins sending routing information. No additional configuration is required to enable RIP traffic on the network.
Table 133: Configuring a RIP Network

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Rip</strong> level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter <code>edit protocols rip</code></td>
</tr>
<tr>
<td>Create the RIP group <strong>alpha1</strong>.</td>
<td>1. Create the RIP group <strong>alpha1</strong>, and add an interface: <code>set group alpha1 neighbor ge-0/0/0.0</code>&lt;br&gt;2. Repeat Step 1 for each interface on this device that you are adding to the RIP group. Only one interface is required.</td>
</tr>
<tr>
<td>Configure a routing policy to advertise directly connected routes.</td>
<td>1. From the [edit] hierarchy level, enter <code>edit policy-options</code>&lt;br&gt;2. Set the match condition to match on direct routes: <code>set policy-statement advertise-rip-routes term from-direct from protocol direct</code>&lt;br&gt;3. Set the match action to accept these routes: <code>set policy-statement advertise-rip-routes term from-direct then accept</code></td>
</tr>
<tr>
<td>Configure the previous routing policy to advertise routes learned from RIP.</td>
<td>1. From the [edit] hierarchy level, enter <code>edit policy-options</code>&lt;br&gt;2. Set the match condition to match on direct routes: <code>set policy-statement advertise-rip-routes term from-rip from protocol rip</code>&lt;br&gt;3. Set the match action to accept these routes: <code>set policy-statement advertise-rip-routes term from-rip then accept</code></td>
</tr>
</tbody>
</table>

**Related Topics**
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding Basic RIP Routing on page 492
- RIP Overview on page 485

**RIP Traffic Control Through Metrics**
- Understanding RIP Traffic Control with Metrics on page 493
- Example: Controlling Traffic with the Incoming Metric (CLI) on page 494
- Example: Controlling Traffic with the Outgoing Metric (CLI) on page 496

**Understanding RIP Traffic Control with Metrics**
To tune a RIP network and control traffic flowing through the network, you increase or decrease the cost of the paths through the network. RIP provides two ways to modify the path cost: an incoming metric and an outgoing metric, which are each
set to 1 by default. These metrics are attributes that manually specify the cost of any route advertised through a host. By increasing or decreasing the metrics—and thus the cost—of links throughout the network, you can control packet transmission across the network.

The incoming metric modifies the cost of an individual segment when a route across the segment is imported into the routing table. For example, if you set the incoming metric on the segment to 3, the individual segment cost along the link is changed from 1 to 3. The increased cost affects all route calculations through that link. Other routes that were previously excluded because of a high hop count might now be selected into the router’s forwarding table.

The outgoing metric modifies the path cost for all the routes advertised out a particular interface. Unlike the incoming metric, the outgoing metric modifies the routes that other routers are learning and thereby controls the way they send traffic.

If an exported route was learned from a member of the same RIP group, the metric associated with that route is the normal RIP metric. For example, a RIP route with a metric of 5 learned from a neighbor configured with an incoming metric of 2 is advertised with a combined metric of 7 when advertised to neighbors in the same group. However, if this route was learned from a RIP neighbor in a different group or from a different protocol, the route is advertised with the metric value configured in the outgoing metric for that group.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- RIP Overview on page 485
- Example: Controlling Traffic with the Incoming Metric (CLI) on page 494
- Example: Controlling Traffic with the Outgoing Metric (CLI) on page 496

**Example: Controlling Traffic with the Incoming Metric (CLI)**

Depending on the RIP network topology and the links between nodes in the network, you might want to control traffic flow through the network to maximize flow across higher-bandwidth links. Figure 61 on page 494 shows a network with alternate routes between Routers A and D.

Figure 61: Controlling Traffic in a RIP Network with the Incoming Metric
In this example, routes to Router D are received by Router A across both of its RIP-enabled interfaces. Because the route through Router B and the route through Router C have the same number of hops, both routes are imported into the forwarding table. However, because the T3 link from Router B to Router D has a higher bandwidth than the T1 link from Router C to Router D, you want traffic to flow from A through B to D.

To force this flow, you can modify the route metrics as they are imported into Router A’s routing table. By setting the incoming metric on the interface from Router A to Router C, you modify the metric on all routes received through that interface. Setting the incoming route metric on Router A changes only the routes in Router A’s routing table, and affects only how Router A sends traffic to Router D. Router D’s route selection is based on its own routing table, which, by default, includes no adjusted metric values.

In the example, Router C receives a route advertisement from Router D and readvertises the route to Router A. When Router A receives the route, it applies the incoming metric on the interface. Instead of incrementing the metric by 1 (the default), Router A increments it by 3 (the configured incoming metric), giving the route from Router A to Router D through Router C a total path metric of 4. Because the route through Router B has a metric of 2, it becomes the preferred route for all traffic from Router A to Router D.

To modify the incoming metric on all routes learned on the link between Router A and Router C and to force traffic through Router B:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 134 on page 495.
3. If you are finished configuring the router, commit the configuration.

Table 134: Modifying the Incoming Metric

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the configuration hierarchy, navigate to the level of an</td>
<td>From the [edit] hierarchy level, enter</td>
</tr>
<tr>
<td>interface in the alpha1 RIP group.</td>
<td>edit protocols rip group alpha1 neighbor ge-0/0/0</td>
</tr>
<tr>
<td>Increase the incoming metric to 3.</td>
<td>Set the incoming metric to 3:</td>
</tr>
<tr>
<td></td>
<td>set metric-in 3</td>
</tr>
</tbody>
</table>

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding RIP Traffic Control with Metrics on page 495
- Example: Controlling Traffic with the Outgoing Metric (CLI) on page 496
- RIP Overview on page 485
**Example: Controlling Traffic with the Outgoing Metric (CLI)**

Figure 62 on page 496 shows a RIP network with alternative routes between Routers A and D.

**Figure 62: Controlling Traffic in a RIP Network with the Outgoing Metric**

In this example, each route from Router A to Router D has two hops. However, because the link from Router A to Router B in RIP group Beta 1 has a higher bandwidth than the link from Router A to Router C in RIP group Alpha 1, you want traffic from Router D to Router A to flow through Router B. To control the way Router D sends traffic to Router A, you can alter the routes that Router D receives by configuring the outgoing metric on Router A's interfaces in the Alpha 1 RIP group.

If the outgoing metric for the Alpha 1 RIP group—the A-to-C link—is changed to 3, Router D calculates the total path metric from to A through C as 4. In contrast, the unchanged default total path metric to A through B in the Beta 1 RIP group is 2. The fact that Router A's interfaces belong to two different RIP groups allows you to configure two different outgoing metrics on its interfaces, because you configure path metrics at the group level.

By configuring the **incoming** metric, you control the way Router A sends traffic to Router D. By configuring the **outgoing** metric on the same router, you control the way Router D sends traffic to Router A.

To modify the outgoing metric on Router A and force traffic through Router B:
1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 135 on page 497.
3. If you are finished configuring the router, commit the configuration.
Table 135: Modifying the Outgoing Metric

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the alpha1 level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter</td>
</tr>
<tr>
<td></td>
<td>edit protocols rip group alpha1</td>
</tr>
<tr>
<td>Increase the outgoing metric to 3.</td>
<td>Set the outgoing metric to 3.</td>
</tr>
<tr>
<td></td>
<td>set metric-out 3</td>
</tr>
</tbody>
</table>

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding RIP Traffic Control with Metrics on page 493
- Example: Controlling Traffic with the Incoming Metric (CLI) on page 494
- RIP Overview on page 485

RIP Authentication

- Understanding RIP Authentication on page 497
- Enabling Authentication with Plain-Text Passwords (CLI Procedure) on page 498
- Enabling Authentication with MD5 Authentication (CLI Procedure) on page 498

Understanding RIP Authentication

RIPv2 provides authentication support so that RIP links can require authentication keys (passwords) before they become active. Authentication provides an additional layer of security on the network beyond the other security features. By default, this authentication is disabled.

Authentication keys can be specified in either plain-text or MD5 form. Authentication requires all routers within the RIP network or subnetwork to have the same authentication type and key (password) configured.

This type of authentication is not supported on RIPv1 networks.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- RIP Overview on page 485
- Enabling Authentication with Plain-Text Passwords (CLI Procedure) on page 498
- Enabling Authentication with MD5 Authentication (CLI Procedure) on page 498
Enabling Authentication with Plain-Text Passwords (CLI Procedure)

To configure authentication that requires a plain-text password to be included in the transmitted packet, enable simple authentication by performing these steps on all RIP devices in the network:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 136 on page 498.
3. If you are finished configuring the router, commit the configuration.

Table 136: Configuring Simple RIP Authentication

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to <strong>Rip</strong> level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter <code>edit protocols rip</code></td>
</tr>
<tr>
<td>Set the authentication type to <strong>simple</strong>.</td>
<td>Set the authentication type to <strong>simple</strong>: <code>set authentication-type simple</code></td>
</tr>
<tr>
<td>Set the authentication key to a simple-text password.</td>
<td>Set the authentication key to a simple-text password: <code>set authentication-key password</code></td>
</tr>
<tr>
<td>The password can be from 1 through 16 contiguous characters long and can include any ASCII strings.</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding RIP Authentication on page 497
- Enabling Authentication with MD5 Authentication (CLI Procedure) on page 498

Enabling Authentication with MD5 Authentication (CLI Procedure)

To configure authentication that requires an MD5 password to be included in the transmitted packet, enable MD5 authentication by performing these steps on all RIP devices in the network:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 137 on page 499.
3. If you are finished configuring the router, commit the configuration.
Table 137: Configuring MD5 RIP Authentication

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to <strong>Rip</strong> level in the configuration hierarchy.</td>
<td>From the <code>[edit]</code> hierarchy level, enter</td>
</tr>
<tr>
<td></td>
<td><code>edit protocols rip</code></td>
</tr>
<tr>
<td>Set the authentication type to <strong>MD5</strong>.</td>
<td>Set the authentication type to <strong>md5</strong>:</td>
</tr>
<tr>
<td></td>
<td><code>set authentication-type md5</code></td>
</tr>
<tr>
<td>Set the MD5 authentication key (password).</td>
<td>Set the MD5 authentication key:</td>
</tr>
<tr>
<td></td>
<td><code>set authentication-key password</code></td>
</tr>
</tbody>
</table>

The key can be from 1 through 16 contiguous characters long and can include any ASCII strings.

**Related Topics**
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding RIP Authentication on page 497
- Enabling Authentication with Plain-Text Passwords (CLI Procedure) on page 498

**Verifying a RIP Configuration**

To verify a RIP configuration, perform the following tasks:
- Verifying the Exchange of RIP Messages on page 499
- Verifying the RIP-Enabled Interfaces on page 500
- Verifying Reachability of All Hosts in the RIP Network on page 501

**Verifying the Exchange of RIP Messages**

**Purpose**
Verify that RIP messages are being sent and received on all RIP-enabled interfaces.

**Action**
From the CLI, enter the `show rip statistics` command.

**Sample Output**

```
user@host> show rip statistics
RIPv2 info: port 520; holddown 120s.
rtts learned rts held down rqsts dropped resps dropped
10 0 0 0

45s  

Counter                Total      Last 5 min    Last minute
Cities
Updates Sent          2855       11           2
Triggered Updates Sent 5           0         0
Responses Sent        0           0         0
Bad Messages          0           0         0
RIPv1 Updates Received 0           0         0
RIPv1 Bad Route Entries 0           0         0
RIPv1 Updates Ignored  0           0         0
```
<table>
<thead>
<tr>
<th>Metric</th>
<th>Total</th>
<th>Last 5 min</th>
<th>Last minute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updates Sent</td>
<td>2855</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>Triggered Updates Sent</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Responses Sent</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bad Messages</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPv1 Updates Received</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPv1 Bad Route Entries</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPv1 Updates Ignored</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPv2 Updates Received</td>
<td>2864</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>RIPv2 Bad Route Entries</td>
<td>14</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIPv2 Updates Ignored</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Authentication Failures</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIP Requests Received</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RIP Requests Ignored</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Meaning

The output shows the number of RIP routes learned. It also shows the number of RIP updates sent and received on the RIP-enabled interfaces. Verify the following information:

- The number of RIP routes learned matches the number of expected routes learned. Subnets learned by direct connectivity through an outgoing interface are not listed as RIP routes.
- RIP updates are being sent on each RIP-enabled interface. If no updates are being sent, the routing policy might not be configured to export routes.
- RIP updates are being received on each RIP-enabled interface. If no updates are being received, the routing policy might not be configured to export routes on the host connected to that subnet. The lack of updates might also indicate an authentication error.

Verifying the RIP-Enabled Interfaces

Purpose

Verify that all the RIP-enabled interfaces are available and active.

Action

From the CLI, enter the `show rip neighbor` command.

Sample Output

```
user@host> show rip neighbor
Source Neighbor     Destination State Address Send Address Receive Address Mode Mode Met
-------- -----       ----------------------- ---------- ---------- ------- ------- ---
ge-0/0/0.0 Dn (null) (null) mcast both       1
ge-0/0/1.0 Up 192.168.220.5 224.0.0.9 mcast both       1
```
Meaning  The output shows a list of the RIP neighbors that are configured on the device. Verify the following information:

- Each configured interface is present. Interfaces are listed in alphabetical order.
- Each configured interface is up. The state of the interface is listed in the **Destination State** column. A state of **Up** indicates that the link is passing RIP traffic. A state of **Dn** indicates that the link is not passing RIP traffic. In a point-to-point link, this state generally means that either the end point is not configured for RIP or the link is unavailable.

**Verifying Reachability of All Hosts in the RIP Network**

**Purpose**  By using the traceroute tool on each loopback address in the network, verify that all hosts in the RIP network are reachable from each Juniper Networks device.

**Action**  For each device in the RIP network:

1. In the J-Web interface, select **Troubleshoot > Traceroute**.
2. In the Remote Host box, type the name of a host for which you want to verify reachability from the device.
3. Click **Start**. Output appears on a separate page.

**Sample Output**

1 172.17.40.254 (172.17.40.254) 0.362 ms 0.284 ms 0.251 ms
2 routera-fxp0.englab.mycompany.net (192.168.71.246) 0.251 ms 0.235 ms 0.200 ms

**Meaning**  Each numbered row in the output indicates a routing hop in the path to the host. The three-time increments indicate the round-trip time (RTT) between the device and the hop for each traceroute packet.

To ensure that the RIP network is healthy, verify the following information:

- The final hop in the list is the host you want to reach.
- The number of expected hops to the host matches the number of hops in the traceroute output. The appearance of more hops than expected in the output indicates that a network segment is probably unreachable. It might also indicate that the incoming or outgoing metric on one or more hosts has been set unexpectedly.

**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- RIP Configuration Overview on page 491
- show rip statistics in the Junos Routing Protocols and Policies Command Reference
- show rip neighbor in the Junos Routing Protocols and Policies Command Reference
- traceroute in the Junos System Basics and Services Command Reference
- RIP Overview on page 485
Verifying Reachability of All Hosts in the RIP Network
OSPF Overview

OSPF is an interior gateway protocol (IGP) that routes packets within a single autonomous system (AS). In an OSPF network, the network topology is distributed among the nodes of the AS and is regularly updated through the exchange of link-state advertisements (LSAs). As a result, OSPF is known as a link-state protocol. Because topology changes are flooded throughout the network, every node maintains the same copy of the network map in its local topological database. Packets are then routed based on the shared topology using the shortest path first (SPF) algorithm.

**NOTE:** In this topic, the term OSPF refers to OSPF version 2 and OSPF version 3.

OSPF creates a topology map by flooding LSAs across OSPF-enabled links. LSAs announce the presence of OSPF-enabled interfaces to adjacent OSPF interfaces. The exchange of LSAs establishes bidirectional connectivity between all adjacent OSPF interfaces (neighbors) using a three-way handshake, as shown in Figure 63 on page 504.
Figure 63: OSPF Three-Way Handshake

In Figure 63 on page 504, Router A sends hello packets out all its OSPF-enabled interfaces when it comes online. Router B receives the packet, which establishes that Router B can receive traffic from Router A. Router B generates a response to Router A to acknowledge receipt of the hello packet. When Router A receives the response, it establishes that Router B can receive traffic from Router A. Router A then generates a final response packet to inform Router B that Router A can receive traffic from Router B. This three-way handshake ensures bidirectional connectivity.

As new neighbors are added to the network or existing neighbors lose connectivity, the adjacencies in the topology map are modified accordingly through the exchange (or absence) of LSAs. These LSAs advertise only the incremental changes in the network, which helps minimize the amount of OSPF traffic on the network. The adjacencies are shared and used to create the network topology in the topological database.

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Routing Overview on page 467
- OSPF Configuration Overview on page 504
- Understanding OSPF Designated Routers on page 506
- Understanding OSPF Areas, Area Border Routers, and Backbones on page 508
- Understanding OSPF Stub Areas and Not-So-Stubby Areas on page 513
- Understanding OSPF Authentication on page 515
- Understanding OSPF Traffic Control on page 517

OSPF Configuration Overview

To activate OSPF on a network, you must enable the protocol on all interfaces within the network on which OSPF traffic is to travel, as explained in the steps that follow. To enable OSPF, you must configure one or more interfaces on the device within an OSPF area. Once the interfaces are configured, OSPF link-state advertisements (LSAs) are transmitted on all OSPF-enabled interfaces, and the network topology is shared throughout the network.
To configure the Juniper Networks device as a node in an OSPF network:


3. Configure the router identifiers for the devices in your OSPF network. See “Example: Configuring the OSPF Router Identifier (CLI)” on page 506.

4. Create the backbone area for your OSPF network and add the appropriate interfaces to the area. See “Example: Configuring a Single-Area OSPF Network (CLI)” on page 509.

**NOTE:** Once you complete this step, OSPF begins sending LSAs. No additional configuration is required to enable OSPF traffic on the network.

5. (Optional) Add additional areas to your network and configure area border routers. See “Example: Configuring a Multiarea OSPF Network (CLI)” on page 511.

6. Enable dial-on-demand routing backup on the OSPF-enabled interface if you are configuring OSPF across a demand circuit such as an ISDN link. (You must have already configured an ISDN interface.) Because demand circuits do not pass all traffic required to maintain an OSPF adjacency (hello packets, for example), you configure dial-on-demand routing so individual nodes in an OSPF network can maintain adjacencies despite the lack of LSA exchanges. See the JUNOS Software Interfaces Configuration Guide for Security Devices.

7. (Optional) Reduce the amount of memory that the nodes use to maintain the topology database by configuring stub and not-so-stubby areas. See “Example: Configuring OSPF Stub and Not-So-Stubby Areas (CLI)” on page 514.

8. (Optional) Ensure that only trusted routers participate in the autonomous system’s (AS’s) routing by enabling authentication. See “Example: Enabling Authentication for OSPF Exchanges (CLI)” on page 516.

9. (Optional) Control the flow of traffic across the network by configuring path metrics and route selection. See “Example: Controlling the Cost of Individual OSPF Network Segments (CLI)” on page 518 and “Example: Controlling OSPF Route Selection in the Forwarding Table (CLI)” on page 519.

**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- OSPF Overview on page 503
- Verifying an OSPF Configuration on page 519
- Configuring OSPF in the Junos Routing Protocols Configuration Guide
- Minimum OSPF Configuration in the Junos Routing Protocols Configuration Guide
OSPF Designated Routers

- Understanding OSPF Designated Routers on page 506
- Example: Configuring the OSPF Router Identifier (CLI) on page 506
- Example: Controlling OSPF Designated Router Election (CLI) on page 507

Understanding OSPF Designated Routers

Large LANs that have many routers and therefore many OSPF adjacencies can produce heavy control-packet traffic as link-state advertisements (LSAs) are flooded across the network. To alleviate the potential traffic problem, OSPF uses designated routers. Rather than broadcasting LSAs to all their OSPF neighbors, the routers send their LSAs to the designated router, which processes the LSAs, generates responses, and multicasts topology updates to all OSPF routers.

In LANs, the election of the designated router takes place when the OSPF network is initially established. When the first OSPF links are active, the router with the highest router identifier (defined by the `router-id` configuration value or the loopback address) is elected designated router. The router with the second highest router identifier is elected the backup designated router. If the designated router fails or loses connectivity, the backup designated router assumes its role and a new backup designated router election takes place between all the routers in the OSPF network.

OSPF uses the router identifier to elect a designated router, unless you manually specify a priority value. At designated router election, the router priorities are evaluated first, and the router with the highest priority is elected designated router.

By default, routers have a priority of 128. A priority of 0 marks the router as ineligible to become the designated router. To configure a router so it is always the designated router, set its priority to 255.

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- OSPF Overview on page 503
- Example: Configuring the OSPF Router Identifier (CLI) on page 506
- Example: Controlling OSPF Designated Router Election (CLI) on page 507

Example: Configuring the OSPF Router Identifier (CLI)

To configure the router identifier for the device:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 138 on page 507.
Table 138: Configuring the Router Identifier

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Routing-options level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter <code>edit routing-options</code></td>
</tr>
<tr>
<td>Set the router ID value to the IP address of the device—for example, 177.162.4.24.</td>
<td>Enter <code>set router-id 177.162.4.24</code></td>
</tr>
</tbody>
</table>

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding OSPF Designated Routers on page 506
- Example: Controlling OSPF Designated Router Election (CLI) on page 507
- OSPF Configuration Overview on page 504
- OSPF Overview on page 503

Example: Controlling OSPF Designated Router Election (CLI)

To change the priority of a device to control designated router election:
1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 139 on page 507.

Table 139: Controlling Designated Router Election

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the OSPF interface address for the device. For example, navigate to the ge-0/0/1 level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter <code>edit protocols ospf area 0.0.0.3 interface ge-0/0/1</code></td>
</tr>
<tr>
<td>Set the device priority to a value between 0 and 255—for example, 200. The default value is 128.</td>
<td>Set the priority value: <code>set priority 200</code></td>
</tr>
</tbody>
</table>

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding OSPF Designated Routers on page 506
- Example: Configuring the OSPF Router Identifier (CLI) on page 506
- OSPF Configuration Overview on page 504
- OSPF Overview on page 503
OSPF Areas, Area Border Routers, and Backbone Areas

- Understanding OSPF Areas, Area Border Routers, and Backbones on page 508
- Example: Configuring a Single-Area OSPF Network (CLI) on page 509
- Example: Configuring a Multiarea OSPF Network (CLI) on page 511

Understanding OSPF Areas, Area Border Routers, and Backbones

OSPF networks in an autonomous system (AS) are administratively grouped into areas. Each area within an AS operates like an independent network and has a unique 32-bit area ID, which functions like a network address. Within an area, the topology database contains only information about the area, link-state advertisements (LSAs) are flooded only to nodes within the area, and routes are computed only within the area. Subnetworks are divided into other areas, which are connected to form the whole of the main network.

The central area of an AS, called the backbone area, has a special function and is always assigned the area ID 0.0.0.0. (Within a simple, single-area network, this is also the ID of the area.) Area IDs are unique numeric identifiers, in dotted decimal notation, but they are not IP addresses. Area IDs need only be unique within an AS. All other networks or areas in the AS must be directly connected to the backbone area by a router that has interfaces in more than one area. These connecting routers are called area border routers (ABRs). Figure 64 on page 508 shows an OSPF topology of three areas connected by two ABRs.

![Figure 64: Multiarea OSPF Topology](image)

Because all areas are adjacent to the backbone area, OSPF routers send all traffic not destined for their own area through the backbone area. The ABRs in the backbone area are then responsible for transmitting the traffic through the appropriate ABR to the destination area. The ABRs summarize the link-state records of each area and...
advertise destination address summaries to neighboring areas. The advertisements contain the ID of the area in which each destination lies, so that packets are routed to the appropriate ABR. For example, in the OSPF areas shown in Figure 64 on page 508, packets sent from Router A to Router C are automatically routed through ABR B.

An OSPF restriction requires all areas to be directly connected to the backbone area so that packets can be properly routed. All packets are routed first to the backbone area by default. Packets that are destined for an area other than the backbone area are then routed to the appropriate ABR and on to the remote host within the destination area.

In large networks with many areas, in which direct connectivity between all areas and the backbone area is physically difficult or impossible, you can configure virtual links to connect noncontiguous areas. For example, Figure 65 on page 509 shows a virtual link between a noncontiguous area and the backbone area through an area connected to both.

![Figure 65: OSPF Topology with a Virtual Link](image)

In the topology shown in Figure 65 on page 509, a virtual link is established between area 0.0.0.3 and the backbone area through area 0.0.0.2. All outbound traffic destined for other areas is routed through area 0.0.0.2 to the backbone area and then to the appropriate ABR. All inbound traffic destined for area 0.0.0.3 is routed to the backbone area and then through area 0.0.0.2.

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- OSPF Overview on page 503
- Example: Configuring a Single-Area OSPF Network (CLI) on page 509
- Example: Configuring a Multiarea OSPF Network (CLI) on page 511

Example: Configuring a Single-Area OSPF Network (CLI)

To use OSPF on the device, you must configure at least one OSPF area, like the one shown in Figure 66 on page 510.
To configure a single-area OSPF network with a backbone area, like the one in Figure 66 on page 510, perform these steps on each device in the network:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 140 on page 510.
3. If you are finished configuring the router, commit the configuration.

![Figure 66: Typical Single-Area OSPF Network Topology](image)

Table 140: Configuring a Single-Area OSPF Network

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <code>Ospf</code> level in the configuration hierarchy.</td>
<td>From the <code>[edit]</code> hierarchy level, enter <code>edit protocols ospf</code></td>
</tr>
<tr>
<td>Create the backbone area with area ID <code>0.0.0.0</code></td>
<td>1. Set the backbone area ID to <code>0.0.0.0</code> and add an interface:</td>
</tr>
<tr>
<td>Add interfaces as needed to the OSPF area—for example, <code>ge-0/0/0</code></td>
<td>set area <code>0.0.0.0</code> interface <code>ge-0/0/0</code></td>
</tr>
<tr>
<td>For information about interface names, see <a href="510">JUNOS Software Interfaces Configuration Guide for Security Devices</a>.]</td>
<td>2. Repeat Step 1 for each interface on this device that you are adding to the backbone area. Only one interface is required.</td>
</tr>
</tbody>
</table>

Related Topics

- [Junos OS Feature Support Reference for SRX Series and J Series Devices](510)
- Understanding OSPF Areas, Area Border Routers, and Backbones on page 508
- Example: Configuring a Multiarea OSPF Network (CLI) on page 511
- OSPF Configuration Overview on page 504
- OSPF Overview on page 503
Example: Configuring a Multiarea OSPF Network (CLI)

To reduce traffic and topology maintenance for the devices in an OSPF autonomous system (AS), you can group them into multiple areas, as shown in Figure 67 on page 511.

Figure 67: Typical Multiarea OSPF Network Topology

To configure a multiarea OSPF network shown in Figure 5, perform the following tasks on the appropriate devices in the network. You must create a backbone area. To link each additional area to the backbone area, you must configure one of the devices as an area border router (ABR).

- Creating the Backbone Area on page 511
- Creating Additional OSPF Areas on page 511
- Configuring Area Border Routers on page 512

Creating the Backbone Area

On each device that is to operate as an ABR in the network, create backbone area 0.0.0.0 with at least one interface enabled for OSPF.

For instruction, see “Example: Configuring a Single-Area OSPF Network (CLI)” on page 509.

Creating Additional OSPF Areas

To create additional OSPF areas:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 141 on page 512.
3. If you are finished configuring the router, commit the configuration.
Table 141: Configuring a Multiarea OSPF Network

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Ospf</strong> level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter</td>
</tr>
<tr>
<td></td>
<td><strong>edit protocols ospf</strong></td>
</tr>
<tr>
<td>Create the additional area with a unique area ID, in dotted decimal notation—for example, 0.0.0.2</td>
<td>1. Set the area ID to 0.0.0.2 and add an interface:</td>
</tr>
<tr>
<td></td>
<td>set area 0.0.0.2 interface ge-0/0/0</td>
</tr>
<tr>
<td>Add interfaces as needed to the OSPF area—for example, ge-0/0/0.</td>
<td>2. Repeat Step 1 for each interface on this device that you are adding to the area. Only one interface is required.</td>
</tr>
</tbody>
</table>

Configuring Area Border Routers

To configure an area border router:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 142 on page 512.
3. If you are finished configuring the router, commit the configuration.

After you create the areas on the appropriate devices and add and enable the appropriate interfaces to the areas, no additional configuration is required to enable OSPF traffic within or across the areas.

Table 142: Configuring Area Border Routers

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Ospf</strong> level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter</td>
</tr>
<tr>
<td></td>
<td><strong>edit protocols ospf</strong></td>
</tr>
<tr>
<td>Verify that the backbone area has at least one interface enabled for OSPF.</td>
<td>View the configuration using the show command:</td>
</tr>
<tr>
<td></td>
<td>show</td>
</tr>
<tr>
<td></td>
<td>For example, device B in Figure 67 on page 511 has the following interfaces enabled for OSPF in the backbone area:</td>
</tr>
<tr>
<td></td>
<td>area 0.0.0.0 { interface ge-0/0/0.0; interface ge-0/0/1.0; }</td>
</tr>
<tr>
<td></td>
<td>To enable an interface on the backbone area, see “Example: Configuring a Single-Area OSPF Network (CLI)” on page 509.</td>
</tr>
<tr>
<td>Create the additional area with a unique area ID—for example, 0,0,0,2</td>
<td>1. Set the area ID to 0.0.0.2 and add an interface:</td>
</tr>
<tr>
<td></td>
<td>set area 0.0.0.2 interface ge-0/0/0</td>
</tr>
<tr>
<td>Add interfaces as needed to the OSPF area—for example, ge-0/0/0.</td>
<td>2. Repeat Step 1 for each interface on this device that you are adding to the area. Only one interface is required.</td>
</tr>
</tbody>
</table>
OSPF Stub Areas and Not-So-Stubby Areas

Understanding OSPF Stub Areas and Not-So-Stubby Areas

To control the advertisement of external routes into an area, OSPF uses stub areas. By designating an area border router (ABR) interface to the area as a stub interface, you suppress external route advertisements through the ABR. Instead, the ABR automatically advertises a default route (through itself) in place of the external routes. Packets destined for external routes are automatically sent to the ABR, which acts as a gateway for outbound traffic and routes them appropriately.
For example, area 0.0.0.3 in Figure 68 on page 513 is not directly connected to the outside network. All outbound traffic is routed through the ABR to the backbone and then to the destination addresses. By designating area 0.0.0.3 as a stub area, you reduce the size of the topology database for that area by limiting the route entries to only those routes internal to the area.

Similar to area 0.0.0.3 in Figure 68 on page 513, area 0.0.0.4 has no external connections. However, area 0.0.0.4 has static customer routes that are not internal OSPF routes. You can limit the external route advertisements to the area and advertise the static customer routes by designating it a not-so-stubby area (NSSA). External routes are flooded into the NSSA and then leaked to the other areas, but external routes from other areas are not advertised within the NSSA.

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- OSPF Overview on page 503
- Example: Configuring OSPF Stub and Not-So-Stubby Areas (CLI) on page 514

**Example: Configuring OSPF Stub and Not-So-Stubby Areas (CLI)**

To control the advertisement of external routes into an area, you can create stub areas and not-so-stubby areas (NSSAs) in an OSPF network. In the network shown in Figure 69 on page 514, area 0.0.0.7 has no external connections and can be configured as a stub area. Area 0.0.0.9 only has external connections to static routes and can be configured as an NSSA.

**Figure 69: OSPF Network Topology with Stub Areas and NSSAs**

To configure stub areas and NSSAs in an OSPF network like the one shown in Figure 69 on page 514:

1. Navigate to the top of the configuration hierarchy.
2. To configure each device in area 0.0.0.7 as a stub area router, perform the configuration tasks described in Table 143 on page 515.

3. If you are finished configuring the router, commit the configuration.

Table 143: Configuring Stub Area and Not-So-Stubby Area Routers

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Navigate to the 0.0.0.7 level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter edit protocols ospf area 0.0.0.7</td>
</tr>
<tr>
<td>2. Configure each device in area 0.0.0.7 as a stub router.</td>
<td>1. Set the stub attribute: set stub 2. Repeat Step 1 for every device in the stub area to configure them with the stub parameter for the area.</td>
</tr>
<tr>
<td>3. Navigate to the 0.0.0.9 level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter edit protocols ospf area 0.0.0.9</td>
</tr>
<tr>
<td>4. Configure each device in area 0.0.0.9 as an NSSA router.</td>
<td>1. Set the nssa attribute: set nssa 2. Repeat Step 1 for every device in the NSSA to configure them with the nssa parameter for the area.</td>
</tr>
</tbody>
</table>

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding OSPF Stub Areas and Not-So-Stubby Areas on page 513
- OSPF Configuration Overview on page 504
- OSPF Overview on page 503

**OSPF Authentication**

- Understanding OSPF Authentication on page 515
- Example: Enabling Authentication for OSPF Exchanges (CLI) on page 516

**Understanding OSPF Authentication**

All OSPF version 2 (OSPFv2) protocol exchanges can be authenticated to guarantee that only trusted routers participate in the autonomous system’s (AS’s) routing. By default, OSPF authentication is disabled.
NOTE: OSPFv3 does not support authentication.

You can enable either of two authentication types:

- Simple authentication—Authenticates by means of a plain-text password (key) included in the transmitted packet.
- MD5 authentication—Authenticates by means of an MD5 checksum included in the transmitted packet.

Because OSPF performs authentication at the area level, all routers within the area must have the same authentication and corresponding password (key) configured. For MD5 authentication to work, both the receiving and transmitting routers must have the same MD5 key.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- OSPF Overview on page 503
- Example: Enabling Authentication for OSPF Exchanges (CLI) on page 516

Example: Enabling Authentication for OSPF Exchanges (CLI)

To enable OSPF authentication on the stub area:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 144 on page 516.

Table 144: Enabling OSPF Authentication

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the 0.0.0.0 level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter <code>edit protocols ospf area 0.0.0.0</code></td>
</tr>
<tr>
<td>Set the authentication type for the stub area to either simple or MD5—for example, MD5.</td>
<td>Set the authentication type: <code>set authentication-type md5</code></td>
</tr>
<tr>
<td>Navigate to the <code>interface-name</code> level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter <code>edit protocols ospf area 0.0.0.0 interface interface-name</code></td>
</tr>
</tbody>
</table>
Table 144: Enabling OSPF Authentication (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the authentication password (key) and, for MD5 authentication</td>
<td>1. Set the authentication password and, for MD5 authentication only, set the key identifier.</td>
</tr>
<tr>
<td>only, the key identifier to associate with the MD5 password.</td>
<td>set authentication-key Chey3nne key-id 2</td>
</tr>
<tr>
<td>■ For simple authentication, set a password of from 1 through</td>
<td>2. Repeat Step 1 for each interface in the stub area for which you are enabling authentication.</td>
</tr>
<tr>
<td>8 ASCII characters—for example, Chey3nne.</td>
<td></td>
</tr>
<tr>
<td>■ For MD5 authentication:</td>
<td></td>
</tr>
<tr>
<td>■ Set a password of from 1 through 16 ASCII characters—for example,</td>
<td></td>
</tr>
<tr>
<td>Chey3nne.</td>
<td></td>
</tr>
<tr>
<td>■ Set a key identifier between 0 (the default) and 255—for example,</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding OSPF Authentication on page 515
- OSPF Configuration Overview on page 504
- OSPF Overview on page 503

OSPF Traffic Control

- Understanding OSPF Traffic Control on page 517
- Example: Controlling the Cost of Individual OSPF Network Segments (CLI) on page 518
- Example: Controlling OSPF Route Selection in the Forwarding Table (CLI) on page 519

Understanding OSPF Traffic Control

Once a topology is shared across the network, OSPF uses the topology to route packets between network nodes. Each path between neighbors is assigned a cost based on the throughput, round-trip time, and reliability of the link. (OSPF assigns a default cost metric of 1 to any link faster than 100 Mbps.) The sum of the costs across a particular path between hosts determines the overall cost of the path. Packets are then routed along the shortest path using the shortest path first (SPF) algorithm. If multiple equal-cost paths exist between a source and destination address, OSPF routes packets along each path alternately, in round-robin fashion.

To control the flow of packets across the network, OSPF allows you to manually assign a cost (or metric) to a particular path segment. For example, if all routers in the OSPF network use default metric values, and you increase the metric on one interface to 5, all paths through this interface have a calculated metric higher than the default and are not preferred.

You can also control the flow of packets through the network using route preferences. When several routes have the same SPF calculation, OSPF uses route preferences to select the route that is installed in the forwarding table. To evaluate a route, OSPF
calculates the sum of the individual preferences of every router along the path and selects the route with the lowest total preference.

By default, internal OSPF routes have a preference value of 10, and external OSPF routes have a preference value of 150. Suppose all routers in your OSPF network use the default preference values. By setting the internal preference to 7 and the external preference to 130, you can ensure that the path through a particular device is selected for the forwarding table any time multiple equal-cost paths to a destination exist.

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- OSPF Overview on page 503
- Example: Controlling the Cost of Individual OSPF Network Segments (CLI) on page 518
- Example: Controlling OSPF Route Selection in the Forwarding Table (CLI) on page 519
- Configuring the Metric Value for OSPF Interfaces

**Example: Controlling the Cost of Individual OSPF Network Segments (CLI)**

To manually set the cost of a network segment on the stub area's Fast Ethernet interface by modifying the interface metric:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 145 on page 518.

**Table 145: Controlling the Cost of Individual Network Segments by Modifying the Metric**

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>ge-0/0/0.0</strong> level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter</td>
</tr>
<tr>
<td></td>
<td>edit protocols ospf area 0.0.0.0 interface ge-0/0/0.0</td>
</tr>
<tr>
<td>Set the interface metric.</td>
<td>Set the interface metric:</td>
</tr>
<tr>
<td></td>
<td>set metric 5</td>
</tr>
</tbody>
</table>

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding OSPF Traffic Control on page 517
- OSPF Configuration Overview on page 504
- Example: Controlling OSPF Route Selection in the Forwarding Table (CLI) on page 519
- OSPF Overview on page 503
Example: Controlling OSPF Route Selection in the Forwarding Table (CLI)

To modify the default OSPF route preferences on a device:
1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 146 on page 519.

Table 146: Controlling Route Selection in the Forwarding Table by Setting Preferences

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Osfp</strong> level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter</td>
</tr>
<tr>
<td></td>
<td><code>edit protocols ospf</code></td>
</tr>
<tr>
<td>Set the external and internal route preferences.</td>
<td>1. Set the external preference:</td>
</tr>
<tr>
<td></td>
<td><code>set external-preference 130</code></td>
</tr>
<tr>
<td></td>
<td>2. Set the internal preference:</td>
</tr>
<tr>
<td></td>
<td><code>set preference 7</code></td>
</tr>
</tbody>
</table>

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding OSPF Traffic Control on page 517
- Example: Controlling the Cost of Individual OSPF Network Segments (CLI) on page 518
- OSPF Configuration Overview on page 504
- OSPF Overview on page 503

Verifying an OSPF Configuration

To verify an OSPF configuration, perform these tasks:
- Verifying OSPF-Enabled Interfaces on page 519
- Verifying OSPF Neighbors on page 520
- Verifying the Number of OSPF Routes on page 521
- Verifying Reachability of All Hosts in an OSPF Network on page 522

Verifying OSPF-Enabled Interfaces

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Verify that OSPF is running on a particular interface and that the interface is in the desired area.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>From the CLI, enter the <code>show ospf interface</code> command.</td>
</tr>
</tbody>
</table>
Sample Output

<table>
<thead>
<tr>
<th>Intf</th>
<th>State</th>
<th>Area</th>
<th>DR ID</th>
<th>BDR ID</th>
<th>Nbrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>at-5/1/0.0</td>
<td>PtToPt</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>1</td>
</tr>
<tr>
<td>ge-2/3/0.0</td>
<td>DR</td>
<td>0.0.0.0</td>
<td>192.168.4.16</td>
<td>192.168.4.15</td>
<td>1</td>
</tr>
<tr>
<td>lo0.0</td>
<td>DR</td>
<td>0.0.0.0</td>
<td>192.168.4.16</td>
<td>0.0.0.0</td>
<td>0</td>
</tr>
<tr>
<td>so-0/0/0.0</td>
<td>Down</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
</tr>
<tr>
<td>so-6/0/1.0</td>
<td>PtToPt</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>1</td>
</tr>
<tr>
<td>so-6/0/2.0</td>
<td>Down</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0</td>
</tr>
<tr>
<td>so-6/0/3.0</td>
<td>PtToPt</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>1</td>
</tr>
</tbody>
</table>

Meaning

The output shows a list of the device interfaces that are configured for OSPF. Verify the following information:

- Each interface on which OSPF is enabled is listed.
- Under Area, each interface shows the area for which it was configured.
- Under Intf and State, the device loopback (lo0.0) interface and LAN interface that are linked to the OSPF network's designated router (DR) are identified.
- Under DR ID, the IP address of the OSPF network's designated router appears.
- Under State, each interface shows a state of PtToPt to indicate a point-to-point connection. If the state is Waiting, check the output again after several seconds. A state of Down indicates a problem.
- The designated router addresses always show a state of DR.

Verifying OSPF Neighbors

Purpose

OSPF neighbors are interfaces that have an immediate adjacency. On a point-to-point connection between the device and another router running OSPF, verify that each router has a single OSPF neighbor.

Action

From the CLI, enter the show ospf neighbor command.

Sample Output

<table>
<thead>
<tr>
<th>Address</th>
<th>Intf</th>
<th>State</th>
<th>ID</th>
<th>Pri</th>
<th>Dead</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.254.225</td>
<td>fxp3.0</td>
<td>2Way</td>
<td>10.250.240.32</td>
<td>128</td>
<td>36</td>
</tr>
<tr>
<td>192.168.254.230</td>
<td>fxp3.0</td>
<td>Full</td>
<td>10.250.240.8</td>
<td>128</td>
<td>38</td>
</tr>
<tr>
<td>192.168.254.229</td>
<td>fxp3.0</td>
<td>Full</td>
<td>10.250.240.35</td>
<td>128</td>
<td>33</td>
</tr>
<tr>
<td>10.1.1.129</td>
<td>fxp2.0</td>
<td>Full</td>
<td>10.250.240.12</td>
<td>128</td>
<td>37</td>
</tr>
<tr>
<td>10.1.1.131</td>
<td>fxp2.0</td>
<td>Full</td>
<td>10.250.240.11</td>
<td>128</td>
<td>38</td>
</tr>
<tr>
<td>10.1.2.1</td>
<td>fxp1.0</td>
<td>Full</td>
<td>10.250.240.9</td>
<td>128</td>
<td>32</td>
</tr>
<tr>
<td>10.1.2.81</td>
<td>fxp0.0</td>
<td>Full</td>
<td>10.250.240.10</td>
<td>128</td>
<td>33</td>
</tr>
</tbody>
</table>

Meaning

The output shows a list of the device's OSPF neighbors and their addresses, interfaces, states, router IDs, priorities, and number of seconds allowed for inactivity ("dead" time). Verify the following information:

- Each interface that is immediately adjacent to the device is listed.
- The device's own loopback address and the loopback addresses of any routers with which the device has an immediate adjacency are listed.
Under State, each neighbor shows a state of Full. Because full OSPF connectivity is established over a series of packet exchanges between clients, the OSPF link might take several seconds to establish. During that time, the state might be displayed as Attempt, Init, or 2way, depending on the stage of negotiation. If, after 30 seconds, the state is not Full, the OSPF configuration between the neighbors is not functioning correctly.

**Verifying the Number of OSPF Routes**

**Purpose**
Verify that the OSPF routing table has entries for the following:
- Each subnetwork reachable through an OSPF link
- Each loopback address reachable on the network

For example, Figure 70 on page 521 shows a sample network with an OSPF topology.

**Figure 70: Sample OSPF Network Topology**

In this topology, OSPF is being run on all interfaces. Each segment in the network is identified by an address with a /24 prefix, with interfaces on either end of the segment being identified by unique IP addresses.

**Action**
From the CLI, enter the `show ospf route` command.

**Sample Output**

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Path Type</th>
<th>Route Type</th>
<th>NH Type</th>
<th>Metric</th>
<th>NextHop Interface</th>
<th>NextHop addr/label</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.12/24</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>1</td>
<td>ge-0/0/1.0</td>
<td>10.0.19.1</td>
</tr>
<tr>
<td>10.10.11/24</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>1</td>
<td>ge-0/0/1.0</td>
<td>10.0.13.1</td>
</tr>
<tr>
<td>10.10.12/24</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>1</td>
<td>ge-0/0/1.0</td>
<td>10.0.19.1</td>
</tr>
<tr>
<td>10.10.11/24</td>
<td>Intra</td>
<td>Network</td>
<td>IP</td>
<td>1</td>
<td>ge-0/0/1.0</td>
<td>10.0.13.1</td>
</tr>
</tbody>
</table>
The output lists each route, sorted by IP address. Routes are shown with a route type of Network, and loopback addresses are shown with a route type of Router.

For the example shown in Figure 70 on page 521, verify that the OSPF routing table has 21 entries, one for each network segment and one for each router's loopback address.

Verifying Reachability of All Hosts in an OSPF Network

**Purpose**  By using the traceroute tool on each loopback address in the network, verify that all hosts in the network are reachable from each device.

**Action**  For each device in the OSPF network:

1. In the J-Web interface, select Troubleshoot > Traceroute.

2. In the Host Name box, type the name of a host for which you want to verify reachability from the device.

3. Click Start. Output appears on a separate page.

**Sample Output**

```
1 172.17.40.254 (172.17.40.254) 0.362 ms 0.284 ms 0.251 ms
2 routera-fxp0.englab.mycompany.net (192.168.71.246) 0.251 ms 0.235 ms 0.200 ms
```

**Meaning**  Each numbered row in the output indicates a routing “hop” in the path to the host. The three-time increments indicate the round-trip time (RTT) between the device and the hop, for each traceroute packet. To ensure that the OSPF network is healthy, verify the following information:

- The final hop in the list is the host you want to reach.
- The number of expected hops to the host matches the number of hops in the traceroute output. The appearance of more hops than expected in the output indicates that a network segment is likely not reachable. In this case, verify the routes with the show ospf route command.

For information about show ospf route, see “Verifying the Number of OSPF Routes” on page 521.
Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- OSPF Configuration Overview on page 504
- traceroute in the Junos System Basics and Services Command Reference
Chapter 20
IS-IS

- IS-IS Overview on page 525
- IS-IS Configuration Overview on page 529
- Example: Configuring IS-IS (CLI) on page 529
- IS-IS Designated Routers on page 530
- Verifying the IS-IS Configuration on page 531

**IS-IS Overview**

The Intermediate System-to-Intermediate System (IS-IS) protocol is a classless interior routing protocol developed by the International Organization for Standardization (ISO) as part of the development of the Open Systems Interconnection (OSI) protocol suite. Like OSPF routing, IS-IS uses hello packets that allow network convergence to occur quickly when network changes are detected. IS-IS uses the shortest path first (SPF) algorithm to determine routes. Using SPF, IS-IS evaluates network topology changes and determines if a full or partial route calculation is required.

This topic contains the following sections:

- IS-IS Areas on page 525
- System Identifier Mapping on page 526
- ISO Network Addresses on page 526
- IS-IS Path Selection on page 527
- Protocol Data Units on page 527

**IS-IS Areas**

An IS-IS network is a single autonomous system (AS), also called a *routing domain*, that consists of end systems and intermediate systems. End systems are network entities that send and receive packets. Intermediate systems (routers) send, receive, and relay (forward) packets.

IS-IS does not force the network to use a hierarchical physical topology. Instead, a single AS can be divided into two types of areas: Level 1 areas and Level 2 areas. A Level 1 area is similar to an OSPF stub area, and a Level 2 area interconnects all Level 1 areas. The router and its interfaces reside within one area, and Level 2 routers share link-state information. No IS-IS area functions strictly as a backbone.
Level 1 routers share intra-area routing information, and Level 2 routers share interarea information about IP addresses available within each area. Uniquely, IS-IS routers can act as both Level 1 and Level 2 routers, sharing intra-area routes with other Level 1 routers and interarea routes with other Level 2 routers.

The propagation of link-state updates is determined by the level boundaries. All routers within a level maintain a complete link-state database of all other routers in the same level. Each router then uses the Dijkstra algorithm to determine the shortest path from the local router to other routers in the link-state database.

**System Identifier Mapping**

To provide assistance with debugging IS-IS, JUNOS Software supports dynamic mapping of ISO system identifiers to the hostname. Each router can be configured with a hostname that allows the system identifier-to-hostname mapping to be sent in a dynamic hostname type length value (TLV) in the IS-IS link-state PDU (LSP). The mapping permits an intermediate system in the routing domain to learn the ISO system identifier of another intermediate system.

**ISO Network Addresses**

IS-IS uses ISO network addresses. Each address identifies a point of connection to the network, such as a router interface, which is called *network service access point* (NSAP). NSAP addresses are supported on the loopback (lo0) interface.

An end system can have multiple NSAP addresses, which differ by the last byte called an *n-selector*. Each NSAP represents a service that is available at the node. In addition to multiple services, a single node can belong to multiple areas.

Each network entity also has a special address called a *network entity title* (NET) with an identical structure to an NSAP address but an *n-selector* of 00. Most end systems and intermediate systems have one NET address, while intermediate systems participating in more than one area can have more than one NET address.

The following ISO addresses are examples of the IS-IS address format:

```
49.0001.00a0.c96b.c490.00
49.0001.2081.9716.9018.00
```

NETs take several forms, depending on your network requirements. NET addresses are hexadecimal and range from 8 octets to 20 octets in length. Generally, the format consists of an authority and format Identifier (AFI), a domain ID, an area ID, a system identifier, and a selector. The simplest format omits the domain ID and is 10 octets long. For example, the NET address `49.0001.1921.6800.1001.00` consists of the following parts:

- 49—AFI
- 0001—Area ID
- 1921.6800.1001—System identifier
- 00—Selector
The system identifier must be unique within the network. For an IP-only network, we recommend using the IP address of an interface on the router. Configuring a loopback NET address with the IP address is helpful when troubleshooting is required on the network.

The first part of the address is the area number, which is a variable number from 1 to 13 bytes. The first byte of the area number, 49, is the authority and format indicator (AFI). The next bytes are the assigned area identifier and can be from 0 to 12 bytes. In the examples, 0001 is the area identifier.

The next 6 bytes are the system identifier and can be any 6 bytes unique throughout the entire domain. The system identifier is commonly the media access control (MAC) address, as shown in the first example, 00a0.c96b.c490. Otherwise, the system identifier is the IP address expressed in binary-coded decimal (BCD) format, as shown in the second example, 2081.9716.9018, which corresponds to 208.197.169.18. The last byte, 00, is the n-selector.

**NOTE:** The system identifier cannot be configured as 0000.0000.0000. Using all zeros as an identifier is not supported and does not form an adjacency.

### IS-IS Path Selection

Level 1 routers store information about all the subnets within an area, and choose intranetwork paths over internetwork paths. Using the area ID portion of the NET address, Level 1 routers determine which neighboring routers are Level 1 routers within the same area.

If the destination address is not within the area, Level 1 routers forward the packet to the nearest router configured as both a Level 1 and Level 2 router within the area. The Level 1 and Level 2 router forwards the packet, using the Level 2 topology, to the proper area. The destination router, which is configured as a Level 1 and Level 2 router, then determines the best path through the destination area.

### Protocol Data Units

IS-IS routers use protocol data units (PDUs) to exchange information. Each protocol data unit (PDU) shares a common header.

#### IS-IS Hello PDU

IS-IS hello PDUs establish adjacencies with other routers and have three different formats: one for point-to-point hello packets, one for Level 1 broadcast links, and one for Level 2 broadcast links. Level 1 routers must share the same area address to form an adjacency, while Level 2 routers do not have this limitation. The request for adjacency is encoded in the Circuit type field of the PDU.

Hello PDUs have a preset length assigned to them. The IS-IS router does not resize any PDU to match the maximum transmission unit (MTU) on a router interface. Each interface supports the maximum IS-IS PDU of 1492 bytes, and hello PDUs are padded.
to meet the maximum value. When the hello is sent to a neighboring router, the connecting interface supports the maximum PDU size.

**Link-State PDU**

A link-state PDU (LSP) contains information about each router in the network and the connected interfaces. Also included is metric and IS-IS neighbor information. Each LSP must be refreshed periodically on the network and is acknowledged by information within a sequence number packet.

On point-to-point links, each LSP is acknowledged by a partial sequence number PDU (PSNP), but on broadcast links, a complete sequence number PDU (CSNP) is sent out over the network. Any router that finds newer LSP information in the CSNP then purges the out-of-date entry and updates the link-state database.

LSPs support variable-length subnet mask addressing.

**Complete Sequence Number PDU**

The complete sequence number PDU (CSNP) lists all the link-state PDUs (LSPs) in the link-state database of the local router. Contained within the CSNP is an LSP identifier, a lifetime, a sequence number, and a checksum for each entry in the database. Periodically, a CSNP is sent on both broadcast and point-to-point links to maintain a correct database. Also, the advertisement of CSNPs occurs when an adjacency is formed with another router. Like IS-IS hello PDUs, CSNPs come in two types: Level 1 and Level 2.

When a device receives a CSNP, it checks the database entries against its own local link-state database. If it detects missing information, the device requests specific LSP details using a partial sequence number PDU (PSNP).

**Partial Sequence Number PDU**

A partial sequence number PDU (PSNP) is used by an IS-IS router to request LSP information from a neighboring router. A PSNP can also explicitly acknowledge the receipt of an LSP on a point-to-point link. On a broadcast link, a CSNP is used as implicit knowledge. Like hello PDUs and CSNPs, the PSNP also has two types: Level 1 and Level 2.

When a device compares a CSNP to its local database and determines that an LSP is missing, the router issues a PSNP for the missing LSP, which is returned in a link-state PDU from the router sending the CSNP. The received LSP is then stored in the local database, and an acknowledgement is sent back to the originating router.

**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Routing Overview on page 467
- Understanding IS-IS Designated Routers on page 530
- IS-IS Configuration Overview on page 529
- OSPF Overview on page 503
IS-IS Configuration Overview

To configure IS-IS:

1. Enable IS-IS if your router is in secure context.

   [edit]
   user@host# set security forwarding-options family iso mode packet-based

   JUNOS Software security processing is not applied to IS-IS packets forwarded by
   the router. By default in secure context, the router drops IS-IS packets.

2. Obtain ISO addresses for participating routers in the autonomous system (AS).

   Configuration Guide.


5. (Optional) Configure designated routers. “Configuring IS-IS Designated Routers
   (CLI Procedure)” on page 531.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- IS-IS Overview on page 525
- Verifying the IS-IS Configuration on page 531
- Configuring IS-IS in the Junos Routing Protocols Configuration Guide
- Minimum IS-IS Configuration in the Junos Routing Protocols Configuration Guide

Example: Configuring IS-IS (CLI)

To configure IS-IS, you must enable IS-IS on the device and configure a NET address
on one of the device interfaces (preferably, the lo0 interface). Additionally, you must
configure the ISO family on all interfaces that are supporting the IS-IS protocol.

In this example, you configure the 49.0001.00a0.c96b.c490.00 NET address on the
lo0 interface. Additionally, you configure the ISO family on the ge-0/0/1 physical
interface.

To configure IS-IS:

1. Navigate to the interfaces level in the configuration hierarchy.

   [edit]
   user@host# edit interfaces

2. Configure the loopback interface lo0.

   [edit interfaces]
   user@host# edit lo0

3. Configure the logical unit on the loopback interface (for example, 0).
4. Add the NET address (for example, 49.0001.00a0.c96b.c490.00) to the loopback interface.

   [edit interfaces lo0 unit 0]
   user@host# set family iso address 49.0001.00a0.c96b.c490.00

5. Configure a physical interface (for example, ge-0/0/1) with the NET address, and add the family type iso.

   [edit interfaces ge-0/0/0 unit 0]
   user@host# set family iso address 49.0001.00a0.c96b.c490.00

6. Navigate to the protocols level in the configuration hierarchy.

   [edit interfaces ge-0/0/0 unit 0]
   user@host# top
   [edit]
   user@host# edit protocols

7. Add the IS-IS protocol to all interfaces on the device.

   [edit protocols]
   user@host# set isis interface all

8. Verify the configuration. See “Verifying the IS-IS Configuration” on page 531.

9. Commit the configuration if you are done configuring the device.

**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- IS-IS Overview on page 525
- IS-IS Configuration Overview on page 529

**IS-IS Designated Routers**

- Understanding IS-IS Designated Routers on page 530
- Configuring IS-IS Designated Routers (CLI Procedure) on page 531

**Understanding IS-IS Designated Routers**

A router advertises its priority to become a designated router in its hello packets. On all multiaccess networks, IS-IS uses the advertised priorities to elect a designated router for the network. This router is responsible for sending network link-state advertisements, which describe all the routers attached to the network. These
advertisements are flooded throughout a single area. The priority value is meaningful only on a multiaccess network. It has no meaning on a point-to-point interface. A router’s priority for becoming the designated router is indicated by an arbitrary number from 0 through 127. The router with the highest priority is elected as the designated router. If routers in the network have the same priority, then the router with the highest MAC address is elected as the designated router. By default, routers have a priority value of 64.

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- IS-IS Overview on page 525
- Configuring IS-IS Designated Routers (CLI Procedure) on page 531

**Configuring IS-IS Designated Routers (CLI Procedure)**

To modify the interface’s priority value, include the following priority statement:

```plaintext
priority number;
```

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding IS-IS Designated Routers on page 530
- IS-IS Configuration Overview on page 529
- Verifying the IS-IS Configuration on page 531

**Verifying the IS-IS Configuration**

To verify IS-IS, perform these tasks:
- Verifying IS-IS Interface Configuration on page 531
- Verifying IS-IS Interface Configuration Detail on page 532
- Verifying IS-IS Adjacencies on page 533
- Verifying IS-IS Adjacencies in Detail on page 533

**Verifying IS-IS Interface Configuration**

**Purpose**
Verify the status of IS-IS-enabled interfaces.

**Action**
From the CLI, enter the `show isis interface brief` command.

**Sample Output**

```plaintext
user@host> show isis interface brief
IS-IS interface database:
Interface  L CirID Level 1 DR Level 2 DR
lo0.0      3  0x1  router1  router.01
ge-0/0/1.0 2  0x9  Disabled  router.03
ge-1/0/0.0 2  0x7  Disabled  router.05
```
Meaning Verify that the output shows the intended configuration of the interfaces on which IS-IS is enabled.

Verifying IS-IS Interface Configuration Detail

Purpose Verify the details of IS-IS-enabled interfaces.

Action From the CLI, enter the `show isis interface detail` command.

Sample Output

```
user@host> show isis interface detail
lo0.0
  Index:3, State:0x7, Circuit id: 0x1, Circuit type:3
  LSP interval: 100 ms, Sysid: router1
  Level Adjacencies Priority Metric Hello(s) Hold(s)
  1    0   64   0     9    27
  2    0   64   0     9    27
ge-0/0/1.0
  Index:3, State:0x106, Circuit id: 0x9, Circuit type:2
  LSP interval: 100 ms, Sysid: router1
  Level Adjacencies Priority Metric Hello(s) Hold(s)
  1    0   64   0     9    27
  2    0   64   0     9    27
```

Meaning Check the following output fields and verify that the output shows the intended configuration of IS-IS-enabled interfaces:

- **Interface**—Interface configured for IS-IS
- **State**—Internal implementation information
- **Circuit id**—Circuit identifier
- **Circuit type**—Configured level of IS-IS:
  - 1—Level 1 only
  - 2—Level 2 only
  - 3—Level 1 and Level 2
- **LSP interval**—Time between IS-IS information messages
- **Sysid**—System identifier
- **L or Level**—Type of adjacency:
  - 1—Level 1 only
  - 2—Level 2 only
  - 3—Level 1 and Level 2
- **Adjacencies**—Adjacencies established on the interface
- **Priority**—Priority value established on the interface
- **Metric**—Metric value for the interface
■ **Hello(s)**—Intervals between hello PDUs
■ **Hold(s)**—Hold time on the interface

**Verifying IS-IS Adjacencies**

**Purpose**
Display brief information about IS-IS neighbors.

**Action**
From the CLI, enter the `show isis adjacency brief` command.

**Sample Output**
```
user@host> show isis adjacency brief
IS-IS adjacency database:
  Interface  System    L  State    Hold (secs) SNPA
  ge-0/0/0.0  192.168.00.5067  2  Up        13
  ge-0/0/1.0  192.168.00.5067  2 Up        25
  ge-0/0/2.0  192.168.00.5067  2 Up        19
```

**Meaning**
Verify adjacent routers in the IS-IS database.

**Verifying IS-IS Adjacencies in Detail**

**Purpose**
Display extensive information about IS-IS neighbors.

**Action**
From the CLI, enter the `show isis adjacency extensive` command.

**Sample Output**
```
R1
  Interface: so-0/0/0.0, Level: 2, State: Up, Expires in 25 secs
  Priority: 0, Up/Down transitions: 1, Last transition: 4w6d 19:38:52 ago
  Circuit type: 2, Speaks: IP, IPv6
  Topologies: Unicast
  Restart capable: Yes
  IP addresses: 10.1.12.1
  Transition log:
  When                  State        Reason
  Wed Jul 13 16:26:11   Up           Seenself

R3
  Interface: so-0/0/1.0, Level: 2, State: Up, Expires in 23 secs
  Priority: 0, Up/Down transitions: 1, Last transition: 6w5d 19:07:16 ago
  Circuit type: 2, Speaks: IP, IPv6
  Topologies: Unicast
  Restart capable: Yes
  IP addresses: 10.1.23.2
  Transition log:
  When                  State        Reason
  Thu Jun 30 16:57:46   Up           Seenself

R6
  Interface: so-0/0/2.0, Level: 2, State: Up, Expires in 25 secs
  Priority: 0, Up/Down transitions: 1, Last transition: 6w0d 18:01:18 ago
  Circuit type: 2, Speaks: IP, IPv6
  Topologies: Unicast
  Restart capable: Yes
```
Meaning
Check the following fields and verify adjacency information about IS-IS neighbors:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Interface through which the neighbor is reachable</th>
</tr>
</thead>
<tbody>
<tr>
<td>L or Level</td>
<td>Configured level of IS-IS:</td>
</tr>
<tr>
<td>1</td>
<td>Level 1 only</td>
</tr>
<tr>
<td>2</td>
<td>Level 2 only</td>
</tr>
<tr>
<td>3</td>
<td>Level 1 and Level 2</td>
</tr>
</tbody>
</table>

An exclamation point before the level number indicates that the adjacency is missing an IP address.

<table>
<thead>
<tr>
<th>State</th>
<th>Status of the adjacency: Up, Down, New, One-way, Initializing, or Rejected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event</td>
<td>Message that identifies the cause of a state</td>
</tr>
<tr>
<td>Down reason</td>
<td>Reason the adjacency is down</td>
</tr>
<tr>
<td>Restart capable</td>
<td>Denotes a neighbor configured for graceful restart</td>
</tr>
<tr>
<td>Transition log</td>
<td>List of transitions including When, State, and Reason</td>
</tr>
</tbody>
</table>

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- IS-IS Configuration Overview on page 529
- show isis interface in the Junos Routing Protocols and Policies Command Reference
- show isis adjacency in the Junos Routing Protocols and Policies Command Reference
BGP Overview

Connections between peering networks are typically made through an exterior gateway protocol (EGP), most commonly BGP. BGP is an EGP used primarily to establish point-to-point connections and transmit data between peer autonomous systems (ASs). Unlike RIP and OSPF links, BGP peering sessions must be explicitly configured at both ends. BGP must explicitly advertise the routes between its peers. The route advertisements determine prefix reachability and the way packets are routed between BGP neighbors. Because BGP uses the packet path to determine route selection, it is considered a path-vector protocol.

This overview contains the following topics:

- BGP Messages for Session Establishment on page 535
- BGP Messages for Session Maintenance on page 536
- IBGP and EBGP on page 536
- Route Selection on page 537
- Local Preference on page 538
- AS Path on page 539
- Origin on page 539
- Multiple Exit Discriminator on page 540
- Scaling BGP for Large Networks on page 542

BGP Messages for Session Establishment

When the routers on either end of a BGP session first boot, the session between them is in the Idle state. The BGP session remains idle until a start event is detected. Typically, the start event is the configuration of a new BGP session or the resetting...
of an existing BGP session. At boot time, the start event is generated by the router as the BGP session is initiated.

After it detects a start event, the BGP host sends TCP request packets to its configured BGP neighbors. These packets are directed only to neighboring interfaces that have been explicitly configured as BGP neighbors. Upon receipt of the TCP request packet, the neighboring host generates a TCP response to complete the three-way handshake and establish a TCP connection between the peers. While this handshake is taking place, the BGP state for the connection is Connect. If a TCP timeout occurs while the originating host is waiting for a TCP response packet, the BGP state for the connection is Active. The Active state indicates that the router is actively listening for a TCP response and the TCP retry timer has been initiated.

Once a TCP connection has been established between both ends of a BGP session, the BGP session state is OpenSent, indicating that the originating router has generated an open message. The open message is an initial BGP handshake that must occur before any route advertisement can take place. Upon receipt of the open message, the neighboring router generates a keepalive message. Receipt of the keepalive message establishes a point-to-point connection, and the BGP session state transitions to Established. While the originating host waits for the keepalive response packet, the BGP session state is OpenConfirm.

**BGP Messages for Session Maintenance**

Once a BGP session has been established, the BGP peers exchange route advertisements by means of update messages. Update messages contain one or more route advertisements, and they can contain one or more prefixes that are to be removed from the BGP routing table. If the peers need to advertise multiple routes, they generate and send multiple update messages as they detect changes to the network. In the absence of changes to the routing table, no update messages are generated.

While a BGP session is active, each router on the BGP session generates keepalive messages periodically. The timing of these messages is determined by the hold time on the session. The hold time is a negotiated value specifying the number of seconds that can elapse without keepalive messages before BGP designates the link inactive. Three messages are sent during every hold time interval.

When a peer connection is closed (either by error or if the BGP session is closed), a notification message is generated and sent to the peer router that did not experience the error or did not terminate the BGP session.

**IBGP and EBGP**

Peer ASs establish links through an external peer BGP session. As a result, all route advertisement between the external peers takes place by means of the EBGP mode of information exchange. To propagate the routes through the AS and advertise them to internal peers, BGP uses IBGP. To advertise the routes to a different peer AS, BGP again uses EBGP.

BGP uses two primary modes of information exchange, internal BGP (IBGP) and external BGP (EBGP), to communicate with internal and external peers, respectively.
To avoid routing loops, IBGP does not advertise routes learned from an internal BGP peer to other internal BGP peers. For this reason, BGP cannot propagate routes throughout an AS by passing them from one router to another. To achieve an IBGP full mesh, you configure a direct peering session every host to every other host within the network. These sessions are configured on every router within the network, as type internal.

As a network grows, the full mesh requirement becomes increasingly difficult to manage. In a network with 1000 routers, the addition of a single router requires that all the routers in the network be modified to account for the new addition. To combat these scaling problems, BGP uses route reflection and BGP confederations.

### Route Selection

The BGP route selection process compares BGP attributes to select a single best path or active route for each prefix in the routing table. The attributes are compared in a particular order. A local BGP router uses the following criteria, in the order presented, to select a route from the routing table for the forwarding table.

1. **Next-hop accessibility**—If the next hop is inaccessible, the local router does not consider the route. The router must verify that it has a route to the BGP next-hop address. If a local route to the next hop does not exist, the local route does not include the router in its forwarding table. If such a route exists, route selection continues.

2. **Highest local preference**—The local router selects the route with the highest local preference value. If multiple routes have the same preference, route selection continues. (See “Local Preference” on page 538.)

3. **Shortest AS path**—The local router selects the route with the fewest entries in the AS path. If multiple routes have the same AS path length, route selection continues.

4. **Lowest origin**—The local router selects the route with the lowest origin value. If multiple routes have the same origin value, route selection continues. (See “Origin” on page 539.)

5. **Lowest MED value**—The local router selects the route with the lowest multiple exit discriminator (MED) value, comparing the routes from the same AS only. If multiple routes have the same MED value, route selection continues. See “Multiple Exit Discriminator” on page 540.

6. **Strictly external paths**—The local router prefers strictly external (EBGP) paths over external paths learned through interior sessions (IBGP). If multiple routes have the same strictly external paths, route selection continues.

7. **Lowest IGP route metric**—The local router selects the path for which the next hop is resolved through the IGP route with the lowest metric. If multiple routes have the same IGP route metric, route selection continues.

8. **Maximum IGP next hops**—The local router selects the path for which the BGP next hop is resolved through the IGP route with the largest number of next hops. If multiple routes have the same number of next hops, route selection continues.

9. **Shortest route reflection cluster list**—The local router selects the path with the shortest route reflection cluster list. Routes without a cluster list are considered
to have a cluster list of length 0. If multiple routes have the same route reflection cluster list, route selection continues.

10. Lowest router ID—The local router selects the route with the lowest IP address value for the BGP router ID. By default, the router IDs of routes received from different ASs are not compared. You can change this default behavior.

11. Lowest peer IP address—The local router selects the path that was learned from the neighbor with the lowest peer IP address.

For configuration instructions, see Configuring Routing Table Path Selection for BGP in the Junos Routing Protocols Configuration Guide.

**Local Preference**

The local preference is typically used to direct all outbound AS traffic to a certain peer. When you configure a local preference, all routes that are advertised through that peer are assigned the preference value. The preference is a numeric value, and higher values are preferred during BGP route selection. Figure 71 on page 538 illustrates how to use local preference to determine BGP route selection.

![Figure 71: Local Preference](image)

The network in Figure 71 on page 538 shows two possible routes to the prefixes accessible through Host E. The first route, through Router A, uses an OC3 link to Router C and is then forwarded to Host E. The second route, through Router B, uses an OC48 link to Router D and is then forwarded to Host E. Although the number of hops to Host E is identical regardless of the route selected, the route through Router B is more desirable because of the increased bandwidth. To force traffic through Router B, you can set the local preference on Router A to 100 and the local preference
on Router B to 300. During BGP route selection, the route with the higher local preference is selected.

**NOTE:** In contrast to almost every other metric associated with dynamic routing protocols, the local preference gives higher precedence to the larger value.

For configuration instructions, see Configuring the Local Preference Value for BGP Routes in the *Junos Routing Protocols Configuration Guide*.

**AS Path**

Routes advertised by BGP maintain a list of the ASs through which the route travels. This information is stored in the route advertisement as the AS path, and it is one of the primary criteria that a local router uses to evaluate BGP routes for inclusion in its forwarding table. Figure 72 on page 539 shows how BGP creates an AS path.

**Figure 72: BGP AS Path**

In the network shown in Figure 72 on page 539, the route from Host A to Host B travels through two intermediate ASs. As the route advertisement is propagated through the BGP network, it accumulates an AS path number each time it exits one AS and enters another. Each AS number is prepended to the AS path, which is stored as part of the route advertisement. When the route advertisement first leaves Host B’s AS, the AS path is 17. When the route is advertised between intermediate ASs, the AS number 7 is prepended to the AS path, which becomes 7 17. When the route advertisement exits the third AS, the AS path becomes 4 7 17. The route with the shortest AS path is preferred for inclusion into the BGP forwarding table.

**Origin**

The BGP router that first advertises a route assigns it one of the following values to identify its origin. During route selection, the lowest origin value is preferred.

- 0—The router originally learned the route through an IGP (OSPF, IS-IS, or a static route).
- 1—The router originally learned the route through an EGP (most likely BGP).
- 2—The route’s origin is unknown.
Multiple Exit Discriminator

A multiple exit discriminator (MED) is an arbitrary metric assigned to a route to determine the exit point to a destination when all other factors are equal. By default, MED metrics are compared only for routes to the same peer AS, but you can also configure routing table path selection options for different ways of comparing MEDs.

Default MED Usage

Because the AS path rather than the number of hops between hosts is the primary criterion for BGP route selection, an AS with multiple connections to a peer AS can have multiple equivalent AS paths. When the routing table contains two routes to the same host in a neighboring AS, an MED metric assigned to each route can determine which to include in the forwarding table. The MED metric you assign can force traffic through a particular exit point in an AS.

Figure 73 on page 540 illustrates how MED metrics are used to determine route selection.

Figure 73: Default MED Example

Figure 73 on page 540 shows AS 1 and AS 2 connected by two separate BGP links to Routers C and D. Host E in AS 1 is located nearer to Router C. Host F, also in AS 1, is located nearer to Router D. Because the AS paths are equivalent, two routes exist for each host, one through Router C and one through Router D. To force all traffic destined for Host E through Router C, the network administrator for AS 2 assigns an MED metric for each router to Host E at its exit point. An MED metric of 10 is assigned to the route to Host E through Router C, and an MED metric of 20 is assigned to the route to Host E through Router D. BGP routers in AS 2 then select the route with the lower MED metric for the forwarding table.
Additional MED Options for Path Selection

By default, only the MEDs of routes that have the same peer ASs are compared. However, you can configure the routing table path selection options listed in Table 147 on page 541 to compare MEDs in different ways. The MED options are not mutually exclusive and can be configured in combination or independently. For the MED options to take effect, you must configure them uniformly all through your network. The MED option or options you configure determine the route selected. Thus we recommend that you carefully evaluate your network for preferred routes before configuring the MED options. See Configuring Routing Table Path Selection for BGP in the Junos Routing Protocols Configuration Guide.

Table 147: MED Options for Routing Table Path Selection

<table>
<thead>
<tr>
<th>Option (Name)</th>
<th>Function</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always comparing MEDs (always-compare-med)</td>
<td>Ensures that the MEDs for paths from peers in different ASs are always compared in the route selection process.</td>
<td>Useful when all enterprises participating in a network agree on a uniform policy for setting MEDs. For example, in a network shared by two ISPs, both must agree that a certain path is the better path to configure the MED values correctly.</td>
</tr>
<tr>
<td>Adding IGP cost to MED (med-plus-igp)</td>
<td>Before comparing MED values for path selection, adds to the MED the cost of the IGP route to the BGP next-hop destination.</td>
<td>Useful when the downstream AS requires the complete cost of a certain route that is received across multiple ASs.</td>
</tr>
</tbody>
</table>
| Applying Cisco IOS nondeterministic behavior (cisco-non-deterministic) | Specifies the nondeterministic behavior of the Cisco IOS software:  
  ■ The active path is always first. All nonactive but eligible paths follow the active path and are maintained in the order in which they were received. Ineligible paths remain at the end of the list.  
  ■ When a new path is added to the routing table, path comparisons are made among all routes, including those paths that must never be selected because they lose the MED tie-breaking rule. | We recommend that you do not configure this option, because the nondeterministic behavior sometimes prevents the system from properly comparing the MEDs between paths. |
Scaling BGP for Large Networks

BGP is not a flooding protocol like RIP or OSPF. Instead, it is a peering protocol that exchanges routes with fully meshed peers only. However, in large networks, the full mesh requirement causes scaling problems. BGP combats scaling problems using route reflectors and confederations.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Routing Overview on page 467
- BGP Configuration Overview on page 542
- Understanding BGP Peering Sessions on page 543
- Understanding BGP Route Reflectors on page 547
- Understanding BGP Confederations on page 551
- BGP Overview in the Junos Routing Protocols Configuration Guide

BGP Configuration Overview

To configure the device as a node in a BGP network:

3. Configure point-to-point peering sessions. See “Example: Configuring BGP Point-to-Point Peering Sessions (CLI)” on page 544.
4. Configure IBGP sessions between peers. See “Example: Configuring Internal BGP Peering Sessions (CLI)” on page 545.
5. Configure a routing policy to advertise the BGP routes.
6. (Optional) Configure route reflector clusters. See “Example: Configuring a Route Reflector (CLI)” on page 549.
7. (Optional) Subdivide autonomous systems (ASs). See “Example: Configuring BGP Confederations (CLI)” on page 552.
8. (Optional) Assign a router ID to each routing device running BGP.
9. (Optional) Configure a local preference to direct all outbound AS traffic to a specific peer. See Configuring the Local Preference Value for BGP Routes in the Junos Routing Protocols Configuration Guide.
10. (Optional) Configure routing table path selection options that define different ways to compare multiple exit discriminators (MEDs). See Configuring Routing Table Path Selection for BGP in the Junos Routing Protocols Configuration Guide.
To establish point-to-point connections between peer autonomous systems (ASs), you configure a BGP session on each interface of a point-to-point link. Generally, such sessions are made at network exit points with neighboring hosts outside the AS. Figure 74 on page 543 shows an example of a BGP peering session.

In Figure 74 on page 543, Router A is a gateway router for AS 3, and Router B is a gateway router for AS 10. For traffic internal to either AS, an IGP (OSPF, for instance) is used. To route traffic between peer ASs, a BGP session is used.

In addition to configuring BGP sessions between peering networks, you must also configure BGP internally to provide a means by which BGP route advertisements can be forwarded throughout the network. Because of the full mesh requirement of IBGP, you must configure individual peering sessions between all internal nodes of the network—unless you use route reflectors or confederations.
Example: Configuring BGP Point-to-Point Peering Sessions (CLI)

Figure 75 on page 544 shows a network with BGP peering sessions. In the sample network, a device in AS 17 has BGP peering sessions to a group of peers called external-peers. Peers A, B, and C reside in AS 22 and have IP addresses 10.10.10.10, 10.10.10.11, and 10.10.10.12. Peer D resides in AS 79, at IP address 10.21.7.2.

Figure 75: Typical Network with BGP Peering Sessions

To configure the BGP peering sessions in the sample network:
1. Navigate to the routing-options level in the configuration hierarchy.
   
   ```
   [edit]
   user@host# edit routing-options
   ```
2. Set the network’s AS number to 17.
   
   ```
   [edit routing-options]
   user@host# set autonomous-system 17
   ```
3. Navigate to the bgp level in the configuration hierarchy.
   
   ```
   [edit routing-options]
   user@host# top
   ```
4. Create the BGP group external-peers, and add the external neighbor address 10.10.10.10 to the group.

```
[edit protocols bgp]
user@host# set group external-peers neighbor 10.10.10.10
```

**NOTE:** Repeat Step 4 for each BGP neighbor (10.10.10.11 and 10.10.10.12) within the external peer group that you are configuring.

5. Set the AS number at the group level for the group external-peers to 22. Because three of the peers in this group (peers A, B, and C) reside in one AS, you can set their AS number as a group.

```
[edit protocols bgp]
user@host# set group external-peers peer-as 22
```

6. Set the AS number at the individual neighbor level for peer D to 79. Because peer D is a member of the group external-peers, it inherits the peer AS number configured at the group level. You must override this value at the individual neighbor level.

```
[edit protocols bgp]
user@host# edit group external-peers
[edit protocols bgp group external-peers]
user@host# set neighbor 10.21.7.2 peer-as 79
```

7. Set the group type to external.

```
[edit protocols bgp group external-peers]
user@host# set type external
```

8. Commit the configuration if you are done configuring the device.

```
[edit protocols bgp group external-peers]
user@host# commit
```

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding BGP Peering Sessions on page 543
- Example: Configuring Internal BGP Peering Sessions (CLI) on page 545
- BGP Configuration Overview on page 542

**Example: Configuring Internal BGP Peering Sessions (CLI)**

Figure 76 on page 546 shows a typical network with external and internal peer sessions. In the sample network, the device in AS 17 is fully meshed with its internal peers in the group `internal-peers`, which have IP addresses starting at 192.168.6.4.
To configure IBGP in the sample network:

1. Navigate to the bgp level in the configuration hierarchy.

   [edit]
   user@host# edit protocols bgp

2. Create the BGP group internal-peers, and add the internal neighbor address 192.168.6.4 to the group. You must configure a full IBGP mesh, which requires that each peer be configured with every other internal peer as a BGP neighbor.

   [edit protocols bgp]
   user@host# edit group internal-peers
   [edit protocols bgp group internal-peers]
   user@host# set neighbor 192.168.6.4

   **NOTE:** Repeat Step 2 for each internal BGP neighbor (192.168.6.5, 192.168.6.6, 192.168.6.7, and 192.168.40.4) within the network.

3. Set the group type to internal.

   [edit protocols bgp group internal-peers]
   user@host# set type internal

4. Commit the configuration if you are done configuring the device.

   [edit protocols bgp group internal-peers]
   user@host# commit

**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding BGP Peering Sessions on page 543
- Example: Configuring BGP Point-to-Point Peering Sessions (CLI) on page 544
- BGP Configuration Overview on page 542
**Understanding BGP Route Reflectors**

Because of the internal BGP (IBGP) full-mesh requirement, most networks use route reflectors to simplify configuration. Using a route reflector, you group routers into clusters, which are identified by numeric identifiers unique to the autonomous system (AS). Within the cluster, you must configure a BGP session from a single router (the route reflector) to each internal peer. With this configuration, the IBGP full-mesh requirement is met.

To use route reflection in an AS, you designate one or more routers as a route reflector—typically, one per point of presence (POP). Route reflectors have the special BGP ability to readvertise routes learned from an internal peer to other internal peers. So rather than requiring all internal peers to be fully meshed with each other, route reflection requires only that the route reflector be fully meshed with all internal peers. The route reflector and all its internal peers form a cluster, as shown in Figure 77 on page 547.

**NOTE:** You must have an Advanced BGP Feature license installed on each device that uses a route reflector. For license details, see the *JUNOS Software Administration Guide*.

**Figure 77: Simple Route Reflector Topology (One Cluster)**

Figure 77 on page 547 shows Router RR configured as the route reflector for Cluster 127. The other routers are designated internal peers within the cluster. BGP routes are advertised to Router RR by any of the internal peers. RR then readvertises those routes to all other peers within the cluster.
You can configure multiple clusters and link them by configuring a full mesh of route reflectors (see Figure 78 on page 548).

**Figure 78: Basic Route Reflection (Multiple Clusters)**

Figure 78 on page 548 shows Route Reflectors RR1, RR2, RR3, and RR4 as fully meshed internal peers. When a router advertises a route to RR1, RR1 readvertises the route to the other route reflectors, which, in turn, readvertise the route to the remaining routers within the AS. Route reflection allows the route to be propagated throughout the AS without the scaling problems created by the full mesh requirement.

However, as clusters become large, a full mesh with a route reflector becomes difficult to scale, as does a full mesh between route reflectors. To help offset this problem, you can group clusters of routers together into clusters of clusters for hierarchical route reflection (see Figure 79 on page 549).
Figure 79 on page 549 shows RR2, RR3, and RR4 as the route reflectors for Clusters 127, 19, and 45, respectively. Rather than fully mesh those route reflectors, the network administrator has configured them as part of another cluster (Cluster 6) for which RR1 is the route reflector. When a router advertises a route to RR2, RR2 readvertises the route to all the routers within its own cluster, and then readvertises the route to RR1. RR1 readvertises the route to the routers in its cluster, and those routers propagate the route down through their clusters.

**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- BGP Overview on page 535
- Example: Configuring a Route Reflector (CLI) on page 549

**Example: Configuring a Route Reflector (CLI)**

Figure 80 on page 550 shows an IBGP network with a Juniper Networks device at IP address 192.168.40.4 acting as a route reflector. In the sample network, each device in Cluster 2.3.4.5 has an internal client relationship to the route reflector. To configure the cluster:

- Create an internal group on the Juniper Networks device, configure an internal peer (neighbor) relationship to every other device in the cluster, and assign a cluster identifier.
- On the other devices you are assigning to the cluster, create the cluster group and configure a client relationship to the route reflector.
To configure IBGP in the network using the Juniper Networks device as a route reflector:

1. On the device that you are using as a route reflector, navigate to the bgp level in the configuration hierarchy.

   ```
   [edit]
   user@host# edit protocols bgp
   ```

2. On the device that you are using as a route reflector, create the BGP group cluster-peers, and add to the group the IP addresses of the internal neighbors that you want in the cluster.

   ```
   [edit protocols bgp]
   user@host# set group cluster-peers neighbor 192.168.6.4
   ```

   **NOTE:** Repeat Step 2 for each BGP neighbor within the cluster that you are configuring.

3. On the device that you are using as a route reflector, set the group type to internal.

   ```
   [edit protocols bgp]
   user@host# edit group internal-peers
   [edit protocols bgp group internal-peers]
   user@host# set type internal
   ```

4. On the device that you are using as a route reflector, configure the cluster identifier for the route reflector.

   ```
   [edit protocols bgp group internal-peers]
   user@host# set cluster 2.3.4.5
   ```
5. On the other devices in the cluster, create the BGP group cluster-peers, and add the internal IP address of the route reflector. You do not need to include the neighbor addresses of the other internal peers, or configure the cluster identifier on these route reflector clients. They need only be configured as internal neighbors.

**NOTE:** If the other devices in the network are from Juniper Networks, then follow these steps. Otherwise, consult the device’s documentation for instructions.

```plaintext
[edit protocols bgp group internal-peers]
user@host# top
[edit]
user@host# edit protocols bgp
[edit protocols bgp]
user@host# set group cluster-peers neighbor 192.168.40.4
```

6. Commit the configuration if you are done configuring the device.

```plaintext
[edit protocols bgp]
user@host# commit
```

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding BGP Route Reflectors on page 547
- BGP Configuration Overview on page 542
- Configuring BGP Route Reflection in the Junos Routing Protocols Configuration Guide

**BGP Confederations**

- Understanding BGP Confederations on page 551
- Example: Configuring BGP Confederations (CLI) on page 552

**Understanding BGP Confederations**

BGP confederations are another way to solve the scaling problems created by the BGP full mesh requirement. BGP confederations effectively break up a large autonomous system (AS) into subautonomous systems (sub-ASs). Each sub-AS must be uniquely identified within the confederation AS by a sub-AS number. Typically, sub-AS numbers are taken from the private AS numbers between 64,512 and 65,535.

Within a sub-AS, the same internal BGP (IBGP) full mesh requirement exists. Connections to other confederations are made with standard external BGP (EBGP), and peers outside the sub-AS are treated as external. To avoid routing loops, a sub-AS uses a confederation sequence, which operates like an AS path but uses only the privately assigned sub-AS numbers.
The confederation AS appears whole to other confederation ASs. The AS path received by other ASs shows only the globally assigned AS number. It does not include the confederation sequence or the privately assigned sub-AS numbers. The sub-AS numbers are removed when the route is advertised out of the confederation AS. Figure 81 on page 552 shows an AS divided into four confederations.

**Figure 81: BGP Confederations**

Figure 81 on page 552 shows AS 3 divided into four sub-ASs, 64517, 64550, 65300, and 65410, which are linked through EBGP sessions. Because the confederations are connected by EBGP, they do not need to be fully meshed. EBGP routes are readvertised to other sub-ASs.

**Related Topics**

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- BGP Overview on page 535
- Example: Configuring BGP Confederations (CLI) on page 552

**Example: Configuring BGP Confederations (CLI)**

Figure 82 on page 553 shows a sample network in which AS 17 has two separate confederations (sub-AS 64512 and sub-AS 64513), each of which has multiple routers. Within a sub-AS, an IGP (OSPF, for example) is used to establish network connectivity with internal peers. Between sub-ASs, an external BGP peering session is established.
To configure the BGP confederations shown in the sample network:

1. Navigate to the routing-options level in the configuration hierarchy.
   
   ```
   [edit]
   user@host# edit routing-options
   ```

2. Set the AS number to the sub-AS number 64512. The sub-AS number is a unique AS number that is usually taken from the pool of private AS numbers from 64512 through 65535.
   
   ```
   [edit routing-options]
   user@host# set autonomous-system 64512
   ```

3. Navigate to the confederation level in the configuration hierarchy.
   
   ```
   [edit routing-options]
   user@host# edit confederation
   ```

4. Set the confederation number to the AS number 17.
   
   ```
   [edit routing-options confederation]
   user@host# set 17
   ```

5. Add the sub-ASs as members of the confederation. Every sub-AS within the AS must be added as a confederation member.
   
   ```
   [edit routing-options confederation]
   user@host# set 17 members 64512
   [edit routing-options confederation]
   user@host# set 17 members 64513
   ```

6. Commit the configuration if you are done configuring the device.
   
   ```
   [edit routing-options confederation]
   user@host# commit
   ```

### Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding BGP Confederations on page 551
Verifying a BGP Configuration

To verify a BGP configuration, perform these tasks.

- Verifying BGP Neighbors on page 554
- Verifying BGP Groups on page 555
- Verifying BGP Summary Information on page 556
- Verifying Reachability of All Peers in a BGP Network on page 556

Verifying BGP Neighbors

**Purpose**
Verify that BGP is running on configured interfaces and that the BGP session is active for each neighbor address.

**Action**
From the CLI, enter the `show bgp neighbor` command.

**Sample Output**
```
user@host> show bgp neighbor
Peer: 10.255.245.12+179 AS 35  Local: 10.255.245.13+2884 AS 35
  Type: Internal    State: Established (route reflector client)Flags: Sync
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  Last Error: None
  Options: Preference LocalAddress HoldTime Cluster AddressFamily Rib-group Refresh
  Address families configured: inet-vpn-unicast inet-labeled-unicast
  Local Address: 10.255.245.13 Holdtime: 90 Preference: 170
  Flags for NLRI inet-vpn-unicast: AggregateLabel
  Flags for NLRI inet-labeled-unicast: AggregateLabel
  Number of flaps: 0
  Peer ID: 10.255.245.12    Local ID: 10.255.245.13    Active Holdtime: 90
  Keepalive Interval: 30
  NLRI advertised by peer: inet-vpn-unicast inet-labeled-unicast
  NLRI for this session: inet-vpn-unicast inet-labeled-unicast
  Peer supports Refresh capability (2)
  Restart time configured on the peer: 300
  Stale routes from peer are kept for: 60
  Restart time requested by this peer: 300
  NLRI that peer supports restart for: inet-unicast inet6-unicast
  NLRI that restart is negotiated for: inet-unicast inet6-unicast
  NLRI of received end-of-rib markers: inet-unicast inet6-unicast
  NLRI of all end-of-rib markers sent: inet-unicast inet6-unicast
  Table inet.0 Bit: 10000
    RIB State: restart is complete
    Send state: in sync
    Active prefixes: 4
    Received prefixes: 6
    Suppressed due to damping: 0
  Table inet6.0 Bit: 20000
    RIB State: restart is complete
    Send state: in sync
```
Verifying BGP Groups

Verifying BGP Groups

Purpose Verify that the BGP groups are configured correctly.

Action From the CLI, enter the show bgp group command.

Sample Output

Meaning The output shows a list of the BGP groups with detailed group information. Verify the following information:

- Each configured group is listed.
- For AS, each group’s remote AS is configured correctly.
- For Local AS, each group’s local AS is configured correctly.
- For Group Type, each group has the correct type (either internal or external).
- For Total peers, the expected number of peers within the group is shown.
For Established, the expected number of peers within the group have BGP sessions in the Established state.

The IP addresses of all the peers within the group are present.

**Verifying BGP Summary Information**

**Purpose**
Verify that the BGP configuration is correct.

**Action**
From the CLI, enter the `show bgp summary` command.

**Sample Output**

```
user@host> show bgp summary
Groups: 1 Peers: 3 Down peers: 0
Table       Tot Paths Act Paths Suppressed History Damp State Pending
inet.0        6          4          0          0          0          0          0

Peer            AS  InPkt     OutPkt    OutQ   Flaps Last Up/Dwn State
10.0.0.2      65002      88675      88652       0       2       42:38 2/4/0 0/0/0
10.0.0.3      65002      54528      54532       0       1      2w4d22h 0/0/0 0/0/0
10.0.0.4      65002      51597      51584       0       0      2w3d22h 2/2/0 0/0/0
```

**Meaning**
The output shows a summary of BGP session information. Verify the following information:

- For **Groups**, the total number of configured groups is shown.
- For **Peers**, the total number of BGP peers is shown.
- For **Down Peers**, the total number of unestablished peers is 0. If this value is not zero, one or more peering sessions are not yet established.
- Under **Peer**, the IP address for each configured peer is shown.
- Under **AS**, the peer AS for each configured peer is correct.
- Under **Up/Dwn State**, the BGP state reflects the number of paths received from the neighbor, the number of these paths that have been accepted, and the number of routes being damped (such as 0/0/0). If the field is **Active**, it indicates a problem in the establishment of the BGP session.

**Verifying Reachability of All Peers in a BGP Network**

**Purpose**
By using the ping tool on each peer address in the network, verify that all peers in the network are reachable from each device.

**Action**
For each device in the BGP network:
1. In the J-Web interface, select **Troubleshoot > Ping Host**.
2. In the Remote Host box, type the name of a host for which you want to verify reachability from the device.
3. Click **Start**. Output appears on a separate page.

**Sample Output**

PING 10.10.10.10 : 56 data bytes
64 bytes from 10.10.10.10: icmp_seq=0 ttl=255 time=0.382 ms
64 bytes from 10.10.10.10: icmp_seq=1 ttl=255 time=0.266 ms

**Meaning** If a host is active, it generates an ICMP response. If this response is received, the round-trip time is listed in the *time* field.

**Related Topics**
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- BGP Configuration Overview on page 542
- BGP Overview on page 535
- show bgp neighbor in the *Junos Routing Protocols and Policies Command Reference*
- show bgp summary in the *Junos Routing Protocols and Policies Command Reference*
- show bgp group in the *Junos Routing Protocols and Policies Command Reference*
- ping in the *Junos System Basics and Services Command Reference*
Chapter 22
Multicast

Multicast Overview

NOTE: Both Protocol Independent Multicast (PIM) version 1 and PIM version 2 are supported. In this topic, the term PIM refers to both versions of the protocol.

Multicast traffic lies between the extremes of unicast (one source, one destination) and broadcast (one source, all destinations). Multicast is a “one source, many destinations” method of traffic distribution, meaning that the destinations needing to receive the information from a particular source receive the traffic stream.

IP network destinations (clients) do not often communicate directly with sources (servers), so the routers between source and destination must be able to determine the topology of the network from the unicast or multicast perspective to avoid routing traffic haphazardly. The multicast router must find multicast sources on the network, send out copies of packets on several interfaces, prevent routing loops, connect interested destinations with the proper source, and keep the flow of unwanted packets to a minimum. Standard multicast routing protocols provide most of these capabilities.

This chapter contains the following topics:

- Multicast Architecture on page 560
- Dense and Sparse Routing Modes on page 561
- Strategies for Preventing Routing Loops on page 562
- Multicast Protocol Building Blocks on page 563
Multicast Architecture

Multicast-capable routers replicate packets on the multicast network, which has exactly the same topology as the unicast network it is based on. Multicast routers use a multicast routing protocol to build a distribution tree that connects receivers (also called listeners) to sources.

Upstream and Downstream Interfaces

A single upstream interface on the router leads toward the source to receive multicast packets. The downstream interfaces on the router lead toward the receivers to transmit packets. A router can have as many downstream interfaces as it has logical interfaces, minus 1. To prevent looping, the router's upstream interface must never receive copies of its own downstream multicast packets.

Subnetwork Leaves and Branches

On a multicast router, each subnetwork of hosts that includes at least one interested receiver is a leaf on the multicast distribution tree (see Figure 83 on page 561). The router must send out a copy of the IP multicast packet on each interface with a leaf. When a new leaf subnetwork joins the tree, a new branch is built so that the router can send out replicated packets on the interface. The number of leaves on an interface does not affect the router. The action is the same for one leaf or a hundred.

A branch that no longer has leaves is pruned from the distribution tree. No multicast packets are sent out on a router interface leading to an IP subnetwork with no interested hosts. Because packets are replicated only where the distribution tree branches, no link ever carries a duplicate flow of packets.

In IP multicast networks, traffic is delivered to multicast groups based on an IP multicast group address instead of a unicast destination address. The groups determine the location of the leaves, and the leaves determine the branches on the multicast network.
Multicast IP Address Ranges

Multicast uses the Class D IP address range (224.0.0.0 through 239.255.255.255). Multicast addresses usually have a prefix length of /32, although other prefix lengths are allowed. Multicast addresses represent logical groupings of receivers and not physical collections of devices, and can appear only as the destination in an IP packet, never as the source address.

Notation for Multicast Forwarding States

The multicast forwarding state in a router is usually represented by one of the following notations:

- *(S,G) notation—S refers to the unicast IP address of the source for the multicast traffic and G refers to the particular multicast group IP address for which S is the source. All multicast packets sent from this source have S as the source address and G as the destination address.

- (*, G) notation—The asterisk (*) is a wildcard for the address of any multicast application source sending to group G. For example, if two sources are originating exactly the same content for multicast group 224.1.1.2, a router can use (*, 224.1.1.2) to represent the state of a router forwarding traffic from both sources to the group.

Dense and Sparse Routing Modes

To keep packet replication to a minimum, multicast routing protocols use the two primary modes shown in Table 148 on page 562.
CAUTION: A common multicast guideline is not to run dense mode on a WAN under any circumstances.

Table 148: Primary Multicast Routing Modes

<table>
<thead>
<tr>
<th>Multicast Mode</th>
<th>Description</th>
<th>Appropriate Network for Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dense mode</td>
<td>Network is flooded with traffic on all possible branches, then pruned back as branches explicitly (by message) or implicitly (time-out silence) eliminate themselves.</td>
<td>LANs—Networks in which all possible subnets are likely to have at least one receiver.</td>
</tr>
<tr>
<td>Sparse mode</td>
<td>Network establishes and sends packets only on branches that have at least one leaf indicating (by message) a need for the traffic.</td>
<td>WANs—Network in which very few of the possible receivers require packets from this source.</td>
</tr>
</tbody>
</table>

**Strategies for Preventing Routing Loops**

Routing loops are disastrous in multicast networks because of the risk of repeatedly replicated packets, which can overwhelm a network. One of the complexities of modern multicast routing protocols is the need to avoid routing loops, packet by packet, much more rigorously than in unicast routing protocols. Three multicast strategies—reverse-path forwarding (RPF), shortest-path tree (SPT), and administrative scoping—help prevent routing loops by defining routing paths in different ways.

**Reverse-Path Forwarding for Loop Prevention**

The router’s multicast forwarding state runs more logically based on the reverse path, from the receiver back to the root of the distribution tree. In RPF, every multicast packet received must pass an RPF check before it can be replicated or forwarded on any interface. When it receives a multicast packet on an interface, the router verifies that the source address in the multicast IP packet is the destination address for a unicast IP packet back to the source.

If the outgoing interface found in the unicast routing table is the same interface that the multicast packet was received on, the packet passes the RPF check. Multicast packets that fail the RPF check are dropped, because the incoming interface is not on the shortest path back to the source. Routers can build and maintain separate tables for RPF purposes. See “Understanding PIM RPF Routing Tables” on page 573.

**Shortest-Path Tree for Loop Prevention**

The distribution tree used for multicast is rooted at the source and is the shortest-path tree (SPT), but this path can be long if the source is at the periphery of the network. Providing a shared tree on the backbone as the distribution tree locates the multicast source more centrally in the network. Shared distribution trees with roots in the core network are created and maintained by a multicast router operating as a rendezvous point (RP), a feature of sparse mode multicast protocols.
Administrative Scoping for Loop Prevention

Scoping limits the routers and interfaces that can forward a multicast packet. Multicast scoping is *administrative* in the sense that a range of multicast addresses is reserved for scoping purposes, as described in RFC 2365, *Administratively Scoped IP Multicast*. Routers at the boundary must filter multicast packets and ensure that packets do not stray beyond the established limit.

**Multicast Protocol Building Blocks**

Multicast is not a single protocol, but a collection of protocols working together to form trees, prune branches, locate sources and groups, and prevent routing loops:

- Distance Vector Multicast Routing Protocol (DVMRP) and Protocol Independent Multicast (PIM) operate between routers. PIM can operate in dense mode and sparse mode.
- Three versions of the Internet Group Management Protocol (IGMP) run between receiver hosts and routers.
- Several other routing mechanisms and protocols enhance multicast networks by providing useful functions not included in other protocols. These include the bootstrap router (BSR) mechanism, auto-rendezvous point (RP), Multicast Source Discovery Protocol (MSDP), Session Announcement Protocol (SAP), Session Description Protocol (SDP), and Pragmatic General Multicast (PGM) protocol.

Table 149 on page 563 lists and summarizes these protocols.

**Table 149: Multicast Protocol Building Blocks**

<table>
<thead>
<tr>
<th>Multicast Protocol</th>
<th>Description</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVMRP</td>
<td>Dense-mode-only protocol that uses the flood-and-prune or implicit join method to deliver traffic everywhere and then determine where the uninterested receivers are. DVRMP uses source-based distribution trees in the form (S,G) and builds its own multicast routing tables for RPF checks.</td>
<td>Not appropriate for large-scale Internet use.</td>
</tr>
<tr>
<td>PIM dense mode</td>
<td>Sends an <em>implicit</em> join message, so routers use the flood-and-prune method to deliver traffic everywhere and then determine where the uninterested receivers are. PIM dense mode uses source-based distribution trees in the form (S,G), and also supports sparse-dense mode, with mixed sparse and dense groups. Both PIM modes use unicast routing information for RPF checks.</td>
<td>Most promising multicast protocol in use for LANs.</td>
</tr>
</tbody>
</table>
### Table 149: Multicast Protocol Building Blocks (continued)

<table>
<thead>
<tr>
<th>Multicast Protocol</th>
<th>Description</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM sparse “Understanding IGMP and Multicast” on page 567</td>
<td>Sends an explicit join message, so routers determine where the interested receivers are and send join messages upstream to their neighbors, building trees from receivers to an RP router, which is the initial source of multicast group traffic. PIM sparse mode builds distribution trees in the form (*,G), but migrates to an (S,G) source-based tree if that path is shorter than the path through the RP router for a particular multicast group’s traffic. Both PIM modes use unicast routing information for RPF checks.</td>
<td>Most promising multicast protocol in use for WANs. See “Understanding PIM and Static RPs” on page 569.</td>
</tr>
<tr>
<td>PIM source-specific multicast (SSM)</td>
<td>Enhancement to PIM sparse mode that allows a client to receive multicast traffic directly from the source, without the help of an RP.</td>
<td>Used with IGMPv3 to create a shortest-path tree between receiver and source.</td>
</tr>
<tr>
<td>IGMPv1</td>
<td>The original protocol defined in RFC 1112, <em>Host Extensions for IP Multicasting</em>. IGMPv1 sends an explicit join message to the router, but uses a timeout to determine when hosts leave a group.</td>
<td>See “Understanding IGMP and Multicast” on page 567.</td>
</tr>
<tr>
<td>IGMPv3</td>
<td>Defined in RFC 3376, <em>Internet Group Management Protocol, Version 3</em>. Among other features, IGMPv3 optimizes support for a single source of content for a multicast group, or source-specific multicast (SSM).</td>
<td>Used with PIM SSM to create a shortest-path tree between receiver and source.</td>
</tr>
<tr>
<td>BSR and Auto-RP</td>
<td>Allow sparse-mode routing protocols to find RPs within the routing domain (autonomous system, or AS). RP addresses can also be statically configured.</td>
<td></td>
</tr>
<tr>
<td>MSDP “Understanding SAP and SDP Multicast Session Announcements” on page 566.</td>
<td>Allows groups located in one multicast routing domain to find RPs in other routing domains. MSDP is not used on an RP if all receivers and sources are located in the same routing domain.</td>
<td>Typically runs on the same router as PIM sparse mode RP. Not appropriate if all receivers and sources are located in the same routing domain.</td>
</tr>
</tbody>
</table>
Table 149: Multicast Protocol Building Blocks (continued)

<table>
<thead>
<tr>
<th>Multicast Protocol</th>
<th>Description</th>
<th>Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP and SDP</td>
<td>Display multicast session names and correlate the names with multicast traffic. SDP is a session directory protocol that advertises multimedia conference sessions and communicates setup information to participants who want to join the session. A client commonly uses SDP to announce a conference session by periodically multicasting an announcement packet to a well-known multicast address and port using SAP.</td>
<td></td>
</tr>
<tr>
<td>PGM</td>
<td>Special protocol layer for multicast traffic that can be used between the IP layer and the multicast application to add reliability to multicast traffic. PGM allows a receiver to detect missing information in all cases and request replacement information if the receiver application requires it.</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Routing Overview on page 467
- Multicast Configuration Overview on page 565
- Comparing Multicast to Unicast in the Junos Multicast Protocols Configuration Guide
- IP Multicast Uses in the Junos Multicast Protocols Configuration Guide

Multicast Configuration Overview

You configure a router network to support multicast applications with a related family of protocols. To use multicast, you must understand the basic components of a multicast network and their relationships, and then configure the device to act as a node in the network.

To configure the device as a node in a multicast network:

1. Determine whether the router is directly attached to any multicast sources. Receivers must be able to locate these sources.
2. Determine whether the router is directly attached to any multicast group receivers. If receivers are present, IGMP is needed.
3. Determine whether to use the sparse, dense, or sparse-dense mode of multicast operation. Each mode has different configuration considerations.
4. Determine the address of the rendezvous point (RP) if sparse or sparse-dense mode is used.
5. Determine whether to locate the RP with the static configuration, bootstrap router (BSR), or auto-RP method.

6. Determine whether to configure multicast to use its own reverse-path forwarding (RPF) routing table when configuring PIM in sparse, dense, or sparse-dense modes.

7. (Optional) Configure the SAP and SDP protocols to listen for multicast session announcements. See “Example: Configuring SAP and SDP to Listen for Session Announcements (CLI)” on page 567.


9. (Optional) Configure the PIM static RP. See “Understanding PIM and Static RPs” on page 569.

10. (Optional) Filter PIM register messages from unauthorized groups and sources. See “Example: Rejecting Incoming PIM Register Messages on an RP Router (CLI)” on page 571 and “Example: Stopping Outgoing PIM Register Messages on a Designated Router (CLI)” on page 572.

11. (Optional) Configure a PIM RPF routing table. See “Example: Configuring a PIM RPF Routing Table (CLI)” on page 574.

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Multicast Overview on page 559
- Verifying a Multicast Configuration on page 575

SAP and SDP Multicast Session Announcements

- Understanding SAP and SDP Multicast Session Announcements on page 566
- Example: Configuring SAP and SDP to Listen for Session Announcements (CLI) on page 567

Understanding SAP and SDP Multicast Session Announcements

Multicast session announcements are handled by two protocols, the Session Announcement Protocol (SAP), and Session Description Protocol (SDP). These two protocols display multicast session names and correlate the names with multicast traffic. Enabling SDP and SAP allows the router to receive announcements about multimedia and other multicast sessions from sources. Enabling SAP automatically enables SDP.

The device listens for session announcements on one or more addresses and ports. By default, the router listens to address and port 224.1.2.254:9875.

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Multicast Overview on page 559
Example: Configuring SAP and SDP to Listen for Session Announcements (CLI) on page 567

Example: Configuring SAP and SDP to Listen for Session Announcements (CLI)

To configure SAP and SDP:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 150 on page 567.

Table 150: Configuring SAP and SDP

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Listen</strong> level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter edit protocols sap</td>
</tr>
</tbody>
</table>
| (Optional) Enter one or more addresses and ports for the device to listen to session announcements on. By default, the device listens to address and port 224.2.127.254:9875. | 1. Set the **address** value to the IP address that the device can listen to session announcements on, in dotted decimal notation. For example:
   set listen 224.2.127.254
2. Set the **port** value to the number of the port that the device can listen to session announcements on, in decimal notation. For example:
   set listen 224.2.127.254 port 9875. |

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding SAP and SDP Multicast Session Announcements on page 566
- Multicast Configuration Overview on page 565

Multicast IGMP

- Understanding IGMP and Multicast on page 567
- Example: Configuring IGMP for Multicast (CLI) on page 568

Understanding IGMP and Multicast

The Internet Group Management Protocol (IGMP) manages the membership of hosts and routers in multicast groups. IGMP is an integral part of IP and must be enabled on all routers and hosts that need to receive IP multicasts. IGMP is automatically enabled on all broadcast interfaces when you configure PIM or DVMRP.
By default, the device runs IGMPv2. However, you might still want to set the IGMP version explicitly on an interface, or all interfaces. Routers running different versions of IGMP negotiate the lowest common version of IGMP supported by hosts on their subnet. One host running IGMPv1 forces the device to use that version and lose features important to other hosts.

**Related Topics**
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Multicast Overview on page 559
- Example: Configuring IGMP for Multicast (CLI) on page 568
- IGMP Overview in the *Junos Multicast Protocols Configuration Guide*

**Example: Configuring IGMP for Multicast (CLI)**

To explicitly configure the IGMP version, perform these steps on each device in the network:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 151 on page 568.
3. If you are finished configuring the router, commit the configuration.

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Interface</strong> level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter <code>edit protocols igmp</code></td>
</tr>
</tbody>
</table>
| Set the IGMP version. By default, the device uses IGMPv2, but this version can be changed through negotiation with hosts unless explicitly configured. | 1. Set the **interface** value to the interface name, or all. For example: `set igmp interface all`
2. Set the **version** value to 1, 2, or 3. For example: `set igmp interface all version 2` |

**Related Topics**
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding IGMP and Multicast on page 567
- Configuring IGMP in the *Junos Multicast Protocols Configuration Guide*
- Enabling IGMP in the *Junos Multicast Protocols Configuration Guide*
- Multicast Configuration Overview on page 565
Understanding PIM and Static RPs

Protocol Independent Multicast (PIM) sparse mode is the most common multicast protocol used on the Internet. PIM sparse mode is the default mode whenever PIM is configured on any interface of the device. However, because PIM must not be configured on the network management interface, you must disable it on that interface.

Each any-source multicast (ASM) group has a shared tree through which receivers learn about new multicast sources and new receivers learn about all multicast sources. The rendezvous point (RP) router is the root of this shared tree and receives the multicast traffic from the source. To receive multicast traffic from the groups served by the RP, the device must determine the IP address of the RP for the source.

One common way for the device to locate RPs is by static configuration of the IP address of the RP. For information about alternate methods of locating RPs, see the JUNOS Multicast Protocols Configuration Guide.

Example: Configuring PIM Sparse Mode and RP Static IP Addresses (CLI)

To configure PIM sparse mode, disable PIM on ge-0/0/0, and configure the IP address of the RP, and perform these steps on each device in the network:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 152 on page 570.
### Table 152: Configuring PIM Sparse Mode and the RP

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Interface</strong> level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter <code>edit protocols pim</code></td>
</tr>
<tr>
<td>Enable PIM on all network interfaces.</td>
<td>Set the <code>interface</code> value to <code>all</code>. For example: <code>set pim interface all</code></td>
</tr>
<tr>
<td>Apply your configuration changes.</td>
<td>Changes in the CLI are applied automatically when you execute the <code>set</code> command.</td>
</tr>
<tr>
<td>Remain at the <strong>Interface</strong> level in the configuration hierarchy.</td>
<td>Remain at the [edit protocols pim interface] hierarchy level.</td>
</tr>
<tr>
<td>Disable PIM on the network management interface.</td>
<td>Disable the <code>ge-0/0/0</code> interface: <code>set pim interface ge-0/0/0 unit 0 disable</code></td>
</tr>
<tr>
<td>Apply your configuration changes.</td>
<td>Changes in the CLI are applied automatically when you execute the <code>set</code> command.</td>
</tr>
<tr>
<td>Navigate to the <strong>Rp</strong> level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter <code>edit protocols pim rp</code></td>
</tr>
<tr>
<td>Configure the IP address of the RP—for example, <strong>192.168.14.27</strong>.</td>
<td>Set the <code>address</code> value to the IP address of the RP: <code>set static address 192.168.14.27</code></td>
</tr>
</tbody>
</table>

**Related Topics**
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Understanding PIM and Static RPs on page 569
- PIM Configuration Statements in the *Junos Multicast Protocols Configuration Guide*
- Configuring Static PIM RPs in the *Junos Multicast Protocols Configuration Guide*
- Multicast Configuration Overview on page 565

**PIM Register Messages**
- Understanding PIM Register Messages on page 571
- Example: Rejecting Incoming PIM Register Messages on an RP Router (CLI) on page 571
- Example: Stopping Outgoing PIM Register Messages on a Designated Router (CLI) on page 572
Understanding PIM Register Messages

When a source in a multicast network becomes active, the source’s designated router (DR) encapsulates multicast data packets into a PIM register message and sends them by means of unicast to the rendezvous point (RP) router.

To prevent unauthorized groups and sources from registering with an RP router, you can define a routing policy to reject PIM register messages from specific groups and sources and configure the policy on the designated router or the RP router.

- If you configure the reject policy on an RP router, it rejects incoming PIM register messages from the specified groups and sources. The RP router also sends a register stop message by means of unicast to the designated router. On receiving the register stop message, the designated router sends periodic null register messages for the specified groups and sources to the RP router.
- If you configure the reject policy on a designated router, it stops sending PIM register messages for the specified groups and sources to the RP router.

**NOTE:** If you have configured the reject policy on an RP router, we recommend that you configure the same policy on all the RP routers in your multicast network.

**NOTE:** If you delete a group and source address from the reject policy configured on an RP router and commit the configuration, the RP router will register the group and source only when the designated router sends a null register message.

**Related Topics**

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Multicast Overview on page 559
- Example: Rejecting Incoming PIM Register Messages on an RP Router (CLI) on page 571
- Example: Stopping Outgoing PIM Register Messages on a Designated Router (CLI) on page 572
- Filtering Multicast Messages in the *Junos Multicast Protocols Configuration Guide*
- Routing Policies Overview on page 581

**Example: Rejecting Incoming PIM Register Messages on an RP Router (CLI)**

To reject incoming PIM register messages on an RP router:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 153 on page 572.
3. If you are finished configuring the router, commit the configuration.
### Table 153: Rejecting Incoming PIM Register Messages on an RP Router

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Policy options level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter edit policy-options</td>
</tr>
</tbody>
</table>
| Define a policy to reject PIM register messages from a group and source address. | 1. Set the match condition for the group address: set policy statement reject-pim-register-msg-rp from route-filter 224.1.1.1/32 exact  
2. Set the match condition for the address of a source in the group: set policy statement reject-pim-register-msg-rp from source-address-filter 10.10.10.1/32 exact  
3. Set the match action to reject PIM register messages from the group and source address: set policy statement reject-pim-register-msg-rp then reject |
| Configure the reject-pim-register-msg-rp policy on the RP router. | 1. From the [edit] hierarchy level, enter edit protocols pim rp  
2. Assign the policy on the RP: set rp-register-policy reject-pim-register-msg-rp |

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding PIM Register Messages on page 571
- Example: Stopping Outgoing PIM Register Messages on a Designated Router (CLI) on page 572
- Configuring Register Message Filtering on a PIM RP or DR in the Junos Multicast Protocols Configuration Guide
- Example: Configuring Register Message Filters on PIM RPs and DRs in the Junos Multicast Protocols Configuration Guide
- Multicast Configuration Overview on page 565

**Example: Stopping Outgoing PIM Register Messages on a Designated Router (CLI)**

To stop outgoing PIM register messages on a designated router:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 154 on page 573.
3. If you are finished configuring the router, commit the configuration.
Table 154: Stopping Outgoing PIM Register Messages on a Designated Router

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Policy options</strong> level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter</td>
</tr>
<tr>
<td></td>
<td>edit policy-options</td>
</tr>
<tr>
<td>Define a policy to not send PIM register messages for a group and source address.</td>
<td>1. Set the match condition for the group address:</td>
</tr>
<tr>
<td></td>
<td>set policy statement stop-pim-register-msg-dr from route-filter 224.2.2.2/32 exact</td>
</tr>
<tr>
<td></td>
<td>2. Set the match condition for the address of a source in the group:</td>
</tr>
<tr>
<td></td>
<td>set policy statement stop-pim-register-msg-dr from source-address-filter 20.20.20.1/32 exact</td>
</tr>
<tr>
<td></td>
<td>3. Set the match action to not send PIM register messages for the group and source address:</td>
</tr>
<tr>
<td></td>
<td>set policy statement stop-pim-register-msg-dr then reject</td>
</tr>
<tr>
<td>Configure the <strong>stop-pim-register-msg-dr</strong> policy on the designated router.</td>
<td>1. From the [edit] hierarchy level, enter</td>
</tr>
<tr>
<td></td>
<td>edit protocols pim rp</td>
</tr>
<tr>
<td></td>
<td>2. Assign the policy on the designated router:</td>
</tr>
<tr>
<td></td>
<td>set dr-register-policy stop-pim-register-msg-dr</td>
</tr>
</tbody>
</table>

**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding PIM Register Messages on page 571
- Example: Rejecting Incoming PIM Register Messages on an RP Router (CLI) on page 571
- Configuring Register Message Filtering on a PIM RP or DR in the *Junos Multicast Protocols Configuration Guide*
- Example: Configuring Register Message Filters on PIM RPs and DRs in the *Junos Multicast Protocols Configuration Guide*
- Multicast Configuration Overview on page 565

**PIM RPF Routing Tables**

- Understanding PIM RPF Routing Tables on page 573
- Example: Configuring a PIM RPF Routing Table (CLI) on page 574

**Understanding PIM RPF Routing Tables**

By default, PIM uses *inet.0* as its reverse-path forwarding (RPF) routing table group. PIM uses an RPF routing table group to resolve its RPF neighbor for a particular multicast source address and for the RP address. PIM can optionally use *inet.2* as its
RPF routing table group. The \texttt{inet.2} routing table is organized more efficiently for RPF checks.

Once configured, the RPF routing table must be applied to a PIM as a routing table group.

\textbf{Related Topics}
- \textit{Junos OS Feature Support Reference for SRX Series and J Series Devices}
- Multicast Overview on page 559
- Example: Configuring a PIM RPF Routing Table (CLI) on page 574
- Configuring a PIM RPF Routing Table in the \textit{Junos Multicast Protocols Configuration Guide}

\textbf{Example: Configuring a PIM RPF Routing Table (CLI)}

To configure and apply a PIM RPF routing table, perform these steps on each device in the network:

1. Navigate to the top of the configuration hierarchy.
2. Perform the configuration tasks described in Table 155 on page 574.
3. If you are finished configuring the router, commit the configuration.

\textbf{Table 155: Configuring a PIM RPF Routing Table}

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the \texttt{Routing options} level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter \texttt{edit routing-options}</td>
</tr>
<tr>
<td>Configure a new group for the RPF routing table.</td>
<td>Enter \texttt{edit rib-groups}</td>
</tr>
<tr>
<td>Configure a name for the new RPF routing table group—for example, \texttt{multicast-rpf-rib}—and use \texttt{inet.2} for its export routing table.</td>
<td>Enter \texttt{set multicast-rpf-rib export-rib inet.2}</td>
</tr>
<tr>
<td>Configure the new RPF routing table group to use \texttt{inet.2} for its import routing table.</td>
<td>Enter \texttt{set multicast-rpf-rib import-rib inet.2}</td>
</tr>
<tr>
<td>Navigate to the \texttt{Rib group} level in the configuration hierarchy.</td>
<td>From the [edit] hierarchy level, enter \texttt{edit protocols pim}</td>
</tr>
<tr>
<td>Apply the new RPF routing table to PIM.</td>
<td>Enter \texttt{set rib-group multicast-rpf-rib}</td>
</tr>
</tbody>
</table>
### Table 155: Configuring a PIM RPF Routing Table (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a routing table group for the interface routes.</td>
<td>From the [edit] hierarchy level, enter <code>edit routing-options rib-groups</code>.</td>
</tr>
<tr>
<td>Configure a name for the RPF routing table group—for example, <code>if-rib</code>—and use <code>inet.2</code> and <code>inet.0</code> for its import routing tables.</td>
<td>Enter <code>set if-rib import-rib inet.2</code> and <code>set if-rib import-rib inet.0</code>.</td>
</tr>
<tr>
<td>Add the new interface routing table group to the interface routes.</td>
<td>From the [edit] hierarchy level, enter <code>edit routing-options interface-routes set rib-group inet if-rib</code>.</td>
</tr>
</tbody>
</table>

### Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding PIM RPF Routing Tables on page 573
- Configuring a PIM RPF Routing Table in the *Junos Multicast Protocols Configuration Guide*
- Multicast Configuration Overview on page 565

### Verifying a Multicast Configuration

To verify a multicast configuration, perform these tasks:
- Verifying SAP and SDP Addresses and Ports on page 575
- Verifying the IGMP Version on page 576
- Verifying the PIM Mode and Interface Configuration on page 576
- Verifying the PIM RP Configuration on page 577
- Verifying the RPF Routing Table Configuration on page 577

### Verifying SAP and SDP Addresses and Ports

**Purpose**
Verify that SAP and SDP are configured to listen on the correct group addresses and ports.

**Action**
From the CLI, enter the `show sap listen` command.

**Sample Output**
```
user@host> show sap listen
Group Address   Port
224.2.127.254   9875
```
Meaning  The output shows a list of the group addresses and ports that SAP and SDP listen on. Verify the following information:
  ■ Each group address configured, especially the default 224.2.127.254, is listed.
  ■ Each port configured, especially the default 9875, is listed.

Verifying the IGMP Version

Purpose  Verify that IGMP version 2 is configured on all applicable interfaces.

Action  From the CLI, enter the show igmp interface command.

Sample Output  user@host> show igmp interface
Interface: ge-0/0/0.0
   Querier: 192.168.4.36
   State:         Up Timeout:     197 Version:  2 Groups:      0

Configured Parameters:
IGMP Query Interval: 125.0
IGMP Query Response Interval: 10.0
IGMP Last Member Query Interval: 1.0
IGMP Robustness Count: 2

Derived Parameters:
IGMP Membership Timeout: 260.0
IGMP Other Querier Present Timeout: 255.0

Meaning  The output shows a list of the interfaces that are configured for IGMP. Verify the following information:
  ■ Each interface on which IGMP is enabled is listed.
  ■ Next to Version, the number 2 appears.

Verifying the PIM Mode and Interface Configuration

Purpose  Verify that PIM sparse mode is configured on all applicable interfaces.

Action  From the CLI, enter the show pim interfaces command.

Sample Output  user@host> show pim interfaces
Instance: PIM.master

<table>
<thead>
<tr>
<th>Name</th>
<th>Stat</th>
<th>Mode</th>
<th>IP V State</th>
<th>Count</th>
<th>DR address</th>
</tr>
</thead>
<tbody>
<tr>
<td>lo0.0</td>
<td>Up</td>
<td>Sparse</td>
<td>4 2 DR</td>
<td>0</td>
<td>127.0.0.1</td>
</tr>
<tr>
<td>pime.32769</td>
<td>Up</td>
<td>Sparse</td>
<td>4 2 P2P</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Meaning  The output shows a list of the interfaces that are configured for PIM. Verify the following information:
  ■ Each interface on which PIM is enabled is listed.
  ■ The network management interface, either ge–0/0/0 or fe–0/0/0, is not listed.
Verifying the PIM RP Configuration

**Purpose**
Verify that the PIM RP is statically configured with the correct IP address.

**Action**
From the CLI, enter the `show pim rps` command.

**Sample Output**
```
user@host> show pim rps
Instance: PIM.master
Address family INET
RP address      Type      Holdtime Timeout Active groups Group prefixes
192.168.14.27   static           0    None             2 224.0.0.0/4
```

**Meaning**
The output shows a list of the RP addresses that are configured for PIM. At least one RP must be configured. Verify the following information:
- The configured RP is listed with the proper IP address.
- Under Type, the word `static` appears.

Verifying the RPF Routing Table Configuration

**Purpose**
Verify that the PIM RPF routing table is configured correctly.

**Action**
From the CLI, enter the `show multicast rpf` command.

**Sample Output**
```
user@host> show multicast rpf
Multicast RPF table: inet.0 , 2 entries...
```

**Meaning**
The output shows the multicast RPF table that is configured for PIM. If no multicast RPF routing table is configured, RPF checks use `inet.0`. Verify the following information:
- The configured multicast RPF routing table is `inet.0`.
- The `inet.0` table contains entries.

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Multicast Configuration Overview on page 565
- show sap listen in the Junos Routing Protocols and Policies Command Reference
- show igmp interface in the Junos Routing Protocols and Policies Command Reference
- show pim interfaces in the Junos Routing Protocols and Policies Command Reference
- show pim rps in the Junos Routing Protocols and Policies Command Reference
- show multicast rpf in the Junos Routing Protocols and Policies Command Reference
Part 3
Routing Policies and Stateless Firewall Filters

- Routing Policies on page 581
- Stateless Firewall Filters on page 607
Chapter 23
Routing Policies

- Routing Policies Overview on page 581
- Routing Policies Configuration Overview on page 582
- Routing Policies on page 583
- Routing Policy Terms on page 584
- Routing Policy Match Conditions and Actions on page 586
- Routing Policy Damping Parameters on page 602

Routing Policies Overview

A routing policy has a major impact on the flow of routing information or packets within and through the device. The match conditions and actions allow you to configure a customized policy to fit your needs.

Routing protocols send information about routes to a router’s neighbors. This information is processed and used to create routing tables, which are then distilled into forwarding tables. Routing policies control the flow of information between the routing protocols and the routing tables and between the routing tables and the forwarding tables. Using policies, you can determine which routes are advertised, specify which routes are imported into the routing table, and modify routes to control which routes are added to the forwarding table.

To create a routing policy, you configure criteria against which routes are compared, and the action that is performed if the criteria are met.

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Routing Policies Configuration Overview on page 582
- Routing Overview on page 467
Routing Policies Configuration Overview

To configure a routing policy:

1. Determine what you want to accomplish with the policy, and thoroughly understand how to achieve your goal using the various match conditions and actions.

2. Make certain that you understand the default policies and actions for the policy you are configuring.


4. Configure an Interior Gateway Protocol (IGP) and Border Gateway Protocol (BGP), if necessary. See:
   - RIP Configuration Overview on page 491
   - OSPF Configuration Overview on page 504
   - IS-IS Configuration Overview on page 529
   - BGP Configuration Overview on page 542

5. Configure the router interface to reject or accept routes, if necessary.

6. Configure static routes, if necessary. See “Static Routing Configuration Overview” on page 475.

7. Name the policy. See “Example: Creating a Routing Policy” on page 583.

8. Configure the policy term. See “Example: Creating a Routing Policy Term” on page 585.


10. (Optional) Advertise additional routes. See “Example: Injecting OSPF Routes into the BGP Routing Table” on page 597.

11. (Optional) Create a forwarding class. See “Example: Grouping Source and Destination Prefixes into a Forwarding Class” on page 594.

12. (Optional) Make a route less preferable to BGP. See “Example: Configuring a Routing Policy to Prepend the AS Path” on page 600.


Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Routing Policies Overview on page 581
- Minimum Routing Policy Configuration in the Junos Policy Framework Configuration Guide
- Testing Routing Policies in the Junos Policy Framework Configuration Guide
Routing Policies

- Understanding Routing Policies on page 583
- Example: Creating a Routing Policy on page 583

Understanding Routing Policies

Each routing policy is identified by a policy name. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters long. To include spaces in the name, enclose the entire name in double quotation marks. Each routing policy name must be unique within a configuration.

Once a policy is created and named, it must be applied before it is active. You apply routing policies using the `import` and `export` statements at the `protocols>protocol-name` level in the configuration hierarchy.

In the `import` statement, you list the name of the routing policy to be evaluated when routes are imported into the routing table from the routing protocol.

In the `export` statement, you list the name of the routing policy to be evaluated when routes are being exported from the routing table into a dynamic routing protocol. Only active routes are exported from the routing table.

To specify more than one policy and create a policy chain, you list the policies using a space as a separator. If multiple policies are specified, the policies are evaluated in the order in which they are specified. As soon as an accept or reject action is executed, the policy chain evaluation ends.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Routing Policies Overview on page 581
- Example: Creating a Routing Policy on page 583
- Router Flows Affected by Policies in the Junos Policy Framework Configuration Guide

Example: Creating a Routing Policy

This example shows how to create a simple routing policy.

- Requirements on page 584
- Overview on page 584
- Configuration on page 584
- Verification on page 584
**Requirements**

Before you begin, determine what you want to accomplish with the policy, configure router interfaces, and configure routing protocols, as explained in “Routing Policies Configuration Overview” on page 582.

**Overview**

In this example, you create a routing policy called policy1.

**Configuration**

**Step-by-Step Procedure**

To create a routing policy:

1. Create the routing policy.
   
   [edit]
   
   user@host# set policy-options policy-statement policy1

2. Commit the configuration if you are done configuring the device.
   
   [edit]
   
   user@host# commit

**NOTE:** The policy does not take effect until you apply it.

**Verification**

To verify your configuration, use the `show policy-options` command.

**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Routing Policies Configuration Overview on page 582
- Understanding Routing Policies on page 583

**Routing Policy Terms**

- Understanding Routing Policy Terms on page 585
- Example: Creating a Routing Policy Term on page 585
Understanding Routing Policy Terms

Routing policies are made up of one or more terms. Each routing policy term is identified by a term name. The name can contain letters, numbers, and hyphens (-) and can be up to 255 characters long. To include spaces in the name, enclose the entire name in double quotation marks.

Each term contains a set of match conditions and a set of actions:

- Match conditions are criteria that a route must match before the actions can be applied. If a route matches all criteria, one or more actions are applied to the route.
- Actions specify whether to accept or reject the route, control how a series of policies are evaluated, and manipulate the characteristics associated with a route.

Generally, a router compares a route against the match conditions of each term in a routing policy, starting with the first and moving through the terms in the order in which they are defined, until a match is made and an explicitly configured or default action of accept or reject is taken. If none of the terms in the policy match the route, the router compares the route against the next policy, and so on, until either an action is taken or the default policy is evaluated.

If none of the match conditions of each term evaluates to true, the final action is executed. The final action is defined in an unnamed term. Additionally, you can define a default action (either accept or reject) that overrides any action intrinsic to the protocol.

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Routing Policies Overview on page 581
- Example: Creating a Routing Policy Term on page 585

Example: Creating a Routing Policy Term

This example shows how to create a routing policy term.

- Requirements on page 585
- Overview on page 586
- Configuration on page 586
- Verification on page 586

Requirements

Before you begin, determine what you want to accomplish with the policy, configure router interfaces, and configure routing protocols, as explained in “Routing Policies Configuration Overview” on page 582.
Overview

In this example, you create a routing policy called policy1 and a term for the policy called term1.

Configuration

Step-by-Step Procedure  To configure a routing policy term:

1. Create the routing policy.

   [edit]
   user@host# edit policy-options policy-statement policy1

2. Create the policy term.

   [edit policy-options policy-statement policy1]
   user@host# set term term1

3. Commit the configuration if you are done configuring the device.

   [edit policy-options policy-statement policy1]
   user@host# commit

NOTE: The policy does not take effect until you apply it.

Verification

To verify your configuration, use the show policy-options command.

Related Topics  ■ Junos OS Feature Support Reference for SRX Series and J Series Devices
    ■ Routing Policies Configuration Overview on page 582
    ■ Understanding Routing Policy Terms on page 585

Routing Policy Match Conditions and Actions

■ Understanding Routing Policy Match Conditions and Actions on page 587
■ Route-Based Match Conditions on page 591
■ Protocol-Based Match Conditions on page 596
■ Autonomous System Path-Based Actions on page 599
Understanding Routing Policy Match Conditions and Actions

A match condition defines the criteria that a route must match for an action to take place. Each term can have one or more match conditions. If a route matches all the match conditions for a particular term, the actions defined for that term are processed.

This topic contains the following sections:
- Match Conditions on page 587
- Actions on page 588

Match Conditions

Each term can consist of two statements, from and to, that define match conditions:
- In the from statement, you define the criteria that an incoming route must match. You can specify one or more match conditions. If you specify more than one, all conditions must match the route for a match to occur.
- In the to statement, you define the criteria that an outgoing route must match. You can specify one or more match conditions. If you specify more than one, all conditions must match the route for a match to occur.

The order of match conditions in a term is not important, because a route must match all match conditions in a term for an action to be taken.

Table 156 on page 587 summarizes key routing policy match conditions.

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggregate-contributor</td>
<td>Matches routes that are contributing to a configured aggregate. This match condition can be used to suppress a contributor in an aggregate route.</td>
</tr>
<tr>
<td>area area-id</td>
<td>Matches a route learned from the specified OSPF area during the exporting of OSPF routes into other protocols.</td>
</tr>
<tr>
<td>as-path name</td>
<td>Matches the name of the path regular expression of an autonomous systems (AS). BGP routes whose AS path matches the regular expression are processed.</td>
</tr>
<tr>
<td>color preference</td>
<td>Matches a color value. You can specify preference values that are finer-grained than those specified in the preference match conditions. The color value can be a number from 0 through 4,294,967,295 (2^32 – 1). A lower number indicates a more preferred route.</td>
</tr>
<tr>
<td>community</td>
<td>Matches the name of one or more communities. If you list more than one name, only one name needs to match for a match to occur. (The matching is effectively a logical OR operation.)</td>
</tr>
<tr>
<td>external [type metric-type]</td>
<td>Matches external OSPF routes, including routes exported from one level to another. In this match condition, type is an optional keyword. The metric-type value can be either 1 or 2. When you do not specify type, this condition matches all external routes.</td>
</tr>
</tbody>
</table>
### Table 156: Summary of Key Routing Policy Match Conditions (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface interface-name</td>
<td>Matches the name or IP address of one or more router interfaces. Use this condition with protocols that are interface-specific. For example, do not use this condition with internal BGP (IBGP). Depending on where the policy is applied, this match condition matches routes learned from or advertised through the specified interface.</td>
</tr>
<tr>
<td>internal</td>
<td>Matches a routing policy against the internal flag for simplified next-hop self policies.</td>
</tr>
<tr>
<td>level level</td>
<td>Matches the IS-IS level. Routes that are from the specified level or are being advertised to the specified level are processed.</td>
</tr>
<tr>
<td>local-preference value</td>
<td>Matches a BGP local preference attribute. The preference value can be from 0 through $4,294,967,295$ ($2^{32} - 1$).</td>
</tr>
<tr>
<td>metric metric</td>
<td>Matches a metric value. The metric value corresponds to the multiple exit discriminator (MED), and metric2 corresponds to the IGP metric if the BGP next hop runs back through another route.</td>
</tr>
<tr>
<td>neighbor address</td>
<td>Matches the address of one or more neighbors (peers).</td>
</tr>
<tr>
<td>next-hop address</td>
<td>Matches the next-hop address or addresses specified in the routing information for a particular route. For BGP routes, matches are performed against each protocol next hop.</td>
</tr>
<tr>
<td>origin value</td>
<td>Matches the BGP origin attribute, which is the origin of the AS path information. The value can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>egp</strong>—Path information originated from another AS.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>igp</strong>—Path information originated from within the local AS.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>incomplete</strong>—Path information was learned by some other means.</td>
</tr>
<tr>
<td>preference preference preference2</td>
<td>Matches the preference value. You can specify a primary preference value (preference) and a secondary preference value (preference2). The preference value can be a number from 0 through $4,294,967,295$ ($2^{32} - 1$). A lower number indicates a more preferred route.</td>
</tr>
<tr>
<td>protocol protocol</td>
<td>Matches the name of the protocol from which the route was learned or to which the route is being advertised. It can be one of the following: <strong>aggregate</strong>, <strong>bgp</strong>, <strong>direct</strong>, <strong>dvmrp</strong>, <strong>isis</strong>, <strong>local</strong>, <strong>ospf</strong>, <strong>pim-dense</strong>, <strong>pim-sparse</strong>, <strong>rip</strong>, <strong>ripng</strong>, <strong>static</strong>.</td>
</tr>
<tr>
<td>route-type value</td>
<td>Matches the type of route. The value can be either <strong>external</strong> or <strong>internal</strong>.</td>
</tr>
</tbody>
</table>

### Actions

An action defines what the router does with the route when the route matches all the match conditions in the from and to statements for a particular term. If a term...
does not have from and to statements, all routes are considered to match and the actions apply to all routes.

Each term can have one or more of the following types of actions. The actions are configured under the then statement.

- Flow control actions, which affect whether to accept or reject the route and whether to evaluate the next term or routing policy
- Actions that manipulate route characteristics
- Trace action, which logs route matches

If you do not specify an action, one of the following results occurs:

- The next term in the routing policy, if one exists, is evaluated.
- If the routing policy has no more terms, the next routing policy, if one exists, is evaluated.
- If there are no more terms or routing policies, the accept or reject action specified by the default policy is executed.

Table 157 on page 589 summarizes the routing policy actions.

<table>
<thead>
<tr>
<th><strong>Table 157: Summary of Key Routing Policy Actions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
</tr>
<tr>
<td>Flow Control Actions</td>
</tr>
<tr>
<td>accept</td>
</tr>
<tr>
<td>reject</td>
</tr>
<tr>
<td>next term</td>
</tr>
<tr>
<td>next policy</td>
</tr>
<tr>
<td>Route Manipulation Actions</td>
</tr>
<tr>
<td>as-path-prepend as-path</td>
</tr>
</tbody>
</table>
### Table 157: Summary of Key Routing Policy Actions (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>as-path-expand last-as count n</strong></td>
<td>Extracts the last AS number in the existing AS path and appends that AS number to the beginning of the AS path n times. Replace n with a number from 1 through 32. The AS numbers are added after the local AS number has been added to the path. This action adds AS numbers to AS sequences only, not to AS sets. If the existing AS path begins with a confederation sequence or set, the appended AS numbers are placed within a confederation sequence. Otherwise, the appended AS numbers are placed with a nonconfederation sequence.</td>
</tr>
<tr>
<td><strong>class class-name</strong></td>
<td>Applies the specified class-of-service (CoS) parameters to routes installed into the routing table.</td>
</tr>
<tr>
<td><strong>color preference</strong>&lt;br&gt;<strong>color2 preference</strong></td>
<td>Sets the preference value to the specified value. The color and color2 preference values can be a number from 0 through 4,294,967,295 ( (2^{32} - 1) ). A lower number indicates a more preferred route.</td>
</tr>
<tr>
<td><strong>damping name</strong></td>
<td>Applies the specified route-damping parameters to the route. These parameters override BGP’s default damping parameters. This action is useful only in import policies.</td>
</tr>
<tr>
<td><strong>local-preference value</strong></td>
<td>Sets the BGP local preference attribute. The preference can be a number from 0 through 4,294,967,295 ( (2^{32} - 1) ).</td>
</tr>
<tr>
<td><strong>metric metric</strong>&lt;br&gt;<strong>metric2 metric</strong>&lt;br&gt;<strong>metric3 metric</strong>&lt;br&gt;<strong>metric4 metric</strong></td>
<td>Sets the metric. You can specify up to four metric values, starting with metric (for the first metric value) and continuing with metric2, metric3, and metric4. For BGP routes, metric corresponds to the MED, and metric2 corresponds to the IGP metric if the BGP next hop loops through another router.</td>
</tr>
<tr>
<td><strong>next-hop address</strong></td>
<td>Sets the next hop. If you specify address as self, the next-hop address is replaced by one of the local router’s addresses. The advertising protocol determines which address to use.</td>
</tr>
</tbody>
</table>

**Related Topics**
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- [Routing Policies Overview on page 581](#)
- [Understanding Route-Based Match Conditions on page 591](#)
- [Understanding Protocol-Based Match Conditions on page 596](#)
- [Understanding Autonomous System Path-Based Actions on page 599](#)
- [Configuring Match Conditions in Routing Policy Terms in the Junos Policy Framework Configuration Guide](#)
- [Configuring Actions in Routing Policy Terms in the Junos Policy Framework Configuration Guide](#)
**Route-Based Match Conditions**

- Understanding Route-Based Match Conditions on page 591
- Example: Rejecting Known Invalid Routes on page 592
- Example: Grouping Source and Destination Prefixes into a Forwarding Class on page 594

**Understanding Route-Based Match Conditions**

You can specify known invalid ("bad") routes to ignore by specifying matches on destination prefixes. When specifying a destination prefix, you can specify an exact match with a specific route, or a less precise match by using match types. You can configure either a common reject action that applies to the entire list, or an action associated with each prefix.

Additionally, you can specify that “good” routes be processed in a particular way. For instance, you can group traffic from specific source or destination addresses into forwarding classes to be processed using the class of service (CoS) feature.

Table 158 on page 591 lists route list match types.

**Table 158: Route List Match Types**

<table>
<thead>
<tr>
<th>Match Type</th>
<th>Match Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>exact</td>
<td>The route shares the same most-significant bits (described by (prefix-length)) and (prefix-length) is equal to the route’s prefix length.</td>
</tr>
<tr>
<td>longer</td>
<td>The route shares the same most-significant bits (described by (prefix-length)) and (prefix-length) is greater than the route’s prefix length.</td>
</tr>
<tr>
<td>orlonger</td>
<td>The route shares the same most-significant bits (described by (prefix-length)) and (prefix-length) is equal to or greater than the route’s prefix length.</td>
</tr>
<tr>
<td>prefix-length-range (prefix-length2)-(prefix-length3)</td>
<td>The route shares the same most-significant bits (described by (prefix-length)), and the route’s prefix length falls between (prefix-length2) and (prefix-length3), inclusive.</td>
</tr>
<tr>
<td>through (destination-prefix)</td>
<td>All the following are true:</td>
</tr>
<tr>
<td></td>
<td>■ The route shares the same most-significant bits (described by (prefix-length)) of the first destination prefix.</td>
</tr>
<tr>
<td></td>
<td>■ The route shares the same most-significant bits (described by (prefix-length)) of the second destination prefix for the number of bits in the prefix length.</td>
</tr>
<tr>
<td></td>
<td>■ The number of bits in the route’s prefix length is less than or equal to the number of bits in the second prefix.</td>
</tr>
</tbody>
</table>

You do not use the `through` match type in most routing policy configurations. See the JUNOS Policy Framework Configuration Guide.
Table 158: Route List Match Types (continued)

<table>
<thead>
<tr>
<th>Match Type</th>
<th>Match Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>upto prefix-length2</td>
<td>The route shares the same most-significant bits (described by prefix-length) and the route's prefix length falls between prefix-length and prefix-length2.</td>
</tr>
</tbody>
</table>

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding Routing Policy Match Conditions and Actions on page 587
- Example: Rejecting Known Invalid Routes on page 592
- Example: Grouping Source and Destination Prefixes into a Forwarding Class on page 594
- Routing Policies Configuration Overview on page 582
- Junos OS Class of Service Configuration Guide for Security Devices

Example: Rejecting Known Invalid Routes

This example shows how to create route-based match conditions for a routing policy.

Requirements on page 592
Overview on page 592
Configuration on page 592
Verification on page 593

Requirements

Before you begin, configure router interfaces and configure routing protocols, as explained in “Routing Policies Configuration Overview” on page 582.

Overview

In this example, you create a policy called rejectpolicy1 that rejects routes with a mask of /8 and greater (/8, /9, /10, and so on) that have the first 8 bits set to 0. This policy also accepts routes less than 8 bits in length by creating a mask of 0/0 up to /7.

Configuration

CLI Quick Configuration

To quickly create a policy that rejects known invalid routes copy the following commands and paste them into the CLI.

```
[edit]
set policy-options policy-statement rejectpolicy1 term rejectterm1 from route-filter 0.0.0.0/0 upto /7 accept
set policy-options policy-statement rejectpolicy1 term rejectterm1 from route-filter 0.0.0.0/8 orlonger reject
set policy-options policy-statement test term 1 from protocol direct
```
Step-by-Step Procedure  

To create a policy that rejects known invalid routes:

1. Create the routing policy.
   
   ```
   [edit]
   user@host# edit policy-options policy-statement rejectpolicy1
   ```

2. Create the policy term.
   
   ```
   [edit policy-options policy-statement rejectpolicy1]
   user@host# edit term rejectterm1
   ```

3. Create a mask that specifies which routes to accept.
   
   ```
   [edit policy-options policy-statement rejectpolicy1 term rejectterm1]
   user@host# set from route-filter 0/0 upto /7 accept
   ```

4. Create a mask that specifies which routes to reject.
   
   ```
   [edit policy-options policy-statement rejectpolicy1 term rejectterm1]
   user@host# set from route-filter 0/8 orlonger reject
   ```

Results  

Confirm your configuration by entering the `show policy-options` command from configuration mode. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

   ```
   user@host# show policy-options
   policy-statement rejectpolicy1 {
     term rejectterm1 {
       from {
         route-filter 0.0.0.0/0 upto /7 accept;
         route-filter 0.0.0.0/8 orlonger reject;
       }
     }
   }
   ```

If you are done configuring the device, enter `commit` from configuration mode.

Verification  

To confirm that the configuration is working properly, perform these tasks:

- Verifying the Route-Based Match Conditions on page 593

Verifying the Route-Based Match Conditions  

Purpose  

Verify that the policy and term are configured on the device with the appropriate route-based match conditions.

Action  

From operational mode, enter the `show policy-options` command.
Example: Grouping Source and Destination Prefixes into a Forwarding Class

This example shows how to group source and destination prefixes into a forwarding class.

Requirements on page 594
Overview on page 594
Configuration on page 594
Verification on page 596

Requirements

Before you begin, configure router interfaces and configure routing protocols, as explained in “Routing Policies Configuration Overview” on page 582.

Overview

In this example, you configure a routing policy called policy1 and a corresponding routing term called term1. Within the term, you configure the route filter to include source routes greater than or equal to 10.210.0.0/16 and destination routes greater than or equal to 10.215.0.0/16. Then you group the source and destination prefixes into a forwarding class called forwarding-class1 and apply policy1 to the forwarding table. The routing policy is evaluated when routes are being exported from the routing table into the forwarding table. Only the active routes are exported from the routing table.

Configuration

To quickly group source and destination prefixes in a forwarding class, copy the following commands and paste them into the CLI.

```
[edit]
set policy-options policy-statement policy1 term term1 from route-filter
    10.210.0.0/16 orlonger
set policy-options policy-statement policy1 term term1 from route-filter
    10.215.0.0/16 orlonger
set policy-options policy-statement policy1 term term1 then forwarding-class
    forwarding-class1
set routing-options forwarding-table export policy1
```
**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see Using the CLI Editor in Configuration Mode.

To group source and destination prefixes in a forwarding class:

1. Create the routing policy.
   
   ```
   [edit]
   user@host# edit policy-options policy-statement policy1
   ```

2. Create the routing term.
   
   ```
   [edit policy-options policy-statement policy1]
   user@host# edit term term1
   ```

3. Specify the source routes to include in the route filter.
   
   ```
   [edit policy-options policy-statement policy1 term term1]
   user@host# set from route-filter 10.210.0.0/16 orlonger
   ```

4. Specify the destination routes to include in the route filter.
   
   ```
   [edit policy-options policy-statement policy1 term term1]
   user@host# set from route-filter 10.215.0.0/16 orlonger
   ```

5. Group the source and destination prefixes into the forwarding class.
   
   ```
   [edit policy-options policy-statement policy1 term term1]
   user@host# set then forwarding-class forwarding-class1
   ```

6. Apply the routing policy to the forwarding table.
   
   ```
   [edit]
   user@host# set routing-options forwarding-table export policy1
   ```

---

**NOTE:** You can refer to the same routing policy one or more times in the same or different export statement.

---

**Results**

Confirm your configuration by entering the `show policy-options` and `show routing-options` commands from configuration mode. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show policy-options
policy-statement policy1 {
  term term1 {
    from {
      route-filter 10.210.0.0/16 orlonger;
      route-filter 10.215.0.0/16 orlonger;
    }
    then forwarding-class forwarding-class1;
  }
}
```
user@host# show routing-options
forwarding-table {
    export policy1;
}

If you are done configuring the device, enter commit from configuration mode.

**Verification**

To confirm that the configuration is working properly, perform these tasks:

- Verifying the Forwarding Class on page 596
- Verifying the Routing Policy on page 596

**Verifying the Forwarding Class**

**Purpose**
Verify that the forwarding table is applied to the routing policy.

**Action**
From operational mode, enter the `show routing-options` command.

**Verifying the Routing Policy**

**Purpose**
Verify that the policy and term are configured on the device with the appropriate routes included in the forwarding class.

**Action**
From operational mode, enter the `show policy-options` command.

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Routing Policies Configuration Overview on page 582
- Understanding Route-Based Match Conditions on page 591
- Example: Rejecting Known Invalid Routes on page 592

**Protocol-Based Match Conditions**

- Understanding Protocol-Based Match Conditions on page 596
- Example: Injecting OSPF Routes into the BGP Routing Table on page 597

**Understanding Protocol-Based Match Conditions**

You can specify a match condition for policies based on protocols by naming a protocol from which the route is learned or to which the route is being advertised. You can specify one of the following protocols: aggregate, BGP, direct, DVMRP, IS-IS, local, OSPF, PIM-dense, PIM-sparse, RIP, or static.
Example: Injecting OSPF Routes into the BGP Routing Table

This example shows you how to create a policy that injects OSPF routes into the BGP routing table.

Requirements
Before you begin, configure router interfaces and configure routing protocols, as explained in “Routing Policies Configuration Overview” on page 582.

Overview
In this example, you create a routing policy called injectpolicy1 and a routing term called injectterm1. The policy injects OSPF routes into the BGP routing table.

Configuration

CLI Quick Configuration
To quickly create a policy that injects OSPF routes into the BGP routing table, copy the following commands and paste them into the CLI.

```
[edit]
set policy-options policy-statement injectpolicy1 term injectterm1 from protocol ospf
set policy-options policy-statement injectpolicy1 term injectterm1 from area 0.0.0.1
set policy-options policy-statement injectpolicy1 term injectterm1 then accept
set policy-options policy-statement test term 1 from protocol direct
set protocols bgp export injectpolicy1
```

Step-by-Step Procedure
The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see Using the CLI Editor in Configuration Mode.

To inject OSPF routes into a BGP routing table:

1. Create the routing policy.

```
[edit]
```
user@host# edit policy-options policy-statement injectpolicy1

2. Create the policy term.
   [edit policy-options policy-statement injectpolicy1]
   user@host# edit term injectterm1

3. Specify OSPF as a match condition.
   [edit policy-options policy-statement injectpolicy1 term injectterm1]
   user@host# set from protocol ospf

4. Specify the routes from an OSPF area as a match condition.
   [edit policy-options policy-statement injectpolicy1 term injectterm1]
   user@host# set from area 1

5. Specify that the route is to be accepted if the previous conditions are matched.
   [edit policy-options policy-statement injectpolicy1 term injectterm1]
   user@host# set then accept

6. Apply the routing policy to BGP.
   [edit]
   user@host# set protocols bgp export injectpolicy1

**Results** Confirm your configuration by entering the `show policy-options` and `show protocols bgp` commands from configuration mode. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show policy-options
policy-statement injectpolicy1 {
    term injectterm1 {
        from {
            protocol ospf;
            area 0.0.0.1;
        }
        then accept;
    }
}
```

user@host# show protocols bgp
export injectpolicy1;

If you are done configuring the device, enter `commit` from configuration mode.

**Verification**

To confirm that the configuration is working properly, perform these tasks:

- Verifying the OSPF-Based Match Conditions on page 599
- Verifying the Routing Policy on page 599
Verifying the OSPF-Based Match Conditions

**Purpose**
Verify that the policy and term are configured on the device with the appropriate OSPF-based match conditions.

**Action**
From operational mode, enter the `show policy-options` command.

Verifying the Routing Policy

**Purpose**
Verify that the routing policy is applied to the routing protocol.

**Action**
From operational mode, enter the `show protocols bgp` command.

**Related Topics**
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Routing Policies Configuration Overview on page 582
- Understanding Protocol-Based Match Conditions on page 596

Autonomous System Path-Based Actions

**Understanding Autonomous System Path-Based Actions**
You can prepend or add one or more autonomous system (AS) numbers at the beginning of an AS path. The AS numbers are added after the local AS number has been added to the path. Prepending an AS path makes a shorter AS path look longer and therefore less preferable to the Border Gateway Protocol (BGP).

For example, from AS 1, there are two equal paths (through AS 2 and AS 3) to reach AS 4. You might want packets from certain sources to use the path through AS 2. Therefore, you must make the path through AS 3 look less preferable so that BGP chooses the path through AS 2. In AS 1, you can prepend multiple AS numbers.

**Related Topics**
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- Routing Policies Configuration Overview on page 582
- Understanding Routing Policy Match Conditions and Actions on page 587
- Example: Configuring a Routing Policy to Prepend the AS Path on page 600
Example: Configuring a Routing Policy to Prepend the AS Path

This example shows how to configure a routing policy to prepend the AS path.

- Requirements on page 600
- Overview on page 600
- Configuration on page 600
- Verification on page 602

Requirements

Before you begin, configure router interfaces and configure routing protocols, as explained in “Routing Policies Configuration Overview” on page 582.

Overview

In this example, you create a routing policy called prependpolicy1 and a term called prependterm1. The routing policy prepends the AS numbers 1 1 1 1 to routes that are greater than or equal to 172.16.0.0/12, 192.168.0.0/16, and 10.0.0.0/8. The policy is applied as an import policy to all BGP routes and is evaluated when routes are imported to the routing table.

Configuration

CLI Quick Configuration

To quickly group source and destination prefixes in a forwarding class, copy the following commands and paste them into the CLI.

```plaintext
[edit]
set policy-options policy-statement prependpolicy1 term prependterm1 from route-filter 172.16.0.0/12 orlonger
set policy-options policy-statement prependpolicy1 term prependterm1 from route-filter 192.168.0.0/16 orlonger
set policy-options policy-statement prependpolicy1 term prependterm1 from route-filter 10.0.0.0/8 orlonger
set policy-options policy-statement prependpolicy1 term prependterm1 then as-path-prepend "1 1 1 1"
set policy-options policy-statement test term 1 from protocol direct
set protocols bgp import prependpolicy1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see Using the CLI Editor in Configuration Mode.

To create a routing policy that prepends AS numbers to multiple routes:

1. Create the routing policy.

   ```plaintext
   [edit]
   user@host# edit policy-options policy-statement prependpolicy1
   ```
2. Create the routing term.
   
   ```bash
   [edit policy-options policy-statement prependpolicy1]
   user@host# edit term prependterm1
   ```

3. Specify the routes to prepend with AS numbers.
   
   ```bash
   [edit policy-options policy-statement prependpolicy1 term prependterm1]
   user@host# set from route-filter 172.16.0.0/12 orlonger
   user@host# set from route-filter 192.168.0.0/16 orlonger
   user@host# set from route-filter 10.0.0.0/8 orlonger
   ```

4. Specify the AS numbers to prepend.
   
   ```bash
   [edit policy-options policy-statement prependpolicy1 term prependterm1]
   user@host# set then as-path-prepend "1 1 1 1"
   ```

**NOTE:** If you enter multiple numbers, you must separate each number with a space. Enclose the numbers in double quotation marks.

5. Apply the policy as an import policy for all BGP routes.
   
   ```bash
   [edit]
   user@host# set protocols bgp import prependpolicy1
   ```

**NOTE:** You can refer to the same routing policy one or more times in the same or different import statement.

**Results**

Confirm your configuration by entering the `show policy-options` and `show protocols bgp` commands from configuration mode. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```bash
user@host# show policy-options
policy-statement prependpolicy1 {
  term prependterm1 {
    from {
      route-filter 172.16.0.0/12 orlonger;
      route-filter 192.168.0.0/16 orlonger;
      route-filter 10.0.0.0/8 orlonger;
    }
    then as-path-prepend "1 1 1 1";
  }
}

user@host# show protocols bgp
import prependpolicy1;
```

If you are done configuring the device, enter `commit` from configuration mode.
**Verification**

To confirm that the configuration is working properly, perform these tasks:

- Verifying the AS Numbers to Prepend on page 602
- Verifying the Routing Policy on page 602

**Verifying the AS Numbers to Prepend**

**Purpose**
Verify that the policy and term are configured on the device and that the appropriate routes are specified to prepend with AS numbers.

**Action**
From operational mode, enter the `show policy-options` command.

**Verifying the Routing Policy**

**Purpose**
Verify that the routing policy is applied to the routing protocol.

**Action**
From operational mode, enter the `show protocols bgp` command.

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Routing Policies Configuration Overview on page 582
- Understanding Autonomous System Path-Based Actions on page 599

**Routing Policy Damping Parameters**

- Understanding Damping Parameters on page 602
- Example: Configuring Damping Parameters on page 603

**Understanding Damping Parameters**

Flap damping reduces the number of update messages by marking routes as ineligible for selection as the active or preferable route. Marking routes in this way leads to some delay, or suppression, in the propagation of route information, but the result is increased network stability. You typically apply flap damping to external BGP (EBGP) routes (routes in different ASs). You can also apply flap damping within a confederation, between confederation member ASs. Because routing consistency within an AS is important, do not apply flap damping to internal BGP (IBGP) routes. (If you do, it is ignored.)

You can specify one or more of the damping parameters described in Table 159 on page 603. If you do not specify a damping parameter, the default value of the parameter is used.
Table 159: Damping Parameters

<table>
<thead>
<tr>
<th>Damping Parameter</th>
<th>Description</th>
<th>Default Value</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>half-life minutes</td>
<td>Decay half-life—Number of minutes after which an arbitrary value is halved if a route stays stable.</td>
<td>15 (minutes)</td>
<td>1 through 4</td>
</tr>
<tr>
<td>max-suppress minutes</td>
<td>Maximum hold-down time for a route, in minutes.</td>
<td>60 (minutes)</td>
<td>1 through 720</td>
</tr>
<tr>
<td>reuse</td>
<td>Reuse threshold—Arbitrary value below which a suppressed route can be used again.</td>
<td>750</td>
<td>1 through 20,000</td>
</tr>
<tr>
<td>suppress</td>
<td>Cutoff (suppression) threshold—Arbitrary value above which a route can no longer be used or included in advertisements.</td>
<td>3000</td>
<td>1 through 20,000</td>
</tr>
</tbody>
</table>

To change the default BGP flap damping values, you define actions by creating a named set of damping parameters and including it in a routing policy with the damping action. For the damping routing policy to work, you also must enable BGP route flap damping.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Routing Policies Overview on page 581
- Example: Configuring Damping Parameters on page 603

Example: Configuring Damping Parameters

This example shows how to configure damping parameters.

- Requirements on page 603
- Overview on page 603
- Configuration on page 604
- Verification on page 606

Requirements

Before you begin, configure router interfaces and configure routing protocols, as explained in “Routing Policies Configuration Overview” on page 582.

Overview

In this example, you configure a routing policy called policy1 and a corresponding routing term called term1. Within the term, you configure the route filter to include source routes greater than or equal to 10.210.0.0/16 and destination routes greater than or equal to 10.215.0.0/16. Then you group the source and destination prefixes into a forwarding class called forwarding-class1 and apply policy1 to the forwarding table. The routing policy is evaluated when routes are being exported from the routing...
table into the forwarding table. Only the active routes are exported from the routing table.

**Configuration**

**CLI Quick Configuration**

To quickly group source and destination prefixes in a forwarding class, copy the following commands and paste them into the CLI.

```plaintext
[edit]
set policy-options policy-statement dampenpolicy1 term dampenterm1 from route-filter 172.16.0.0/12 orlonger damping group1
set policy-options policy-statement dampenpolicy1 term dampenterm1 from route-filter 192.168.0.0/16 orlonger
set policy-options policy-statement dampenpolicy1 term dampenterm1 from route-filter 10.0.0.0/8 orlonger
set policy-options policy-statement test term 1 from protocol direct
set policy-options damping group1 half-life 30 set policy-options damping group1 reuse 750
set policy-options damping group1 suppress 3000
set policy-options damping group1 max-suppress 60
set policy-options damping group2 half-life 40
set policy-options damping group2 reuse 1000
set policy-options damping group2 suppress 400
set policy-options damping group2 max-suppress 45
set policy-options damping group3 disable
set protocols bgp damping
set protocols bgp group groupA neighbor 172.16.15.14 import dampenpolicy1
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see Using the CLI Editor in Configuration Mode.

To configure damping parameters:

1. Create the routing policy.
   
   ```plaintext
   [edit]
   user@host# edit policy-options policy-statement dampenpolicy1
   ```

2. Create the routing term.
   
   ```plaintext
   [edit policy-options policy-statement policy-statement dampenpolicy1]
   user@host# edit term dampenterm1
   ```

3. Specify the routes to dampen and associate each group of routes with a group name.
   
   ```plaintext
   [edit policy-options policy-statement dampenpolicy1 term dampenterm1]
   user@host# set from route-filter 172.16.0.0/12 orlonger damping group1
   user@host# set from route-filter 192.168.0.0/16 orlonger
   user@host# set from route-filter 10.0.0.0/8 orlonger
   ```

4. Create and configure the damping parameter groups.
   
   ```plaintext
   [edit policy-options damping]
   ```
user@host# set group1 half-life 30 max-suppress 60 reuse 750 suppress 3000
user@host# set group2 half-life 40 max-suppress 45 reuse 1000 suppress 400
user@host# set group3 disable

5. Enable damping for BGP.

[edit]
user@host# set protocols bgp damping

6. Apply the policy as an import policy for the BGP neighbor.

[edit]
user@host# set protocols bgp groupA neighbor 172.16.15.14 import dampenpolicy1

**NOTE:** You can refer to the same routing policy one or more times in the same or different import statement.

---

**Results** Confirm your configuration by entering the `show policy-options` and `show protocols bgp` commands from configuration mode. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

user@host# show policy-options
policy-statement dampenpolicy1 {
  term dampenterm1 {
    from {
      route-filter 172.16.0.0/12 orlonger damping group1;
      route-filter 192.168.0.0/16 orlonger;
      route-filter 10.0.0.0/8 orlonger;
    }
  }
}
damping group1 {
  half-life 30;
  reuse 750;
  suppress 3000;
  max-suppress 60;
}
damping group2 {
  half-life 40;
  reuse 1000;
  suppress 400;
  max-suppress 45;
}
damping group3 {
  disable;
}

user@host# show protocols bgp
damping;
group groupA {
neighbor 172.16.15.14 {
    import dampenpolicy1;
}

If you are done configuring the device, enter commit from configuration mode.

**Verification**

To confirm that the configuration is working properly, perform these tasks:
- Verifying the Damping Parameters on page 606
- Verifying the Routing Policy on page 606

**Verifying the Damping Parameters**

**Purpose**
Verify that the policy and term are configured on the device and that the appropriate damping parameters are specified within the term.

**Action**
From operational mode, enter the `show policy-options` command.

**Verifying the Routing Policy**

**Purpose**
Verify that damping is enabled for BGP and that the routing policy is applied to the routing protocol.

**Action**
From operational mode, enter the `show protocols bgp` command.

**Related Topics**
- JUNOS Software Interfaces and Routing Configuration Guide
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Routing Policies Configuration Overview on page 582
- Understanding Damping Parameters on page 602
Chapter 24

Stateless Firewall Filters

- Stateless Firewall Filter Overview on page 607
- Stateless Firewall Filter Configuration Overview on page 608
- Stateless Firewall Filter Terms on page 609
- Trusted Source Stateless Firewall Filters on page 618
- Flood Prevention Stateless Firewall Filters on page 623
- Fragment Handling Stateless Firewall Filters on page 631

Stateless Firewall Filter Overview

A *stateless firewall filter* evaluates the contents of packets transiting the device from a source to a destination, or packets originating from, or destined for, the Routing Engine. Stateless firewall filters applied to the Routing Engine interface protect the processes and resources owned by the Routing Engine. A stateless firewall filter evaluates every packet, including fragmented packets.

The primary goal of a typical stateless firewall filter is to protect the Routing Engine processes and resources from malicious or untrusted packets. You can configure a firewall filter to do the following:

- Restrict traffic destined for the Routing Engine based on its source, protocol, and application.
- Limit the traffic rate of packets destined for the Routing Engine to protect against flood, or denial-of-service (DoS), attacks.
- Address special circumstances associated with fragmented packets destined for the Routing Engine. Because the device evaluates every packet against a firewall filter (including fragments), you must configure the filter to accommodate fragments that do not contain packet header information. Otherwise, the filter discards all but the first fragment of a fragmented packet.

You can apply a stateless firewall filter to an input or output interface, or to both. Every packet, including fragmented packets, is evaluated against stateless firewall filters.
NOTE: A stateless firewall filter, often called a firewall filter or access control list (ACL), statically evaluates packet contents. In contrast, a stateful firewall filter, or stateful firewall policy, uses connection state information derived from past communications and other applications to make dynamic control decisions.

### Related Topics
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- SRX Series Services Gateways Processing Overview in the *Junos OS Security Configuration Guide*
- Understanding Stateful and Stateless Data Processing for J Series Services Routers in the *Junos OS Security Configuration Guide*
- Security Policies Overview in the *Junos OS Security Configuration Guide*
- Firewall Filter Overview in the *Junos Policy Framework Configuration Guide*
- Firewall Filter Components in the *Junos Policy Framework Configuration Guide*

### Stateless Firewall Filter Configuration Overview

Before you create a stateless firewall filter, determine your objectives:

- **Purpose of the firewall filter**—For example, the purpose might be to limit traffic to certain protocols, IP source or destination addresses, or data rates, or to prevent denial-of-service (DoS) attacks.

- **Appropriate packet header fields to match**—For example, you might want to match IP header fields (such as source and destination IP addresses, protocols, and IP options), TCP header fields (such as source and destination ports and flags), or ICMP header fields (such as ICMP packet type and code).

- **Action to take if a match occurs**—For example, you might want to accept, discard, or evaluate the next term.

- **(Optional) Action modifiers (additional actions to take if a packet matches)**—For example, you might want to count, log, rate limit, or police a packet.

- **Interface on which the firewall filter is applied**—For example, you might want the input or output side, or both sides, of the Routing Engine interface or a non-Routing Engine interface.

To create the firewall filter:

1. Create and configure the filter. (Unlike a stateful firewall filter, you can configure a stateless firewall filter before configuring the interfaces on which the filter is applied.) See:
   - Example: Configuring a Stateless Firewall Filter to Accept Traffic From Trusted Sources on page 618
   - Example: Configuring a Stateless Firewall Filter to Protect Against TCP and ICMP Floods on page 624
Example: Configuring a Stateless Firewall Filter to Handle Fragments on page 632

- Configuring Firewall Filters in the Junos Policy Framework Configuration Guide
- Configuring Standard Firewall Filters in the Junos Policy Framework Configuration Guide

2. Apply the filter to an interface. You can apply a stateless firewall to the input or output sides, or both, of an interface.

- To filter packets transiting the device, apply the firewall filter to any non-Routing Engine interface.
- To filter packets originating from, or destined for, the Routing Engine, apply the firewall filter to the loopback (lo0) interface.

See Applying Firewall Filters to Interfaces in the Junos Policy Framework Configuration Guide.

**CAUTION:** If a packet does not match any terms in a firewall filter rule, the packet is discarded. Avoid configuring a stateless firewall filter that prevents you from accessing the device after you commit the configuration. For example, if you configure a firewall filter that does not match HTTP or HTTPS packets, you cannot access the device with the J-Web interface.

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices

### Stateless Firewall Filter Terms

- Understanding Stateless Firewall Filter Terms on page 609
- Stateless Firewall Filter Match Conditions on page 610
- Stateless Firewall Filter Actions and Action Modifiers on page 615

#### Understanding Stateless Firewall Filter Terms

All stateless firewall filters contain one or more terms, and each term consists of two components—match conditions and actions. The match conditions define the values or fields that the packet must contain to be considered a match. If a packet is a match, the corresponding action is taken. By default, a packet that does not match a firewall filter is discarded.

**NOTE:** A firewall filter with a large number of terms can adversely affect both the configuration commit time and the performance of the Routing Engine.
Additionally, you can configure a stateless firewall filter within the term of another filter. This method enables you to add common terms to multiple filters without having to modify all filter definitions. You can configure one filter with the desired common terms, and configure this filter as a term in other filters. Consequently, to make a change in these common terms, you need to modify only one filter that contains the common terms, instead of multiple filters.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- How Firewall Filters Are Evaluated in the Junos Policy Framework Configuration Guide
- Configuring Nested Firewall Filters in the Junos Policy Framework Configuration Guide

Stateless Firewall Filter Match Conditions

Table 160 on page 610 and Table 161 on page 613 list the match conditions you can specify in stateless firewall filter terms.

NOTE: When the device compares the stateless firewall filter match conditions to a packet, it compares only the header fields specified in the match condition. There is no implied protocol match. For example, if you specify a match of destination-port ssh, the device checks for a value of 0x22 in the 2-byte field that is two bytes after the IP packet header. The protocol field of the packet is not checked.

Table 160: IPv4 Stateless Firewall Filter Match Conditions

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Numeric Range Match Conditions</td>
<td></td>
</tr>
<tr>
<td>keyword-except</td>
<td>Negates a match—for example, destination-port-except number.</td>
</tr>
<tr>
<td></td>
<td>The following keywords accept the -except extension: destination-port, dscp, esp-spi, forwarding-class, fragment-offset, icmp-code, icmp-type, interface-group, ip-options, packet-length, port, precedence, protocol, and source-port.</td>
</tr>
<tr>
<td>destination-port number</td>
<td>Matches a TCP or UDP destination port field. You cannot specify both the port and destination-port match conditions in the same term. Normally, you specify this match in conjunction with the protocol tcp or protocol udp match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify a text synonym. For example, you can specify telnet or 23.</td>
</tr>
<tr>
<td>esp-spi spi-value</td>
<td>Matches an IPsec ESP SPI value. Match on this specific SPI value. You can specify the ESP SPI value in hexadecimal, binary, or decimal form.</td>
</tr>
<tr>
<td>forwarding-class class</td>
<td>Matches a forwarding class. Specify assured-forwarding, best-effort, expedited-forwarding, or network-control.</td>
</tr>
</tbody>
</table>
### Table 160: IPv4 Stateless Firewall Filter Match Conditions (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fragment-offset number</td>
<td>Matches the fragment offset field.</td>
</tr>
<tr>
<td>icmp-code number</td>
<td>Matches the ICMP code field. Normally, you specify this match condition in conjunction with the <code>protocol icmp</code> match statement to determine which protocol is being used on the port. This value or keyword provides more specific information than <code>icmp-type</code>. Because the value's meaning depends on the associated <code>icmp-type</code>, you must specify <code>icmp-type</code> along with <code>icmp-code</code>. In place of the numeric value, you can specify a text synonym. For example, you can specify <code>ip-header-bad</code> or 0.</td>
</tr>
<tr>
<td>icmp-type number</td>
<td>Matches the ICMP packet type field. Normally, you specify this match condition in conjunction with the <code>protocol icmp</code> match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify a text synonym. For example, you can specify <code>time-exceeded</code> or 11.</td>
</tr>
<tr>
<td>interface-group group-number</td>
<td>Matches the interface group on which the packet was received. An interface group is a set of one or more logical interfaces.</td>
</tr>
<tr>
<td>packet-length bytes</td>
<td>Matches the length of the received packet, in bytes. The length refers only to the IP packet, including the packet header, and does not include any Layer 2 encapsulation overhead.</td>
</tr>
<tr>
<td>port number</td>
<td>Matches a TCP or UDP source or destination port field. You cannot specify both the <code>port</code> match and either the <code>destination-port</code> or <code>source-port</code> match conditions in the same term. Normally, you specify this match condition in conjunction with the <code>protocol tcp</code> or <code>protocol udp</code> match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify a text synonym. For example, you can specify <code>bgp</code> or 179.</td>
</tr>
<tr>
<td>precedence ip-precedence-field</td>
<td>Matches the IP precedence field. You can specify precedence in hexadecimal, binary, or decimal form. In place of the numeric value, you can specify <code>immediate</code> or 0x40.</td>
</tr>
<tr>
<td>protocol number</td>
<td>Matches the IP protocol field. In place of the numeric value, you can specify a text synonym. For example, you can specify <code>ospf</code> or 89.</td>
</tr>
<tr>
<td>source-port number</td>
<td>Matches the TCP or UDP source port field. You cannot specify the <code>port</code> and <code>source-port</code> match conditions in the same term. Normally, you specify this match condition in conjunction with the <code>protocol tcp</code> or <code>protocol udp</code> match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify a text synonym. For example, you can specify <code>http</code> or 80.</td>
</tr>
</tbody>
</table>

**Address Match Conditions**
### Table 160: IPv4 Stateless Firewall Filter Match Conditions (continued)

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address prefix</td>
<td>Matches the IP source or destination address field. You cannot specify both the address and the destination-address or source-address match conditions in the same term.</td>
</tr>
<tr>
<td>destination-address prefix</td>
<td>Matches the IP destination address field. You cannot specify the destination-address and address match conditions in the same term.</td>
</tr>
<tr>
<td>destination-prefix-list prefix-list</td>
<td>Matches the IP destination prefix list field. You cannot specify the destination-prefix-list and prefix-list match conditions in the same term.</td>
</tr>
<tr>
<td>prefix-list prefix-list</td>
<td>Matches the IP source or destination prefix list field. You cannot specify both the prefix-list and the destination-prefix-list or source-prefix-list match conditions in the same term.</td>
</tr>
<tr>
<td>source-address prefix</td>
<td>Matches the IP source address field. You cannot specify the source-address and address match conditions in the same rule.</td>
</tr>
<tr>
<td>source-prefix-list prefix-list</td>
<td>Matches the IP source prefix list field. You cannot specify the source-prefix-list and prefix-list match conditions in the same term.</td>
</tr>
</tbody>
</table>

**Bit-Field Match Conditions with Values**

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fragment-flags number</td>
<td>Matches an IP fragmentation flag. In place of the numeric value, you can specify a text synonym. For example, you can specify more-fragments or 0x2000.</td>
</tr>
<tr>
<td>ip-options number</td>
<td>Matches an IP option. In place of the numeric value, you can specify a text synonym. For example, you can specify recordroute or 7.</td>
</tr>
<tr>
<td>tcp-flags number</td>
<td>Matches a TCP flag. Normally, you specify this match condition in conjunction with the protocol tcp match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify a text synonym. For example, you can specify syn or 0x02.</td>
</tr>
</tbody>
</table>

**Bit-Field Text Synonym Match Conditions**

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>first-fragment</td>
<td>Matches the first fragment of a fragmented packet. This condition does not match unfragmented packets.</td>
</tr>
<tr>
<td>is-fragment</td>
<td>Matches the trailing fragment of a fragmented packet. It does not match the first fragment of a fragmented packet. To match both first and trailing fragments, you can use two terms, or you can use fragment-offset 0-8191.</td>
</tr>
<tr>
<td>tcp-established</td>
<td>Matches a TCP packet other than the first packet of a connection. This match condition is a synonym for &quot;(ack</td>
</tr>
<tr>
<td>tcp-initial</td>
<td>Matches the first TCP packet of a connection. This match condition is a synonym for &quot;(syn &amp; lack)&quot;. This condition does not implicitly check that the protocol is TCP. To do so, specify the protocol tcp match condition.</td>
</tr>
</tbody>
</table>
### Table 161: IPv6 Stateless Firewall Filter Match Conditions

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Numeric Range Match Conditions</strong></td>
<td></td>
</tr>
<tr>
<td><em>keyword</em>-except</td>
<td>Negates a match—for example, destination-port-except <em>number</em>.</td>
</tr>
<tr>
<td></td>
<td>The following keywords accept the <em>-except</em> extension: destination-port, dscp, esp-spi, forwarding-class, fragment-offset, icmp-code, icmp-type, interface-group, ip-options, packet-length, port, precedence, protocol, and source-port.</td>
</tr>
<tr>
<td>destination-port <em>number</em></td>
<td>Matches a TCP or UDP destination port field. You cannot specify both the <em>port</em> and <code>destination-port</code> match conditions in the same term. Normally, you specify this match in conjunction with the <code>protocol tcp</code> or <code>protocol udp</code> match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify a text synonym. For example, you can specify <code>telnet</code> or <code>23</code>.</td>
</tr>
<tr>
<td>source-port <em>number</em></td>
<td>Matches the TCP or UDP source port field. You cannot specify the <em>port</em> and <code>source-port</code> match conditions in the same term. Normally, you specify this match condition in conjunction with the <code>protocol tcp</code> or <code>protocol udp</code> match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify a text synonym. For example, you can specify <code>http</code> or <code>80</code>.</td>
</tr>
<tr>
<td>forwarding-class <em>class</em></td>
<td>Matches a forwarding class. Specify <code>assured-forwarding</code>, <code>best-effort</code>, <code>expedited-forwarding</code>, or <code>network-control</code>.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td></td>
</tr>
<tr>
<td>icmp-code <em>number</em></td>
<td>Matches the ICMP code field. Normally, you specify this match condition in conjunction with the <code>protocol icmp</code> match statement to determine which protocol is being used on the port. This value or keyword provides more specific information than <code>icmp-type</code>. Because the value's meaning depends on the associated <code>icmp-type</code>, you must specify <code>icmp-type</code> along with <code>icmp-code</code>. In place of the numeric value, you can specify <code>ip-header-bad</code> or <code>0</code>.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>Applies to SRX100, SRX210, SRX240, and SRX650 devices only.</td>
</tr>
<tr>
<td>icmp-type <em>number</em></td>
<td>Matches the ICMP packet type field. Normally, you specify this match condition in conjunction with the <code>protocol icmp</code> match statement to determine which protocol is being used on the port. In place of the numeric value, you can specify a text synonym. For example, you can specify <code>time-exceeded</code> or <code>11</code>.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>Applies to SRX100, SRX210, SRX240, and SRX650 devices only.</td>
</tr>
<tr>
<td>interface-group <em>group-number</em></td>
<td>Matches the interface group on which the packet was received. An interface group is a set of one or more logical interfaces.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>Applies to SRX100, SRX210, SRX240, and SRX650 devices only.</td>
</tr>
</tbody>
</table>
Table 161: IPv6 Stateless Firewall Filter Match Conditions *(continued)*

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>packet-length bytes</td>
<td>Matches the length of the received packet, in bytes. The length refers only to the IP packet, including the packet header, and does not include any Layer 2 encapsulation overhead.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>Applies to SRX100, SRX210, SRX240, and SRX650 devices only.</td>
</tr>
<tr>
<td>port number</td>
<td>Matches a TCP or UDP source or destination port field. You cannot specify both the port match and either the destination-port or source-port match conditions in the same term. Normally, you specify this match condition in conjunction with the protocol tcp or protocol udp match statement to determine which protocol is being used on the port.</td>
</tr>
<tr>
<td></td>
<td>In place of the numeric value, you can specify a text synonym. For example, you can specify bgp or 179.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>Applies to SRX100, SRX210, SRX240, and SRX650 devices only.</td>
</tr>
</tbody>
</table>

Address Match Conditions

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination-address prefix</td>
<td>Matches the IP destination address field. You cannot specify the destination-address and address match conditions in the same term.</td>
</tr>
<tr>
<td>source-address prefix</td>
<td>Matches the IP source address field. You cannot specify the source-address and address match conditions in the same rule.</td>
</tr>
</tbody>
</table>

Bit-Field Match Conditions with Values

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp-flags number</td>
<td>Matches a TCP flag. Normally, you specify this match condition in conjunction with the protocol tcp match statement to determine which protocol is being used on the port.</td>
</tr>
<tr>
<td></td>
<td>In place of the numeric value, you can specify a text synonym. For example, you can specify syn or 0x02.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>Applies to SRX100, SRX210, SRX240, and SRX650 devices only.</td>
</tr>
</tbody>
</table>

Bit-Field Text Synonym Match Conditions

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp-established</td>
<td>Matches a TCP packet other than the first packet of a connection. This match condition is a synonym for &quot;(ack</td>
</tr>
<tr>
<td></td>
<td>This condition does not implicitly check that the protocol is TCP. To do so, specify the protocol tcp match condition.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>Applies to SRX100, SRX210, SRX240, and SRX650 devices only.</td>
</tr>
<tr>
<td>tcp-initial</td>
<td>Matches the first TCP packet of a connection. This match condition is a synonym for &quot;(syn &amp; lack)&quot;.</td>
</tr>
<tr>
<td></td>
<td>This condition does not implicitly check that the protocol is TCP. To do so, specify the protocol tcp match condition.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>Applies to SRX100, SRX210, SRX240, and SRX650 devices only.</td>
</tr>
</tbody>
</table>
To specify a bit-field match condition with values, such as `tcp-flags`, you must enclose the values in quotation marks (" "). You can use bit-field logical operators to create expressions that are evaluated for matches. For example, if the following expression is used in a filter term, a match occurs if the packet is the initial packet of a TCP session:

```
tcp-flags "syn & !ack"
```

You can use text synonyms to specify some common bit-field matches. In the previous example, you can specify `tcp-initial` as the same match condition.

**NOTE:**

Some of the numeric range and bit-field match conditions allow you to specify a text synonym. For a complete list of synonyms:

- If you are using the J-Web interface, select the synonym from the appropriate list.
- If you are using the CLI, type a question mark (?) after the from statement.

Table 162 on page 615 lists the bit-field logical operators in order of highest to lowest precedence.

### Table 162: Stateless Firewall Filter Bit-Field Logical Operators

<table>
<thead>
<tr>
<th>Logical Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(...)</td>
<td>Grouping</td>
</tr>
<tr>
<td>!</td>
<td>Negation</td>
</tr>
<tr>
<td>&amp; or +</td>
<td>Logical AND</td>
</tr>
<tr>
<td></td>
<td>or ,</td>
</tr>
</tbody>
</table>

**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Configuring IPv4 Match Conditions in the Junos Policy Framework Configuration Guide
- Configuring IPv6 Match Conditions in the Junos Policy Framework Configuration Guide
- How to Specify Firewall Filter Match Conditions in the Junos Policy Framework Configuration Guide

**Stateless Firewall Filter Actions and Action Modifiers**

Table 163 on page 616 and Table 164 on page 616 list the actions and action modifiers you can specify in stateless firewall filter terms.
### Table 163: IPv4 Stateless Firewall Filter Actions and Action Modifiers

<table>
<thead>
<tr>
<th>Action or Action Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept</td>
<td>Accepts a packet. This is the default if the packet matches. However, we strongly recommend that you always explicitly configure an action in the <code>then</code> statement.</td>
</tr>
<tr>
<td>discard</td>
<td>Discards a packet silently, without sending an ICMP message. Packets are available for logging and sampling before being discarded.</td>
</tr>
<tr>
<td>next term</td>
<td>Continues to the next term for evaluation.</td>
</tr>
<tr>
<td>reject message-type</td>
<td>Discards a packet, sending an ICMP destination unreachable message. Rejected packets are available for logging and sampling. You can specify one of the following message types: administratively-prohibited (default), bad-host-tos, bad-network-tos, host-prohibited, host-unknown, host-unreachable, network-prohibited, network-unknown, network-unreachable, port-unreachable, precedence-cutoff, precedence-violation, protocol-unreachable, source-host-isolated, source-route-failed, or tcp-reset. If you specify tcp-reset, a TCP reset is returned (indicating the end of a TCP flow), if the packet is a TCP packet. Otherwise, nothing is returned.</td>
</tr>
<tr>
<td>routing-instance</td>
<td>Routes the packet using the specified routing instance.</td>
</tr>
<tr>
<td>count counter-name</td>
<td>Counts the number of packets passing this term. The name can contain letters, numbers, and hyphens (-), and can be up to 24 characters long. A counter name is specific to the filter that uses it, so all interfaces that use the same filter increment the same counter.</td>
</tr>
<tr>
<td>forwarding-class class-name</td>
<td>Classifies the packet to the specified forwarding class.</td>
</tr>
<tr>
<td>log</td>
<td>Logs the packet's header information in the Routing Engine. You can access this information by entering the CLI <code>show firewall log</code> command.</td>
</tr>
<tr>
<td>loss-priority priority</td>
<td>Sets the scheduling priority of the packet. The priority can be low or high.</td>
</tr>
<tr>
<td>packet-mode</td>
<td>Updates a bit field in the packet key buffer, which specifies traffic that will bypass flow-based forwarding. Packets with the <code>packet-mode</code> action modifier follow the packet-based forwarding path and bypass flow-based forwarding completely. For more information about selective stateless packet-based services, see the <a href="#">JUNOS Software Administration Guide</a>.</td>
</tr>
<tr>
<td>policer policer-name</td>
<td>Applies rate limits to the traffic using the named policer.</td>
</tr>
<tr>
<td>sample</td>
<td>Samples the traffic on the interface. Use this modifier only when traffic sampling is enabled. See the <a href="#">JUNOS Policy Framework Configuration Guide</a>.</td>
</tr>
<tr>
<td>syslog</td>
<td>Records information in the system logging facility. This action can be used in conjunction with all options except <code>discard</code>.</td>
</tr>
</tbody>
</table>

### Table 164: IPv6 Stateless Firewall Filter Actions and Action Modifiers

<table>
<thead>
<tr>
<th>Action or Action Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept</td>
<td>Accepts a packet. This is the default if the packet matches. However, we strongly recommend that you always explicitly configure an action in the <code>then</code> statement.</td>
</tr>
</tbody>
</table>
### Table 164: IPV6 Stateless Firewall Filter Actions and Action Modifiers (continued)

<table>
<thead>
<tr>
<th>Action or Action Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>discard</td>
<td>Discards a packet silently, without sending an ICMP message. Packets are available for logging and sampling before being discarded.</td>
</tr>
<tr>
<td>next term</td>
<td>Continues to the next term for evaluation.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Applies to SRX100, SRX210, SRX240, and SRX650 devices only.</td>
</tr>
<tr>
<td>reject message-type</td>
<td>Discards a packet, sending an ICMP destination unreachable message. Rejected packets are available for logging and sampling. You can specify one of the following message types: administratively-prohibited (default), bad-host-tos, bad-network-tos, host-prohibited, host-unknown, host-unreachable, network-prohibited, network-unknown, network-unreachable, port-unreachable, precedence-cutoff, precedence-violation, protocol-unreachable, source-host-isolated, source-route-failed, or tcp-reset. If you specify tcp-reset, a TCP reset is returned (indicating the end of a TCP flow), if the packet is a TCP packet. Otherwise, nothing is returned.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Applies to SRX100, SRX210, SRX240, and SRX650 devices only.</td>
</tr>
<tr>
<td>routing-instance</td>
<td>Routes the packet using the specified routing instance.</td>
</tr>
<tr>
<td></td>
<td>In filter-based forwarding, the IPv6 filter does not identify fragmented IPv6 packets and does not forward them to routing instances other than those used by normal packets.</td>
</tr>
<tr>
<td>count counter-name</td>
<td>Counts the number of packets passing this term. The name can contain letters, numbers, and hyphens (-), and can be up to 24 characters long. A counter name is specific to the filter that uses it, so all interfaces that use the same filter increment the same counter.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Applies to SRX100, SRX210, SRX240, and SRX650 devices only.</td>
</tr>
<tr>
<td>loss-priority priority</td>
<td>Sets the scheduling priority of the packet. The priority can be low, high, medium high, or medium low.</td>
</tr>
<tr>
<td>log</td>
<td>Logs the packet’s header information in the Routing Engine. You can access this information by entering the CLI <code>show firewall log</code> command.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Applies to SRX100, SRX210, SRX240, and SRX650 devices only.</td>
</tr>
<tr>
<td>forwarding-class class-name</td>
<td>Classifies the packet to the specified forwarding class.</td>
</tr>
<tr>
<td>policer policer-name</td>
<td>Applies rate limits to the traffic using the named policer.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Applies to SRX100, SRX210, SRX240, and SRX650 devices only.</td>
</tr>
<tr>
<td>syslog</td>
<td>Records information in the system-logging facility. This action can be used in conjunction with all options except discard.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Applies to SRX100, SRX210, SRX240, and SRX650 devices only.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Configuring Actions in Firewall Filter Terms in the Junos Policy Framework Configuration Guide
Trusted Source Stateless Firewall Filters

- Understanding Trusted Source Stateless Firewall Filters on page 618
- Example: Configuring a Stateless Firewall Filter to Accept Traffic from Trusted Sources on page 618

Understanding Trusted Source Stateless Firewall Filters

You can create a stateless firewall filter that specifies which protocols and services, or applications, are allowed to reach the Routing Engine. Applying this type of filter ensures that packets are from a trusted source and protects the processes running on the Routing Engine from an external attack.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Example: Blocking Telnet and SSH Access in the Junos Policy Framework Configuration Guide
- Example: Blocking TFTP Access in the Junos Policy Framework Configuration Guide
- Example: Accepting OSPF Packets from Certain Addresses in the Junos Policy Framework Configuration Guide
- Example: Accepting DHCP Packets with Specific Addresses in the Junos Policy Framework Configuration Guide

Example: Configuring a Stateless Firewall Filter to Accept Traffic from Trusted Sources

This example shows how to create a stateless firewall filter that protects the Routing Engine from traffic originating from untrusted sources.

- Requirements on page 618
- Overview on page 619
- Configuration on page 619
- Verification on page 621

Requirements

No special configuration beyond device initialization is required before configuring stateless firewall filters.
Overview

In this example, you create a stateless firewall filter called protect-RE that discards all traffic destined for the Routing Engine except SSH and BGP protocol packets from specified trusted sources. This example includes the following firewall filter terms:

- **ssh-term**—Accepts TCP packets with a source address of 192.168.122.0/24 and a destination port that specifies SSH.
- **bgp-term**—Accepts TCP packets with a source address of 10.2.1.0/24 and a destination port that specifies BGP.
- **discard-rest-term**—For all packets that are not accepted by ssh-term or bgp-term, creates a firewall filter log and system logging records, then discards all packets.

**NOTE:** You can move terms within the firewall filter using the insert command. See insert in the Junos CLI User Guide.

Configuration

**CLI Quick Configuration**

To quickly configure the stateless firewall filter, copy the following commands and paste them into the CLI.

```
[edit]
user@host# edit firewall family inet filter protect-RE
```

```
set firewall family inet filter protect-RE term ssh-term from source-address 192.168.122.0/24
set firewall family inet filter protect-RE term ssh-term from protocol tcp
set firewall family inet filter protect-RE term ssh-term from destination-port ssh
set firewall family inet filter protect-RE term ssh-term then accept
set firewall family inet filter protect-RE term bgp-term from source-address 10.2.1.0/24
set firewall family inet filter protect-RE term bgp-term from protocol tcp
set firewall family inet filter protect-RE term bgp-term from destination-port bgp
set firewall family inet filter protect-RE term bgp-term then accept
set firewall family inet filter protect-RE term discard-rest-term then log
set firewall family inet filter protect-RE term discard-rest-term then syslog
set firewall family inet filter protect-RE term discard-rest-term then discard
set interfaces lo0 unit 0 family inet filter input protect-RE
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see Using the CLI Editor in Configuration Mode.

To configure the stateless firewall filter:

1. Create the stateless firewall filter.

```
[edit]
user@host# edit firewall family inet filter protect-RE
```
2. Create the first filter term.
   
   ```
   [edit firewall family inet filter protect-RE]
   user@host# edit term ssh-term
   ```

3. Define the protocol, destination port, and source address match conditions for the term.
   
   ```
   [edit firewall family inet filter protect-RE term ssh-term]
   user@host# set from protocol tcp destination-port ssh source-address 192.168.122.0/24
   ```

4. Define the actions for the term.
   
   ```
   [edit firewall family inet filter protect-RE term ssh-term]
   user@host# set then accept
   ```

5. Create the second filter term.
   
   ```
   [edit firewall family inet filter protect-RE]
   user@host# edit term bgp-term
   ```

6. Define the protocol, destination port, and source address match conditions for the term.
   
   ```
   [edit firewall family inet filter protect-RE term bgp-term]
   user@host# set from protocol tcp destination-port bgp source-address 10.2.1.0/24
   ```

7. Define the action for the term.
   
   ```
   [edit firewall family inet filter protect-RE term bgp-term]
   user@host# set then accept
   ```

8. Create the third filter term.
   
   ```
   [edit firewall family inet filter protect-RE]
   user@host# edit term discard-rest-term
   ```

9. Define the action for the term.
   
   ```
   [edit firewall family inet filter protect-RE term discard-rest]
   user@host# set then log syslog discard
   ```

10. Apply the filter to the input side of the Routing Engine interface.
    
    ```
    [edit]
    user@host# set interfaces lo0 unit 0 family inet filter input protect-RE
    ```

**Results**  Confirm your configuration by entering the `show firewall` command and the `show interfaces lo0` command from configuration mode. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show firewall
family inet {
   filter protect-RE {
      term ssh-term {
```
from {
    source-address {
        192.168.122.0/24;
    }
    protocol tcp;
    destination-port ssh;
}
    then accept;
}
term bgp-term {
    from {
        source-address {
            10.2.1.0/24;
        }
        protocol tcp;
        destination-port bgp;
    }
    then accept;
}
term discard-rest-term {
    then {
        log;
        syslog;
        discard;
    }
}
}

user@host# show interfaces lo0
unit 0 {
    family inet {
        filter {
            input protect-RE;
        }
        address 127.0.0.1/32;
    }
}

If you are done configuring the device, enter commit from configuration mode.

Verification
To confirm that the configuration is working properly, perform these tasks:

- Displaying Stateless Firewall Filter Configurations on page 621
- Verifying a Services, Protocols, and Trusted Sources Firewall Filter on page 622
- Displaying Stateless Firewall Filter Logs on page 622

**Displaying Stateless Firewall Filter Configurations**

**Purpose**  
Verify the configuration of the firewall filter.
**Action** From configuration mode, enter the `show firewall` command and the `show interfaces lo0` command.

**Meaning** Verify that the output shows the intended configuration of the firewall filter. In addition, verify that the terms are listed in the order in which you want the packets to be tested. You can move terms within a firewall filter by using the `insert` CLI command.

---

**Verifying a Services, Protocols, and Trusted Sources Firewall Filter**

**Purpose** Verify that the actions of the firewall filter terms are taken.

**Action** Send packets to the device that match the terms. In addition, verify that the filter actions are not taken for packets that do not match.

- Use the `ssh host-name` command from a host at an IP address that matches `192.168.122.0/24` to verify that you can log in to the device using only SSH from a host with this address prefix.
- Use the `show route summary` command to verify that the routing table on the device does not contain any entries with a protocol other than `Direct`, `Local`, `BGP`, or `Static`.

**Sample Output**

```
% ssh 192.168.249.71
%ssh host
user@host's password:
--- JUNOS 6.4-20040518.0 (JSERIES) #0: 2004-05-18 09:27:50 UTC
user@host>
user@host> show route summary
Router ID: 192.168.249.71
inet.0: 34 destinations, 34 routes (33 active, 0 holddown, 1 hidden)
   Direct:     10 routes,     9 active
   Local:      9 routes,      9 active
   BGP:       10 routes,     10 active
   Static:     5 routes,      5 active
...```

**Meaning** Verify the following information:

- You can successfully log in to the device using SSH.
- The `show route summary` command does not display a protocol other than `Direct`, `Local`, `BGP`, or `Static`.

---

**Displaying Stateless Firewall Filter Logs**

**Purpose** Verify that packets are being logged. If you included the `log` or `syslog` action in a term, verify that packets matching the term are recorded in the firewall log or your system logging facility.
Action

From operational mode, enter the `show firewall log` command.

Sample Output

```plaintext
user@host> show firewall log

Log:

<table>
<thead>
<tr>
<th>Time</th>
<th>Filter</th>
<th>Action</th>
<th>Interface</th>
<th>Protocol</th>
<th>Src Addr</th>
<th>Dest Addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:11:02</td>
<td>pfe</td>
<td>D</td>
<td>ge-0/0/0.0</td>
<td>TCP</td>
<td>172.17.28.19</td>
<td>192.168.70.71</td>
</tr>
<tr>
<td>15:11:01</td>
<td>pfe</td>
<td>D</td>
<td>ge-0/0/0.0</td>
<td>TCP</td>
<td>172.17.28.19</td>
<td>192.168.70.71</td>
</tr>
<tr>
<td>15:11:01</td>
<td>pfe</td>
<td>D</td>
<td>ge-0/0/0.0</td>
<td>TCP</td>
<td>172.17.28.19</td>
<td>192.168.70.71</td>
</tr>
<tr>
<td>15:11:01</td>
<td>pfe</td>
<td>D</td>
<td>ge-0/0/0.0</td>
<td>TCP</td>
<td>172.17.28.19</td>
<td>192.168.70.71</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Meaning

Each record of the output contains information about the logged packet. Verify the following information:

- Under **Time**, the time of day the packet was filtered is shown.
- The **Filter** output is always `pfe`.
- Under **Action**, the configured action of the term matches the action taken on the packet—A (accept), D (discard), R (reject).
- Under **Interface**, the inbound (ingress) interface on which the packet arrived is appropriate for the filter.
- Under **Protocol**, the protocol in the IP header of the packet is appropriate for the filter.
- Under **Src Addr**, the source address in the IP header of the packet is appropriate for the filter.
- Under **Dest Addr**, the destination address in the IP header of the packet is appropriate for the filter.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- show route summary in the Junos Routing Protocols and Policies Command Reference
- show firewall in the Junos Routing Protocols and Policies Command Reference
- show firewall log in the Junos Routing Protocols and Policies Command Reference
- show interfaces (Loopback) in the Junos Interfaces Command Reference

Flood Prevention Stateless Firewall Filters

- Understanding Flood Prevention Stateless Firewall Filters on page 624
- Example: Configuring a Stateless Firewall Filter to Protect Against TCP and ICMP Floods on page 624
Understanding Flood Prevention Stateless Firewall Filters

You can create stateless firewall filters that limit certain TCP and ICMP traffic destined for the Routing Engine. A router without this kind of protection is vulnerable to TCP and ICMP flood attacks—also called denial-of-service (DoS) attacks. For example:

- A TCP flood attack of SYN packets initiating connection requests can overwhelm the device until it can no longer process legitimate connection requests, resulting in denial of service.
- An ICMP flood can overload the device with so many echo requests (ping requests) that it expends all its resources responding and can no longer process valid network traffic, also resulting in denial of service.

Applying the appropriate firewall filters to the Routing Engine protects against these types of attacks.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Example: Blocking TCP Connections to a Certain Port Except from BGP Peers in the Junos Policy Framework Configuration Guide
- Example: Accepting Packets with Specific IPv6 TCP Flags in the Junos Policy Framework Configuration Guide
- Example: Defining a Policer for a Destination Class in the Junos Policy Framework Configuration Guide

Example: Configuring a Stateless Firewall Filter to Protect Against TCP and ICMP Floods

This example shows how to create a stateless firewall filter that protects against TCP and ICMP denial-of-service attacks.

- Requirements on page 624
- Overview on page 625
- Configuration on page 626
- Verification on page 629

Requirements

No special configuration beyond device initialization is required before configuring stateless firewall filters.
Overview

In this example, you create a stateless firewall filter called protect-RE that polices TCP and ICMP packets. This example includes the following policers:

- **tcp-connection-policer**—Limits the traffic rate of the TCP packets to 500,000 bps and the burst size to 15,000 bytes. Packets that exceed the traffic rate are discarded.
- **icmp-policer**—Limits the traffic rate of the ICMP packets to 1,000,000 bps and the burst size to 15,000 bytes. Packets that exceed the traffic rate are discarded.

When specifying limits, the bandwidth limit can be from 32,000 bps to 32,000,000,000 bps and the burst size limit can be from 1,500 bytes through 100,000,000 bytes. Use the following abbreviations when specifying limits: k (1,000), m (1,000,000), and g (1,000,000,000).

Each policer is incorporated into the action of a filter term. This example includes the following terms:

- **tcp-connection-term**—Polices certain TCP packets with a source address of 192.168.122.0/24 or 10.2.1.0/24. These addresses are defined in the trusted-addresses prefix list.
  Policed packets include connection request packets (SYN and ACK flag bits equal 1 and 0), connection release packets (FIN flag bit equals 1), and connection reset packets (RST flag bit equals 1).
- **icmp-term**—Polices echo request packets, echo response packets, unreachable packets, and time-exceeded packets. All of these ICMP packets are counted in the icmp-counter counter.

**NOTE:** You can move terms within the firewall filter using the `insert` command. See `insert` in the *Junos CLI User Guide*.

If you want to include the terms created in this procedure in the protect-RE firewall filter configured in “Example: Configuring a Stateless Firewall Filter to Accept Traffic From Trusted Sources” on page 618, perform the configuration tasks in this example first, then configure the terms as described in “Example: Configuring a Stateless Firewall Filter to Accept Traffic From Trusted Sources” on page 618. This approach ensures that the rate-limiting terms are included as the first two terms in the firewall filter.

**NOTE:** You can move terms within the firewall filter using the `insert` command. See `insert` in the *Junos CLI User Guide*.
Configuration

**CLI Quick Configuration** To quickly configure the stateless firewall filter, copy the following commands and paste them into the CLI.

```
[edit]
set firewall family inet filter protect-RE term tcp-connection-term from source-prefix-list trusted-addresses
set firewall family inet filter protect-RE term tcp-connection-term from protocol tcp
set firewall family inet filter protect-RE term tcp-connection-term from tcp-flags 
"(syn & !ack) | fin | rst"
set firewall family inet filter protect-RE term tcp-connection-term then policer tcp-connection-policer
set firewall family inet filter protect-RE term tcp-connection-term then accept
set firewall family inet filter protect-RE term icmp-term from protocol icmp
set firewall family inet filter protect-RE term icmp-term from icmp-type echo-request
set firewall family inet filter protect-RE term icmp-term from icmp-type echo-reply
set firewall family inet filter protect-RE term icmp-term from icmp-type time-exceeded
set firewall family inet filter protect-RE term icmp-term then policer icmp-policer
set firewall family inet filter protect-RE term icmp-term then count icmp-counter
set firewall family inet filter protect-RE term icmp-term then accept
set firewall policer tcp-connection-policer filter-specific
set firewall policer tcp-connection-policer if-exceeding bandwidth-limit 1m
set firewall policer tcp-connection-policer if-exceeding burst-size-limit 15k
set firewall policer tcp-connection-policer then discard
set firewall policer icmp-policer filter-specific
set firewall policer icmp-policer if-exceeding bandwidth-limit 1m
set firewall policer icmp-policer if-exceeding burst-size-limit 15k
set firewall policer icmp-policer then discard
set policy-options prefix-list trusted-addresses 10.2.1.0/24
set policy-options prefix-list trusted-addresses 192.168.122.0/24
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see Using the CLI Editor in Configuration Mode.

To configure stateless firewall filter policers:

1. Define the first policer.
   ```
   [edit]
   user@host# edit firewall policer tcp-connection-policer
   ```
2. Define the action for the policer.
   ```
   [edit firewall policer tcp-connection-policer]
   user@host# set then discard
   ```
3. Define the rate limits for the policer.
   ```
   [edit firewall policer tcp-connection-policer]
   user@host# set filter-specific if-exceeding burst-size-limit 15k bandwidth-limit 500k
   ```
4. Define the second policer.
   [edit]
   user@host# edit firewall policer imcp-policer

5. Define the action for the policer.
   [edit firewall policer icmp-policer]
   user@host# set then discard

6. Set the rate limits for the policer.
   [edit firewall policer imcp-policer]
   user@host# set filter-specific if-exceeding burst-size-limit 15k
   bandwidth-limit 1m

7. Define the prefix list.
   [edit]
   user@host# set policy-options prefix-list trusted-addresses 192.168.122.0/24
   user@host# set policy-options prefix-list trusted-addresses 10.2.1.0/24

8. Create the stateless firewall filter.
   [edit]
   user@host# edit firewall family inet filter protect-RE

9. Define the first term for the filter.
   [edit firewall family inet filter protect-RE]
   user@host# edit term tcp-connection-term

10. Define the source address match condition for the term.
    [edit firewall family inet filter protect-RE term tcp-connection-term]
    user@host# set from source-prefix-list trusted-addresses

11. Define protocol match conditions for the term.
    [edit firewall family inet filter protect-RE term tcp-connection-term]
    user@host# set from protocol tcp tcp-flags "(syn & !ack) | fin | rst"

12. Define the actions for the term.
    [edit firewall family inet filter protect-RE term tcp-connection-term]
    user@host# set then policer tcp-connection-policer accept

13. Define the second term.
    [edit]
    user@host# edit firewall family inet filter protect-RE term icmp-term

14. Define the protocol for the term.
    [edit firewall family inet filter protect-RE term icmp-term]
    user@host# set from protocol icmp

15. Define the match conditions for the term.
    [edit firewall family inet filter protect-RE term icmp-term]
16. Define the action for the term.

[edit firewall family inet filter protect-RE term icmp-term]
user@host# set then policer icmp-policer count icmp-counter accept

Results  Confirm your configuration by entering the show firewall command and the show policy-options command from configuration mode. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

user@host# show firewall
family inet {
  filter protect-RE {
    term tcp-connection-term {
      from {
        source-prefix-list {
          trusted-addresses;
        }
        protocol tcp;
        tcp-flags "(syn & !ack) | fin | rst";
      } then {
        policer tcp-connection-policer;
        accept;
      }
    }
    term icmp-term {
      from {
        protocol icmp;
        icmp-type [ echo-request echo-reply unreachable time-exceeded ];
      } then {
        policer icmp-policer;
        count icmp-counter;
        accept;
      }
    }
  }
  policer tcp-connection-policer {
    filter-specific;
    if-exceeding {
      bandwidth-limit 1m;
      burst-size-limit 15k;
    } then discard;
  }
  policer icmp-policer {
    filter-specific;
    if-exceeding {
bandwidth-limit 1m;
burst-size-limit 15k;
}
    then discard;
}

user@host# show policy-options
prefix-list trusted-addresses {
    10.2.1.0/24;
    192.168.122.0/24;
}

If you are done configuring the device, enter commit from configuration mode.

**Verification**

To confirm that the configuration is working properly, perform these tasks:

- Displaying Stateless Firewall Filter Configurations on page 629
- Verifying a TCP and ICMP Flood Firewall Filter on page 629
- Displaying Firewall Filter Statistics on page 630

**Displaying Stateless Firewall Filter Configurations**

**Purpose**
Verify the configuration of the firewall filter.

**Action**
From configuration mode, enter the `show firewall` command.

**Meaning**
Verify that the output shows the intended configuration of the firewall filter. In addition, verify that the terms are listed in the order in which you want the packets to be tested. You can move terms within a firewall filter by using the `insert` CLI command.

**Verifying a TCP and ICMP Flood Firewall Filter**

**Purpose**
Verify that the actions of the firewall filter terms are taken.

**Action**
Send packets to the device that match the terms. In addition, verify that the filter actions are not taken for packets that do not match.

- Verify that the device can establish only TCP sessions with a host at an IP address that matches `192.168.122.0/24` or `10.2.1.0/24`. For example, log in to the device with the `telnet host-name` command from another host with one of these address prefixes.
- Use the `ping host-name` command to verify that the device responds only to ICMP packets (such as ping requests) that do not exceed the policer traffic rates.
- Use the `ping host-name size bytes` command to exceed the policer traffic rates by sending ping requests with large data payloads.

**Sample Output**

```
user@host> telnet 192.168.249.71
```

Verification ■ 629
Trying 192.168.249.71...
Connected to host.acme.net.
Escape character is '^]'.

host (ttyp0)
login: user
Password:

--- JUNOS 6.4-20040521.1 built 2004-05-21 09:38:12 UTC

Meaning Verify the following information:
■ You can successfully log in to the device using Telnet.
■ The device sends responses to the ping host command.
■ The device does not send responses to the ping host size 20000 command.

Displaying Firewall Filter Statistics

Purpose Verify that packets are being policed and counted.

Action From operational mode, enter the show firewall filter filter-name command.

Sample Output user@host> show firewall filter protect-RE
Filter: protect-RE
Counters:
  Name             Bytes   Packets
  icmp-counter     1040000  5600
Policers:
  Name           Packets
  tcp-connection-policer  643254873
  icmp-policer        7391

Meaning Verify the following information:
■ Next to Filter, the name of the firewall filter is correct.
■ Under Counters:
Under Name, the names of any counters configured in the firewall filter are correct.

Under Bytes, the number of bytes that match the filter term containing the count counter-name action are shown.

Under Packets, the number of packets that match the filter term containing the count counter-name action are shown.

Under Policers:

Under Name, the names of any policers configured in the firewall filter are correct.

Under Packets, the number of packets that match the conditions specified for the policer are shown.

Related Topics

Junos OS Feature Support Reference for SRX Series and J Series Devices

show firewall in the Junos Routing Protocols and Policies Command Reference

ping in the Junos System Basics and Services Command Reference.

telnet in the Junos System Basics and Services Command Reference.

Fragment Handling Stateless Firewall Filters

Understanding Fragment Handling Stateless Firewall Filters on page 631

Example: Configuring a Stateless Firewall Filter to Handle Fragments on page 632

Example: Configuring a Filter to Match on IPv6 Flags on page 636

Understanding Fragment Handling Stateless Firewall Filters

You can create stateless firewall filters that handle fragmented packets destined for the Routing Engine. By applying these policies to the Routing Engine, you protect against the use of IP fragmentation as a means to disguise TCP packets from a firewall filter.

For example, consider an IP packet that is fragmented into the smallest allowable fragment size of 8 bytes (a 20-byte IP header plus an 8-byte payload). If this IP packet carries a TCP packet, the first fragment (fragment offset of 0) that arrives at the device contains only the TCP source and destination ports (first 4 bytes), and the sequence number (next 4 bytes). The TCP flags, which are contained in the next 8 bytes of the TCP header, arrive in the second fragment (fragment offset of 1).

See RFC 1858, Security Considerations for IP Fragment Filtering.
Example: Configuring a Stateless Firewall Filter to Handle Fragments

This example shows how to create a stateless firewall filter that handles packet fragments.

Requirements on page 632
Overview on page 632
Configuration on page 632
Verification on page 635

Requirements

No special configuration beyond device initialization is required before configuring stateless firewall filters.

Overview

In this example, you create a stateless firewall filter called fragment-RE that handles fragmented packets. This example includes the following firewall filter terms:

- **small-offset-term**—Discards small (1–5) offset packets to ensure that subsequent terms in the firewall filter can be matched against all the headers in the packet. In addition, the term adds a record to the system logging facility.

- **not-fragmented-term**—Accepts unfragmented TCP packets with a source address of 10.2.1.0/24 and a destination port that specifies the BGP protocol. A packet is considered unfragmented if its MF flag and its fragment offset in the TCP header equal 0.

- **first-fragment-term**—Accepts the first fragment of a fragmented TCP packet with a source address of 10.2.1.0/24 and a destination port that specifies the BGP protocol.

- **fragment-term**—Accepts all fragments that were not discarded by small-offset-term. (packet fragments 6–8191). However, only those fragments that are part of a packet containing a first fragment accepted by first-fragment-term are reassembled by the device.

Packet fragments offset can be from 1 through 8191.

NOTE: You can move terms within the firewall filter using the insert command. See insert in the Junos CLI User Guide.

Configuration

**CLI Quick Configuration**

To quickly configure the stateless firewall filter, copy the following commands and paste them into the CLI.

```
[edit]
```
set firewall family inet filter fragment-RE term small-offset-term from fragment-offset 1-5
set firewall family inet filter fragment-RE term small-offset-term then syslog
discard

set firewall family inet filter fragment-RE term not-fragmented-term from source-address 10.2.1.0/24
set firewall family inet filter fragment-RE term not-fragmented-term from fragment-offset 0
set firewall family inet filter fragment-RE term not-fragmented-term from fragment-flags 0x0
set firewall family inet filter fragment-RE term not-fragmented-term from protocol tcp

set firewall family inet filter fragment-RE term not-fragmented-term from destination-port bgp

set firewall family inet filter fragment-RE term first-fragment-term from source-address 10.2.1.0/24
set firewall family inet filter fragment-RE term first-fragment-term from first-fragment
tcp

set firewall family inet filter fragment-RE term first-fragment-term from protocol tcp

set firewall family inet filter fragment-RE term first-fragment-term then accept
set firewall family inet filter fragment-RE term fragment-term from fragment-offset 6-8191

set firewall family inet filter fragment-RE term fragment-term then accept

---

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see Using the CLI Editor in Configuration Mode.

To configure the stateless firewall filter:

1. Define the stateless firewall filter.
   
   [edit]
   user@host# edit firewall family inet filter fragment-RE

2. Define the first term for the filter.
   
   [edit firewall family inet filter fragment-RE]
   user@host# edit term small-offset-term

3. Define the match conditions for the term.
   
   [edit firewall family inet filter fragment-RE term small-offset-term]
   user@host# set from fragment-offset 1-5

4. Define the action for the term.
   
   [edit firewall family inet filter fragment-RE term small-offset-term]
   user@host# set then syslog discard

5. Define the second term for the filter.
   
   [edit]
   user@host# edit firewall family inet filter fragment-RE term not-fragmented-term
6. Define the match conditions for the term.

   [edit firewall family inet filter fragment-RE term not-fragmented-term]
   user@host# set from fragment-flags 0x0 fragment-offset 0 protocol tcp
destination-port bgp source-address 10.2.1.0/24

7. Define the action for the term.

   [edit firewall family inet filter fragment-RE term not-fragmented-term]
   user@host# set then accept

8. Define the third term for the filter.

   [edit]
   user@host# edit firewall family inet filter fragment-RE term first-fragment-term

9. Define the match conditions for the term.

   [edit firewall family inet filter fragment-RE term first-fragment-term]
   user@host# set from first-fragment protocol tcp destination-port bgp
      source-address 10.2.1.0/24

10. Define the action for the term.

    [edit firewall family inet filter fragment-RE term first-fragment-term]
    user@host# set then accept

11. Define the last term for the filter.

    [edit]
    user@host# edit firewall family inet filter fragment-RE term fragment-term

12. Define the match conditions for the term.

    [edit firewall family inet filter fragment-RE term fragment-term]
    user@host# set from fragment-offset 0-8191

13. Define the action for the term.

    [edit firewall family inet filter fragment-RE term fragment-term]
    user@host# set then accept

Results  Confirm your configuration by entering the show firewall command from configuration
mode. If the output does not display the intended configuration, repeat the
configuration instructions in this example to correct it.

user@host# show firewall
family inet {
  filter fragment-RE {
    term small-offset-term {
      from {
        fragment-offset 1-5;
      }
      then {
        syslog;
        discard;
      }
    }
  }
}
If you are done configuring the device, enter `commit` from configuration mode.

**Verification**

To confirm that the configuration is working properly, perform these tasks:

- Displaying Stateless Firewall Filter Configurations on page 635
- Verifying a Firewall Filter that Handles Fragments on page 636

**Displaying Stateless Firewall Filter Configurations**

**Purpose**
Verify the configuration of the firewall filter. You can analyze the flow of the filter terms by displaying the entire configuration.

**Action**
From configuration mode, enter the `show firewall` command.

**Meaning**
Verify that the output shows the intended configuration of the firewall filter. In addition, verify that the terms are listed in the order in which you want the packets to be tested. You can move terms within a firewall filter by using the `insert` CLI command.
Verifying a Firewall Filter that Handles Fragments

Purpose
Verify that the actions of the firewall filter terms are taken.

Action
Send packets to the device that match the terms. In addition, verify that the filter actions are not taken for packets that do not match.

- Verify that packets with small fragment offsets are recorded in the router’s system logging facility.
- Use the `show route summary` command to verify that the routing table does not contain any entries with a protocol other than Direct, Local, BGP, or Static.

Sample Output
```
user@host> show route summary
Router ID: 192.168.249.71

inet.0: 34 destinations, 34 routes (33 active, 0 holddown, 1 hidden)
  Direct:  10 routes,  9 active
  Local:   9 routes,  9 active
  BGP:    10 routes, 10 active
  Static:  5 routes,  5 active
...
```

Meaning
Verify that the `show route summary` command does not display a protocol other than Direct, Local, BGP, or Static.

Related Topics

Example: Configuring a Filter to Match on IPv6 Flags

This example shows how to configure a filter to match on IPv6 TCP flags.

- Requirements on page 636
- Overview on page 636
- Configuration on page 637
- Verification on page 637

Requirements
No special configuration beyond device initialization is required before configuring stateless firewall filters.

Overview
In this example, you configure a filter to match on IPv6 TCP flags. You can use this example to configure IPv6 TCP flags in the SRX100, SRX210, SRX240, SRX650, and J Series devices.
**Configuration**

**Step-by-Step Procedure**  To configure a filter to match on IPv6 TCP flags:

1. Include the family statement at the firewall hierarchy level, specifying inet6 as the protocol family.
   
   ```
   [edit]
   user@host# firewall family inet6
   ```
   
2. Create the stateless firewall filter.
   
   ```
   [edit firewall family inet6]
   user@host# filter tcpfilt
   ```
   
3. Define the first term for the filter.
   
   ```
   [edit edit firewall family inet6 filter tcpfilt]
   user@host# term 1
   ```
   
4. Define the source address match conditions for the term.
   
   ```
   [edit firewall family inet6 filter tcpfilt term 1]
   user@host# from next-header tcp tcp-flags syn
   ```
   
5. Define the actions for the term.
   
   ```
   [edit firewall family inet6 filter tcpfilt term 1 from next-header tcp tcp-flags syn]
   user@host# then count tcp_syn_pkt log accept
   ```
   
6. If you are done configuring the device, commit the configuration.
   
   ```
   [edit]
   user@host# commit
   ```

**Verification**

To verify that the configuration is working properly, enter the `show firewall filter tcpfilt` command.
Part 4
Layer 2 Bridging and Switching

- Configuring Ethernet Ports for Switching on page 641
- Configuring Layer 2 Bridging and Transparent Mode on page 675
Chapter 25

Configuring Ethernet Ports for Switching

Certain ports on Juniper Networks devices can function as Ethernet access switches that switch traffic at Layer 2 and route traffic at Layer 3.

For information about Ethernet link aggregation for SRX3000 and SRX5000 line devices, see the “Aggregated Ethernet” chapter of the Junos OS Interfaces Configuration Guide for Security Devices.

For information about which devices support the features documented in this chapter, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.

This chapter contains the following topics:

- Ethernet Ports Switching Overview on page 641
- Switching Features Overview on page 642
- Understanding Switching Modes on the J Series Services Router on page 653
- Connecting J Series uPIMs in a Daisy-Chain on page 654
- Configuring Switching Modes on J Series uPIMs on page 654
- Verifying Switching Mode Configuration on J Series uPIMs on page 656
- Configuring Enhanced Switching Mode Features on page 657

**Ethernet Ports Switching Overview**

You can deploy supported devices in branch offices as an access or desktop switch with integrated routing capability, thus eliminating intermediate access switch devices from your network topology. The Ethernet ports provide switching while the Routing Engine provides routing functionality, enabling you to use a single device to provide routing, access switching, and WAN interfaces.

**Supported Devices and Ports**

Juniper Networks supports switching features on the following Ethernet ports and devices:

- Multiport Gigabit Ethernet uPIMs on the J Series device
- Onboard Ethernet ports (Gigabit and Fast Ethernet built-in ports) on the SRX100, SRX210, and SRX240 devices
- Multiport Gigabit Ethernet XPIM on the SRX650 device
Table 165: Supported Devices and Ports for Switching Features

<table>
<thead>
<tr>
<th>Device</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>J Series devices</td>
<td>Multiport Gigabit Ethernet uPIMs</td>
</tr>
<tr>
<td>SRX240 devices</td>
<td>Onboard Gigabit Ethernet ports (ge-0/0/0 through ge-0/0/15)</td>
</tr>
<tr>
<td>SRX210 devices</td>
<td>Onboard Gigabit Ethernet ports (ge-0/0/0 and ge-0/0/1)</td>
</tr>
<tr>
<td></td>
<td>Onboard Fast Ethernet ports (fe-0/0/2 and fe-0/0/7)</td>
</tr>
<tr>
<td>SRX100 devices</td>
<td>Onboard Fast Ethernet ports (fe-0/0/0 and fe-0/0/7)</td>
</tr>
<tr>
<td>SRX650 devices</td>
<td>Multiport Gigabit Ethernet XPIM modules</td>
</tr>
</tbody>
</table>

On J Series and SRX650 devices, you can set multiport switch modules (uPIMs and XPIMs, respectively) to three modes of operation: routing (the default), switching, or enhanced switching. Routed traffic is forwarded from any port of the Gigabit Ethernet uPIM to the WAN interface. Switched traffic is forwarded from one port of the Gigabit Ethernet uPIM to another port on the same Gigabit Ethernet uPIM. Switched traffic is not forwarded from a port on one uPIM to a port on a different uPIM.

On the SRX100, SRX220, and SRX240 devices, you can set the onboard Gigabit Ethernet ports to operate as either switched ports or routed ports.

Related Topics

- Switching Features Overview on page 642

Switching Features Overview

This topic describes the Layer 2 switching features for supported devices and ports. For more information, see the JUNOS Software Documentation for EX Series Switches.

This topic covers:

- VLANs on page 643
- Integrated Bridging and Routing on page 644
- Spanning Tree Protocols on page 644
- Generic VLAN Registration Protocol on page 644
- Link Aggregation on page 644
- 802.1X Port-Based Network Authentication on page 646
- Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) on page 649
- IGMP Snooping on page 651
- Q-in-Q VLAN Tagging on page 652
VLANs

Bridging divides a single physical LAN into two or more virtual LANs, or VLANs. Each VLAN is a collection of network nodes that are grouped together to form a separate broadcast domain. On an Ethernet network that is a single LAN, all traffic is forwarded to all nodes on the LAN. On VLANs, frames whose origin and destination are in the same VLAN are forwarded only within the VLAN. VLANs thus limit the amount of traffic flowing across the entire LAN, reducing the possible number of collisions and packet retransmissions within a VLAN and on the LAN as a whole.

On an Ethernet LAN, all network nodes must be physically connected to the same network. Each VLAN is identified by a single IP subnetwork and by standardized IEEE 802.1Q encapsulation.

To pass traffic within a VLAN, the switch uses Layer 2 forwarding protocols, including IEEE 802.1Q, Spanning Tree Protocol (STP), and Generic VLAN Registration Protocol (GVRP). To pass traffic between two VLANs, the switch uses standard Layer 3 routing protocols, such as static routing, OSPF, and RIP.

NOTE: Independent VLAN learning (IVL) is supported on SRX100, SRX240, and SRX650 devices and shared VLAN learning (SVL) is supported on J Series devices and SRX210 devices.

Types of Switch Ports

The ports, or interfaces, on a switch operate in either access mode or trunk mode.

An interface in access mode connects to a network device, such as a desktop computer, an IP telephone, a printer, a file server, or a security camera. The interface itself belongs to a single VLAN. The frames transmitted over an access interface are normal Ethernet frames.

Trunk interfaces handle traffic for multiple VLANs, multiplexing the traffic for all those VLANs over the same physical connection. Trunk interfaces are generally used to interconnect switches to one another.

IEEE 802.1Q Encapsulation and Tags

To identify which VLAN the traffic belongs to, all frames on an Ethernet VLAN are identified by a tag, as defined in the IEEE 802.1Q standard. These frames are tagged and are encapsulated with 802.1Q tags.

For a simple network that has only a single VLAN, all traffic has the same 802.1Q tag. When an Ethernet LAN is divided into VLANs, each VLAN is identified by a unique 802.1Q tag. The tag is applied to all frames so that the network nodes receiving the frames know to which VLAN a frame belongs. Trunk ports, which multiplex traffic among a number of VLANs, use the tag to determine the origin of frames and where to forward them.
**Integrated Bridging and Routing**

Integrated bridging and routing (IRB) provides support for simultaneous Layer 2 bridging and Layer 3 routing within the same bridge domain. Packets arriving on an interface of the bridge domain are switched or routed based on the destination MAC address of the packet. Packets with the router’s MAC address as the destination are routed to other Layer 3 interfaces.

**Spanning Tree Protocols**

Spanning Tree Protocol (STP), defined in IEEE 802.1D, creates a tree of links in the Ethernet switched network. Links that cause loops in the network are disabled, thereby providing a single active link between any two switches.

**NOTE:** Only STP is supported on the SRX210 device.

Rapid Spanning Tree Protocol (RSTP), originally defined in IEEE 802.1w and later merged into IEEE 802.1D, facilitates faster spanning tree convergence after a topology change.

Multiple Spanning Tree Protocol (MSTP), initially defined in IEEE 802.1s and later included in IEEE 802.1Q, supports mapping of multiple VLANs onto a single spanning tree instance. This reduces the number of spanning tree instances required in a switched network with many VLANs.

**Generic VLAN Registration Protocol**

The Generic VLAN Registration Protocol (GVRP) is an application protocol of the Generic Attribute Registration Protocol (GARP) and is defined in the IEEE 802.1Q standard. GVRP learns VLANs on a particular 802.1Q trunk port and adds the corresponding trunk port to the VLAN if the advertised VLAN is preconfigured on the switch.

The VLAN registration information sent by GVRP includes the current VLAN membership—that is, which switches are members of which VLANs—and which switch ports are in which VLAN. GVRP shares all VLAN information configured manually on a local switch.

As part of ensuring that VLAN membership information is current, GVRP removes switches and ports from the VLAN information when they become unavailable. Pruning VLAN information limits the network VLAN configuration to active participants only, reducing network overhead, and targets the scope of broadcast, unknown unicast, and multicast (BUM) traffic to interested devices only.

**Link Aggregation**

You can combine multiple physical Ethernet ports to form a logical point-to-point link, known as a link aggregation group (LAG) or bundle. A LAG provides more
bandwidth than a single Ethernet link can provide. Additionally, link aggregation provides network redundancy by load-balancing traffic across all available links. If one of the links should fail, the system automatically load-balances traffic across all remaining links. You can select up to eight Ethernet interfaces and include them within a link aggregation group.

**NOTE:** Link aggregation is supported only for Ethernet interfaces that are configured in switching mode (family ethernet-switching). Aggregating interfaces that are configured in routed mode (family inet) is not supported.

Link aggregation can be used for point-to-point connections. It balances traffic across the member links only within an aggregated Ethernet bundle and effectively increases the uplink bandwidth. Another advantage of link aggregation is increased availability, because the LAG is composed of multiple member links. If one member link fails, the LAG continues to carry traffic over the remaining links.

**Link Aggregation Group (LAG)**

You can configure a LAG by specifying the link number as a physical device and then associating a set of ports with the link. All the ports must have the same speed and be in full-duplex mode. JUNOS Software assigns a unique ID and port priority to each port.

**NOTE:** You must enable Link Aggregation Control Protocol (LACP) when you configure a LAG.

The ID and priority are not configurable. When configuring a LAG, consider the following guidelines:

- Up to 8 Ethernet ports can be created in each bundle.
- Each LAG must be configured on both sides of the link.
- The ports on either side of the link must be set to the same speed.

A typical deployment for a LAG would be to aggregate trunk links between an access switch and a distribution switch or customer edge (CE) device. LAGs are not supported on virtual chassis port links. LAGs can only be used for a point-to-point connection. At least one end of the LAG should be configured as active.

**Link Aggregation Control Protocol (LACP)**

LACP, a subcomponent of IEEE 802.3ad, provides additional functionality for LAGs. When LACP is not enabled, a local LAG might attempt to transmit packets to a remote single interface, which causes the communication to fail. When LACP is enabled, a local LAG cannot transmit packets unless a LAG with LACP is also configured on the remote end of the link.
By default, Ethernet links do not exchange protocol data units (PDUs), which contain information about the state of the link. You can configure Ethernet links to actively transmit PDUs, or you can configure the links to passively transmit them, sending out LACP PDUs only when they receive them from another link. The transmitting link is known as the actor and the receiving link is known as the partner.

**NOTE:** Presently, LACP can be configured only for the Ethernet switching family.

---

**802.1X Port-Based Network Authentication**

IEEE 802.1X, also known as port-based network access control (PNAC), is a mechanism to provide authentication to devices attached on the LAN. Hosts are authenticated when they initially connect to a LAN. Authenticating hosts before they receive an IP address from a DHCP server prevents unauthorized hosts from gaining access to the LAN.

A LAN network configured for 802.1X authentication contains three basic components:

- **Supplicant**—The IEEE term for a host that requests to join the network. The host can be responsive or nonresponsive. A responsive host is one on which 802.1X authentication is enabled and that provides authentication credentials (such as a user name and password). A nonresponsive host is one on which 802.1X authentication is not enabled.

- **Authenticator Port Access Entity**—The IEEE term for the authenticator. The SRX Series or J Series device is the authenticator and controls access by blocking all traffic to and from supplicants until they are authenticated.

- **Authentication server**—The server containing the back-end database that makes authentication decisions. (JUNOS Software supports RADIUS authentication servers.) The authentication server contains credential information for each supplicant that can connect to the network. The authenticator forwards credentials supplied by the supplicant to the authentication server. If the credentials forwarded by the authenticator match the credentials in the authentication server database, access is granted. If the credentials forwarded do not match, access is denied.

The implementation of 802.1X authentication provides the following features for the specified devices:

<table>
<thead>
<tr>
<th>Feature</th>
<th>SRX100</th>
<th>SRX210</th>
<th>SRX240</th>
<th>SRX650</th>
<th>J Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic VLAN assignment</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Authentication bypass</td>
<td>Yes (without VLAN option)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (without VLAN option)</td>
</tr>
<tr>
<td>Guest VLAN</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>RADIUS server failure fallback</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
The 802.1X implementation provides the following supplicant capacities:

<table>
<thead>
<tr>
<th>VoIP VLAN support</th>
<th>No</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS accounting</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MAC RADIUS authentication</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Dynamic VLAN Assignment

When a supplicant first connects to an SRX Series or J Series device, the authenticator sends a request to the supplicant to begin 802.1X authentication. If the supplicant is an 802.1X-enabled device, it responds, and the authenticator relays an authentication request to the RADIUS server.

As part of the reply to the authentication request, the RADIUS server returns information about the VLAN to which the port belongs. By configuring the VLAN information at the RADIUS server, you can control the VLAN assignment on the port.

### MAC RADIUS Authentication

If the authenticator sends three requests to a supplicant to begin 802.1X authentication and receives no response, the supplicant is considered nonresponsive. For a nonresponsive supplicant, the authenticator sends a request to the RADIUS server for authentication of the supplicant’s MAC address. If the MAC address matches an entry in a predefined list of MAC addresses on the RADIUS server, authentication is granted and the authenticator opens LAN access on the interface where the supplicant is connected.

You can configure the number of times the authenticator attempts to receive a response and the time period between attempts.

### Static MAC Bypass

The authenticator can allow particular supplicants direct access to the LAN and bypass the authentication server by including the supplicants’ MAC addresses in the static MAC bypass list configured on the SRX Series or J Series device. This list is checked.
If a match is found, the supplicant is considered successfully authenticated and the interface is opened up for it. No further authentication is done for that supplicant. If a match is not found and 802.1X authentication is enabled for the supplicant, the device continues with MAC RADIUS authentication on the authentication server.

For each MAC address in the list, you can configure the VLAN to which the supplicant is moved or the interfaces on which the supplicant can connect.

**Guest VLAN**

You can specify a guest VLAN that provides limited network access for nonresponsive supplicants. If a guest-vlan is configured, the authenticator connects all nonresponsive supplicants to the predetermined VLAN, providing limited network access, often only to the Internet. This type of configuration can be used to provide Internet access to visitors without compromising company security.

**NOTE:** If you specify a guest VLAN, all nonresponsive supplicants are connected to the guest VLAN without an attempt to authenticate by MAC address.

**VoIP VLAN Support**

When VoIP is used with 802.1X, the RADIUS server authenticates the phone, and Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) provides the class-of-service (CoS) parameters for the phone. (For more information, refer to “Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)” on page 649.)

You can configure 802.1X authentication to work with VoIP in multiple-suppliant or single-suppliant mode:

- **Multiple-suppliant mode**—Allows multiple supplicants to connect to the interface. Each supplicant is authenticated individually.
- **Single-suppliant mode**—Authenticates only the first supplicant. All other supplicants who connect later to the interface are allowed to “piggyback” on the first supplicant’s authentication and gain full access.

**Server Reject VLAN**

By default, when authentication fails, the supplicant is denied access to the network. However, you can specify a VLAN to which the supplicant is moved if authentication fails. The server reject VLAN is similar to a guest VLAN. With a server reject VLAN, however, authentication is first attempted by credential, then by MAC address. If both authentication methods fail, the supplicant is given access to a predetermined VLAN with limited network access.
**RADIUS Server Failure Fallback**

You can define one of four actions to be taken if no RADIUS authentication server is reachable (if, for example, a server failure or a timeout has occurred on the authentication server).

- **deny**—(default) Prevent traffic from flowing from the supplicant through the interface.
- **permit**—Allow traffic to flow from the supplicant through the interface as if the supplicant were successfully authenticated by the RADIUS server.
- **use-cache**—Force successful authentication if authentication was granted before the failure or timeout. This ensures that authenticated users are not adversely affected by a failure or timeout.
- **vlan vlan-name | vlan-id** —Move the supplicant to a different VLAN specified by name or ID. This applies only to the first supplicant connecting to the interface.

NOTE: For **permit**, **use-cache**, and **vlan** fallback actions to work, 802.1X supplicants need to accept an out of sequence SUCCESS packet.

**RADIUS Accounting**

Configuring RADIUS accounting on a SRX Series or J Series device lets you collect statistical data about users logging on and off a LAN, and sends it to a RADIUS accounting server. The collected data can be used for general network monitoring, to analyze and track usage patterns, or to bill a user based on the amount of time or type of services accessed.

To configure RADIUS accounting, specify one or more RADIUS accounting servers to receive the statistical data from the device, and select the type of accounting data to be collected. To view the collected statistics, you can access the log file configured to receive them.

**Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)**

Devices use LLDP and LLDP-MED to learn and distribute device information on network links. The information allows the device to quickly identify a variety of systems, resulting in a LAN that interoperates smoothly and efficiently.

LLDP-capable devices transmit information in Type Length Value (TLV) messages to neighbor devices. Device information can include specifics, such as chassis and port identification and system name and system capabilities. The TLVs leverage this information from parameters that have already been configured in the Juniper Networks JUNOS Software.

LLDP-MED goes one step further, exchanging IP-telephony messages between the device and the IP telephone. These TLV messages provide detailed information on
PoE policy. The PoE Management TLVs let the device ports advertise the power level and power priority needed. For example, the device can compare the power needed by an IP telephone running on a PoE interface with available resources. If the device cannot meet the resources required by the IP telephone, the device could negotiate with the telephone until a compromise on power is reached.

The following basic TLVs are supported:

- **Chassis Identifier**—The MAC address associated with the local system.
- **Port identifier**—The port identification for the specified port in the local system.
- **Port Description**—The user-configured port description. The port description can be a maximum of 256 characters.
- **System Name**—The user-configured name of the local system. The system name can be a maximum of 256 characters.
- **System Description**—The system description containing information about the software and current image running on the system. This information is not configurable, but taken from the software.
- **System Capabilities**—The primary function performed by the system. The capabilities that system supports; for example, bridge or router. This information is not configurable, but based on the model of the product.
- **Management Address**—The IP management address of the local system.

The following LLDP-MED TLVs are supported:

- **LLDP-MED Capabilities**—A TLV that advertises the primary function of the port. The capabilities values range 0 through 15:
  - 0—Capabilities
  - 1—Network policy
  - 2—Location identification
  - 3—Extended power via medium-dependent interface power-sourcing equipment (MDI-PSE)
  - 4—Inventory
  - 5–15—Reserved

- **LLDP-MED Device Class Values:**
  - 0—Class not defined
  - 1—Class 1 device
  - 2—Class 2 device
  - 3—Class 3 device
  - 4—Network connectivity device
  - 5–255—Reserved
Network Policy—A TLV that advertises the port VLAN configuration and associated Layer 2 and Layer 3 attributes. Attributes include the policy identifier, application types, such as voice or streaming video, 802.1Q VLAN tagging, and 802.1p priority bits and DiffServ code points.

Endpoint Location—A TLV that advertises the physical location of the endpoint.

Extended Power via MDI—A TLV that advertises the power type, power source, power priority, and power value of the port. It is the responsibility of the PSE device (network connectivity device) to advertise the power priority on a port.

LLDP and LLDP-MED must be explicitly configured on uPIMs (in enhanced switching mode) on J Series devices, base ports on SRX100, SRX210, and SRX240 devices, and Gigabit Backplane Physical Interface Modules (GPIMs) on SRX650 devices. To configure LLDP on all interfaces or on a specific interface, use the `lldp` statement at the `[set protocols]` hierarchy. To configure LLDP-MED on all interfaces or on a specific interface, use the `lldp-med` statement at the `[set protocols]` hierarchy.

**IGMP Snooping**

Internet Group Management Protocol (IGMP) snooping regulates multicast traffic in a switched network. With IGMP snooping enabled, a LAN switch monitors the IGMP transmissions between a host (a network device) and a multicast router, keeping track of the multicast groups and associated member ports. The switch uses that information to make intelligent multicast-forwarding decisions and forward traffic to the intended destination interfaces. J Series devices support IGMPv1 and IGMPv2.

**How IGMP Snooping Works**

A J Series device usually learns unicast MAC addresses by checking the source address field of the frames it receives. However, a multicast MAC address can never be the source address for a packet. As a result, the switch floods multicast traffic on the VLAN, consuming significant amounts of bandwidth.

IGMP snooping regulates multicast traffic on a VLAN to avoid flooding. When IGMP snooping is enabled, the switch intercepts IGMP packets and uses the content of the packets to build a multicast cache table. The cache table is a database of multicast groups and their corresponding member ports. The cache table is then used to regulate multicast traffic on the VLAN.

When the router receives multicast packets, it uses the cache table to selectively forward the packets only to the ports that are members of the destination multicast group.

**How Hosts Join and Leave Multicast Groups**

Hosts can join multicast groups in either of two ways:

- By sending an unsolicited IGMP join message to a multicast router that specifies the IP multicast that the host is attempting to join.
- By sending an IGMP join message in response to a general query from a multicast router.
A multicast router continues to forward multicast traffic to a VLAN provided that at least one host on that VLAN responds to the periodic general IGMP queries. For a host to remain a member of a multicast group, therefore, it must continue to respond to the periodic general IGMP queries.

To leave a multicast group, a host can either not respond to the periodic general IGMP queries, which results in a “silent leave” (the only leave option for hosts connected to switches running IGMPv1), or send a group-specific IGMPv2 leave message.

**Q-in-Q VLAN Tagging**

Q-in-Q tunneling, defined by the IEEE 802.1ad standard, allows service providers on Ethernet access networks to extend a Layer 2 Ethernet connection between two customer sites.

In Q-in-Q tunneling, as a packet travels from a customer VLAN (C-VLAN) to a service provider’s VLAN, a service provider-specific 802.1Q tag is added to the packet. This additional tag is used to segregate traffic into service–provider–defined service VLANs (S-VLANs). The original customer 802.1Q tag of the packet remains and is transmitted transparently, passing through the service provider’s network. As the packet leaves the S-VLAN in the downstream direction, the extra 802.1Q tag is removed.

There are three ways to map C-VLANs to an S-VLAN:

- **All-in-one bundling**—Use the `dot1q-tunneling` statement at the `[edit vlans]` hierarchy to map without specifying customer VLANs. All packets from a specific access interface are mapped to the S-VLAN.
- **Many-to-one bundling**—Use the `customer-vlans` statement at the `[edit vlans]` hierarchy to specify which C-VLANs are mapped to the S-VLAN.
- **Mapping C-VLAN on a specific interface**—Use the `mapping` statement at the `[edit vlans]` hierarchy to map a specific C-VLAN on a specified access interface to the S-VLAN.

The following table lists the C-VLAN to S-VLAN mapping supported on SRX Series devices:

<table>
<thead>
<tr>
<th>Mapping</th>
<th>SRX210</th>
<th>SRX240</th>
<th>SRX650</th>
<th>J Series Devices (PIM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>All-in-one bundling</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Many-to-one bundling</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Mapping C-VLAN on a specific</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>interface</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following table lists the C-VLAN to S-VLAN mapping supported on SRX Series devices:
NOTE: On SRX650 devices, in the dot1q-tunneling configuration options, customer VLANs range and VLAN push do not work together for the same S-VLAN, even when you commit the configuration. If both are configured, then VLAN push takes priority over customer VLANs range.

Integrated bridging and routing (IRB) interfaces are supported on Q-in-Q VLANs for SRX210, SRX240, SRX650, and J Series devices. Packets arriving on an IRB interface on a Q-in-Q VLAN are routed regardless of whether the packet is single or double tagged. The outgoing routed packets contain an S-VLAN tag only when exiting a trunk interface; the packets exit the interface untagged when exiting an access interface.

In a Q-in-Q deployment, customer packets from downstream interfaces are transported without any changes to source and destination MAC addresses. You can disable MAC address learning at both the interface level and the VLAN level. Disabling MAC address learning on an interface disables learning for all the VLANs of which that interface is a member. When you disable MAC address learning on a VLAN, MAC addresses that have already been learned are flushed.

Understanding Switching Modes on the J Series Services Router

On the J Series device, you set the uPIM to one of three operating modes: routing (the default), switching, or enhanced switching.

When you set a multiport uPIM to switching mode, the uPIM appears as a single entity for monitoring purposes. The only physical port settings that you can configure are autonegotiation, speed, and duplex mode on each uPIM port, and these settings are optional.

Routing Mode

In routing mode, the multiport uPIM has the same configuration options as any other Gigabit Ethernet interface. To configure uPIM Gigabit Ethernet interfaces in routing mode, see "Configuring Gigabit Ethernet Interfaces—Quick Configuration" and "Configuring Network Interfaces with a Configuration Editor."

Switching Mode

In switching mode, the uPIM appears in the list of interfaces as a single interface, which is the first interface on the uPIM—for example, ge-2/0/0. You can optionally configure each uPIM port only for autonegotiation, speed, and duplex mode. A uPIM in switching mode can perform the following functions:

- Layer 3 forwarding—Routes traffic destined for WAN interfaces and other PIMs present on the chassis.
- Layer 2 forwarding—Switches intra-LAN traffic from one host on the LAN to another LAN host (one port of uPIM to another port of same uPIM).
**Enhanced Switching Mode**

In enhanced switching mode, each port can be configured for switching or routing mode. This usage differs from the routing and switching modes, in which all ports must be in either switching or routing mode. The uPIM in enhanced switching mode provides the following features:

- Supports configuration of different types of VLANs and inter-VLAN routing
- Supports Layer 2 control plane protocols such as Spanning Tree Protocol (STP) and Link Aggregation Control Protocol (LACP)
- Supports port-based Network Access Control (PNAC) by means of authentication servers

**NOTE:** The SRX100 and SRX210 devices support enhanced switching mode only. When you set a multiport uPIM to enhanced switching mode, all the Layer 2 switching features are supported on the uPIM.

**NOTE:** You can configure uPIM in enhanced switching mode only in JUNOS 9.2 or later releases.

**Connecting J Series uPIMs in a Daisy-Chain**

You cannot combine multiple uPIMs to act as a single integrated switch. However, you can connect uPIMs on the same chassis externally by physically connecting a port on one uPIM to a port on another uPIM in a daisy-chain fashion.

Two or more uPIMs daisy-chained together create a single switch with a higher port count than either individual uPIM. One port on each uPIM is used solely for the connection. For example, if you daisy-chain a 6-port uPIM and an 8-port uPIM, the result operates as a 12-port uPIM. Any port of a uPIM can be used for daisy-chaining.

Configure the IP address for only one of the daisy-chained uPIMs, making it the primary uPIM. The secondary uPIM routes traffic to the primary uPIM, which forwards it to the Routing Engine. This results in some increase in latency and packet drops due to oversubscription of the external link.

Only one link between the two uPIMs is supported. Connecting more than one link between uPIMs creates a loop topology, which is not supported.

**Configuring Switching Modes on J Series uPIMs**

You can set a multiport Gigabit Ethernet uPIM on a J Series device to either switching or enhanced switching mode. The default mode of operation is routing mode.
When you set a multiport uPIM to switching mode, the uPIM appears as a single entity for monitoring purposes. The only physical port settings that you can configure are autonegotiation, speed, and duplex mode on each uPIM port, and these settings are optional.

### Before You Begin

For background information, read “Understanding Switching Modes on the J Series Services Router” on page 653.

### NOTE:

You cannot configure switch ports from J-Web Quick Configuration pages. You must use the J-Web or CLI configuration editor.

### J-Web Configuration

To set the uPIM mode of operation to switching:

1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Chassis, click Configure or Edit.
3. Next to Fpc, click Add new entry.
4. In the Slot field, enter the number of the slot of the chassis in which the uPIM is inserted, and click OK.
5. Next to Pic, click Add new Entry.
6. Enter 0 in the Slot field. (This number is always 0 on a J Series device.)
7. Next to Ethernet, click Configure.
8. From the Pic mode list, choose switching and click OK.

To set the uPIM mode of operation to enhanced switching:

1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Chassis, click Configure or Edit.
3. Next to Fpc, click Add new entry.
4. In the Slot field, enter the number of the slot of the chassis in which the uPIM is inserted, and click OK.
5. Next to Pic, click Add new Entry.
6. Enter 0 in the Slot field. (This number is always 0 on a J Series device.)
7. Next to Ethernet, click Configure.
8. From the Pic mode list, choose enhanced-switching and click OK.

To set a physical parameter on a port on the uPIM:
1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Interfaces, click Configure or Edit.
3. Click the name of the uPIM interface—for example ge-2/0/0.
4. Next to Switch options, click Configure.
5. Next to Switch port, click Add new entry.
6. In the Port field, enter the number of the port you want to configure.
7. Choose the settings for Autonegotiation, Link mode, and Speed, and click OK.

**CLI Configuration**

To set the uPIM mode of operation to switching:

```
user@host# set chassis fpc slot-number pic 0 ethernet pic-mode switching
```

To set the uPIM mode of operation to enhanced switching:

```
user@host# set chassis fpc slot-number pic 0 ethernet pic-mode enhanced-switching
```

To set a physical parameter on a port on the uPIM:

```
user@host# set interfaces ge-2/0/0 switch-options switch-port 1 auto-negotiation
```

**Related Topics**

- Verifying Switching Mode Configuration on J Series uPIMs on page 656

**Verifying Switching Mode Configuration on J Series uPIMs**

The operational mode command for checking the status and statistics for multiport uPIMs in switching mode is different from that in routing mode. For uPIMs in routing mode, the operational commands are the same as for other Gigabit Ethernet interfaces, such as the 1-port Gigabit Ethernet ePIM and built-in Gigabit Ethernet ports.

However, not all operational mode commands are supported for ports of a uPIM in switching mode. For example, the operational mode command for monitoring port statistics is not supported.

**Before You Begin**

See “Configuring Switching Modes on J Series uPIMs” on page 654.

**NOTE:** To clear the statistics for the individual switch ports, use the clear interfaces statistics ge-pim/0/0 switch-port port-number command.
To verify the status and view statistics for a port on a uPIM in switching mode:

user@host#  **show interfaces ge-slot/0/0 switch-port port-number**

Port 0, Physical link is Up

Speed: 100mbps, Auto-negotiation: Enabled

Statistics:

<table>
<thead>
<tr>
<th></th>
<th>Receive</th>
<th>Transmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total bytes</td>
<td>28437086</td>
<td>21792250</td>
</tr>
<tr>
<td>Total packets</td>
<td>409145</td>
<td>88008</td>
</tr>
<tr>
<td>Unicast packets</td>
<td>9987</td>
<td>83817</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>145002</td>
<td>0</td>
</tr>
<tr>
<td>Broadcast packets</td>
<td>254156</td>
<td>4191</td>
</tr>
<tr>
<td>Multiple collisions</td>
<td>23</td>
<td>10</td>
</tr>
<tr>
<td>FIFO/CRC/Align errors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MAC pause frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Oversized frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Runt frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Jabber frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fragment frames</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Discarded frames</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Autonegotiation information:
Negotiation status: Complete
Link partner:
  Link mode: Full-duplex, Flow control: None, Remote fault: OK, Link partner Speed: 100 Mbps
Local resolution:
  Flow control: None, Remote fault: Link OK

---

**Configuring Enhanced Switching Mode Features**

This section describes how to configure enhanced switching mode features on SRX Series and J Series devices.

---

**Before You Begin**

See “Configuring Switching Modes on J Series uPIMs” on page 654.

---

This section covers:

- Configuring VLANs—Quick Configuration on page 657
- Configuring a Spanning Tree—Quick Configuration on page 660
- Configuring LACP in J-Web on page 663
- Configuring 802.1X Features on page 666
- Configuring IGMP Snooping—Quick Configuration on page 671
- Configuring GVRP—Quick Configuration on page 673

---

**Configuring VLANs—Quick Configuration**

Each VLAN is a collection of network nodes that are grouped together to form separate broadcast domains. On an Ethernet network that is a single LAN, all traffic is forwarded to all nodes on the LAN. On VLANs, frames whose origin and destination
are in the same VLAN are forwarded only within the local VLAN. Frames that are not
destined for the local VLAN are the only ones forwarded to other broadcast domains.
VLANs thus limit the amount of traffic flowing across the entire LAN, reducing the
possible number of collisions and packet retransmissions within a VLAN and on the
LAN as a whole.

On an Ethernet LAN, all network nodes must be physically connected to the same
network. On VLANs, the physical location of the nodes is not important, so you can
group network devices in any way that makes sense for your organization, such as
by department or business function, by types of network nodes, or even by physical
location. Each VLAN is identified by a single IP subnetwork and by standardized IEEE
802.1Q encapsulation.

You can use the J-Web Quick Configuration to add a new VLAN or to edit or delete
an existing VLAN.

To access the VLAN Quick Configuration:
1. In the J-Web user interface, select Configure > Switching > VLAN.
   The VLAN Configuration page displays a list of existing VLANs. If you select a
   specific VLAN, the specific VLAN details are displayed in the Details section.
2. Click one:
   ■ Add—Creates a VLAN.
   ■ Edit—Edits an existing VLAN configuration.
   ■ Delete—Deletes an existing VLAN.

   **NOTE:** If you delete a VLAN, the VLAN configuration for all the associated interfaces
   is also deleted.

   When you are adding or editing a VLAN, enter information as described in Table
   166 on page 658.
3. Click one:
   ■ To apply changes to the configuration, click OK.
   ■ To cancel the configuration without saving changes, click Cancel.

**Table 166: VLAN Configuration Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>General tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN Name</td>
<td>Specifies a unique name for the VLAN.</td>
<td>Enter a name.</td>
</tr>
</tbody>
</table>
Table 166: VLAN Configuration Details (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID/Range</td>
<td>Specifies the identifier or range for the VLAN.</td>
<td>Select one:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ VLAN ID—Type a unique identification number from 1 through 4094. If no value is specified, it defaults to 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ VLAN Range—Type a number range to create VLANs with IDs corresponding to the range. For example, the range 2–3 will create two VLANs with the ID 2 and 3.</td>
</tr>
<tr>
<td>Description</td>
<td>Describes the VLAN.</td>
<td>Enter a brief description for the VLAN.</td>
</tr>
<tr>
<td>MAC-Table-Aging-Time</td>
<td>Specifies the maximum time that an entry can remain in the forwarding table before it ages out.</td>
<td>Type the number of seconds from 60 through 1000000.</td>
</tr>
<tr>
<td>Input Filter</td>
<td>Specifies the VLAN firewall filter that is applied to incoming packets.</td>
<td>To apply an input firewall filter, select the firewall filter from the list.</td>
</tr>
<tr>
<td>Output Filter</td>
<td>Specifies the VLAN firewall filter that is applied to outgoing packets.</td>
<td>To apply an output firewall filter, select the firewall filter from the list.</td>
</tr>
<tr>
<td>Ports tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ports</td>
<td>Specifies the ports to be associated with this VLAN for data traffic. You can also remove the port association.</td>
<td>Click one:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Add—Select the ports from the available list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Remove—Select the port that you do not want associated with the VLAN.</td>
</tr>
<tr>
<td>IP Address tab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Layer 3 Information</td>
<td>Specifies IP address options for the VLAN.</td>
<td>Select to enable the IP address options.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Specifies the IP address of the VLAN.</td>
<td>Enter the IP address.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Specifies the range of logical addresses within the address space that is assigned to an organization.</td>
<td>Enter the address, for example, 255.255.255.0. You can also specify the address prefix.</td>
</tr>
<tr>
<td>Input Filter</td>
<td>Specifies the VLAN interface firewall filter that is applied to incoming packets.</td>
<td>To apply an input firewall filter to an interface, select the firewall filter from the list.</td>
</tr>
<tr>
<td>Output Filter</td>
<td>Specifies the VLAN interface firewall filter that is applied to outgoing packets.</td>
<td>To apply an output firewall filter to an interface, select the firewall filter from the list.</td>
</tr>
<tr>
<td>ARP/MAC Details</td>
<td>Specifies the details for configuring the static IP address and MAC.</td>
<td>Click the ARP/MAC Details button. Enter the static IP address and MAC address in the window that is displayed.</td>
</tr>
<tr>
<td>VoIP tab</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 166: VLAN Configuration Details (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports</td>
<td>Specifies the ports to be associated with this VLAN for voice traffic. You can also remove the port association.</td>
<td>Click one:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Add—Select the ports from the available list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Remove—Select the port that you do not want associated with the VLAN.</td>
</tr>
</tbody>
</table>

Configuring a Spanning Tree—Quick Configuration

Juniper devices provide Layer 2 loop prevention through Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). You can configure bridge protocols data unit (BPDU) protection on interfaces to prevent them from receiving BPDUs that could result in STP misconfigurations, which could lead to network outages.

You can use the J-Web Quick Configuration to add a spanning tree or to edit or delete an existing spanning tree.

To access the Spanning Tree Quick Configuration:

1. In the J-Web user interface, select Configure > Switching > Spanning Tree.
   
   The Spanning Tree Configuration page displays a list of existing spanning trees. If you select a specific spanning tree, the specific spanning tree details are displayed in the General and Interfaces tabs.

2. Click one of the following:
   ■ Add—Creates a spanning tree.
   ■ Edit—Edits an existing spanning-tree configuration.
   ■ Delete—Deletes an existing spanning tree.

   When you are adding a spanning tree, select a protocol name:
   ■ If you select STP, enter information as described in Table 167 on page 661.
   ■ If you select RSTP, enter information as described in Table 168 on page 661.
   ■ If you select MSTP, enter information as described in Table 169 on page 662.

   Select the Ports tab to configure the ports associated with this spanning tree. Click one of the following:
   ■ Add—Creates a new spanning-tree interface configuration.
   ■ Edit—Modifies an existing spanning-tree interface configuration.
   ■ Delete—Deletes an existing spanning-tree interface configuration.

   When you are adding or editing a spanning-tree port, enter information as described in Table 170 on page 663.

3. Click one:
To apply changes to the configuration, click **OK**.

To cancel the configuration without saving changes, click **Cancel**.

### Table 167: STP Configuration Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Name</td>
<td>Displays the spanning-tree protocol.</td>
<td>View only.</td>
</tr>
<tr>
<td>Disable</td>
<td>Disables STP on the interface.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>BPDU Protect</td>
<td>Specifies that BPDU blocks are to be processed.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>Bridge Priority</td>
<td>Specifies the bridge priority. The bridge priority determines which bridge is elected as the root bridge. If two bridges have the same path cost to the root bridge, the bridge priority determines which bridge becomes the designated bridge for a LAN segment.</td>
<td>Select a value.</td>
</tr>
<tr>
<td>Forward Delay</td>
<td>Specifies the number of seconds an interface waits before changing from spanning-tree learning and listening states to the forwarding state.</td>
<td>Enter a value from 4 through 30 seconds.</td>
</tr>
<tr>
<td>Hello Time</td>
<td>Specifies time interval in seconds at which the root bridge transmits configuration BPDUs.</td>
<td>Enter a value from 1 through 10 seconds.</td>
</tr>
<tr>
<td>Max Age</td>
<td>Specifies the maximum aging time in seconds for all MST instances. The maximum aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.</td>
<td>Enter a value from 6 through 40 seconds.</td>
</tr>
</tbody>
</table>

### Table 168: RSTP Configuration Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Name</td>
<td>Displays the spanning-tree protocol.</td>
<td>View only.</td>
</tr>
<tr>
<td>Disable</td>
<td>Specifies whether RSTP must be disabled on the interface.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>BPDU Protect</td>
<td>Specifies that BPDU blocks are to be processed.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>Bridge Priority</td>
<td>Specifies the bridge priority. The bridge priority determines which bridge is elected as the root bridge. If two bridges have the same path cost to the root bridge, the bridge priority determines which bridge becomes the designated bridge for a LAN segment.</td>
<td>Select a value.</td>
</tr>
<tr>
<td>Forward Delay</td>
<td>Specifies the number of seconds a port waits before changing from its spanning-tree learning and listening states to the forwarding state.</td>
<td>Enter a value from 4 through 30 seconds.</td>
</tr>
<tr>
<td>Hello Time</td>
<td>Specifies the hello time in seconds for all MST instances.</td>
<td>Enter a value from 1 through 10 seconds.</td>
</tr>
</tbody>
</table>
Table 168: RSTP Configuration Parameters *(continued)*

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Age</td>
<td>Specifies the maximum aging time in seconds for all MST instances.</td>
<td>Enter a value from 6 through 40 seconds.</td>
</tr>
<tr>
<td></td>
<td>The maximum aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.</td>
<td></td>
</tr>
</tbody>
</table>

Table 169: MSTP Configuration Parameters

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Name</td>
<td>Displays the spanning-tree protocol.</td>
<td>View only.</td>
</tr>
<tr>
<td>Disable</td>
<td>Specifies whether MSTP must be disabled on the interface.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>BPDU Protect</td>
<td>Specifies that BPDU blocks are to be processed.</td>
<td>To enable this option, select the check box.</td>
</tr>
<tr>
<td>Bridge Priority</td>
<td>Specifies the bridge priority. The bridge priority determines which bridge is elected as the root bridge. If two bridges have the same path cost to the root bridge, the bridge priority determines which bridge becomes the designated bridge for a LAN segment.</td>
<td>Select a value.</td>
</tr>
<tr>
<td>Forward Delay</td>
<td>Specifies the number of seconds a port waits before changing from its spanning-tree learning and listening states to the forwarding state.</td>
<td>Enter a value from 4 through 30 seconds.</td>
</tr>
<tr>
<td>Hello Time</td>
<td>Specifies the hello time in seconds for all MST instances.</td>
<td>Enter a value from 1 through 10 seconds.</td>
</tr>
<tr>
<td>Max Age</td>
<td>Specifies the maximum aging time for all MST instances. The maximum aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.</td>
<td>Enter a value from 6 through 40 seconds.</td>
</tr>
<tr>
<td>Configuration Name</td>
<td>MSTP region name carried in the MSTP bridge protocol data units (BPDUs).</td>
<td>Enter a name.</td>
</tr>
<tr>
<td>Max Hops</td>
<td>Maximum number of hops a BPDU can be forwarded in the MSTP region</td>
<td>Enter a value from 1 through 255.</td>
</tr>
<tr>
<td>Revision Level</td>
<td>Revision number of the MSTP region configuration.</td>
<td>Enter a value from 0 through 65535.</td>
</tr>
</tbody>
</table>

MSTI tab

<table>
<thead>
<tr>
<th>MSTI Id</th>
<th>Specifies the multiple spanning-tree instance (MSTI) identifier. MSTI IDs are local to each region, so you can reuse the same MSTI ID in different regions.</th>
<th>Click one:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Add—Creates a MSTI.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Edit—Edits an existing MSTI.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Delete—Deletes an existing MSTI.</td>
</tr>
</tbody>
</table>
### Table 169: MSTP Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge Priority</td>
<td>Specifies the bridge priority. The bridge priority determines which bridge is elected as the root bridge. If two bridges have the same path cost to the root bridge, the bridge priority determines which bridge becomes the designated bridge for a LAN segment.</td>
<td>Select a value.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Specifies the VLANs for the MSTI.</td>
<td>Click one:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Add—Selects VLANs from the list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Remove—Deletes the selected VLAN.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Specifies the interface for the MSTP protocol.</td>
<td>Click one:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Add—Selects interfaces from the list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Edit—Edits the selected interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Remove—Deletes the selected interface.</td>
</tr>
</tbody>
</table>

### Table 170: Spanning-Tree Ports Configuration Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Specifies the interface for the spanning-tree protocol type.</td>
<td>Select an interface.</td>
</tr>
<tr>
<td>Cost</td>
<td>Specifies the link cost to control which bridge is the designated bridge and which interface is the designated interface.</td>
<td>Enter a value from 1 through 200,000,000.</td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies the interface priority to control which interface is elected as the root port.</td>
<td>Select a value.</td>
</tr>
<tr>
<td>Edge</td>
<td>Configures the interface as an edge interface. Edge interfaces immediately transition to a forwarding state.</td>
<td>Select to configure the interface as an edge interface.</td>
</tr>
<tr>
<td>Mode</td>
<td>Specifies the link mode.</td>
<td>Select one:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Point to Point</strong>—For full-duplex links, select this mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Shared</strong>—For half-duplex links, select this mode.</td>
</tr>
</tbody>
</table>

### Configuring LACP in J-Web

Use the link aggregation feature to aggregate one or more Ethernet interfaces to form a virtual link or link aggregation group (LAG). The MAC client can treat this virtual...
link like a single link. Link aggregation increases bandwidth, provides graceful
degradation as failure occurs, and increases availability.

You can use the J-Web interface to add a new LAG or to edit or delete an existing
LAG.

**NOTE:** The interfaces that are already configured with MTU, duplex, flow control, or
logical interfaces are displayed. However, when you select an already configured
interface, a warning message is displayed.

To access the LACP Configuration:
1. In the J-Web user interface, select **Configure > Interfaces > Link Aggregation**.
The Aggregated Interfaces list is displayed.
2. Click one of the following:
   - **Device Count**—Creates an aggregated Ethernet interface, or LAG. You can
     choose the number of device that you want to create. Information displayed
     on the link aggregation page are specified in Table 171 on page 664 and the
details of aggregation are specified in Table 172 on page 665
   - **Add**—Adds a new aggregated Ethernet Interface, or LAG. Enter information
     as specified in Table 173 on page 665.
   - **Edit**—Modifies a selected LAG
     - **Aggregation**—Modifies an selected LAG. Enter information as specified
       in Table 173 on page 665.
     - **VLAN**—Specifies VLAN options for the selected LAG. See Table 174 on
       page 666 for details on the options.
     - **IP Option**—Configuring IP address to LAG is not supported and when
       you try to configure the IP address an error message is displayed.
   - **Delete**—Deletes the selected LAG.
   - **Disable Port** or **Enable Port**—Disables or enables the administrative status
     on the selected interface.

<table>
<thead>
<tr>
<th>Table 171: LACP (Link Aggregation Control Protocol) Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Field</strong></td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>Aggregated Interface</td>
</tr>
<tr>
<td>Link Status</td>
</tr>
<tr>
<td>VLAN (VLAN ID)</td>
</tr>
<tr>
<td>Description</td>
</tr>
</tbody>
</table>
### Table 172: Details of Aggregation

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Status</td>
<td>Displays if the interface is enabled (Up) or disabled (Down).</td>
</tr>
<tr>
<td>Logical Interfaces</td>
<td>Shows the logical interface of the aggregated interface.</td>
</tr>
<tr>
<td>Member Interfaces</td>
<td>Member interfaces hold all the aggregated interfaces of the selected interfaces.</td>
</tr>
<tr>
<td>Port Mode</td>
<td>Specifies the mode of operation for the port: trunk or access.</td>
</tr>
<tr>
<td>Native VLAN (VLAN ID)</td>
<td>VLAN identifier to associate with untagged packets received on the interface.</td>
</tr>
<tr>
<td>IP Address/Subnet Mask</td>
<td>Specifies the address of the aggregated interfaces.</td>
</tr>
<tr>
<td>IPV6 Address/Subnet Mask</td>
<td>Specifies the IPV6 address of the aggregated interfaces.</td>
</tr>
</tbody>
</table>

### Table 173: Aggregated Ethernet Interface Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregated Interface</td>
<td>Indicates the name of the aggregated interface.</td>
<td>Enter the aggregated interface name. If an aggregated interface already exists, then the field is displayed as read-only.</td>
</tr>
<tr>
<td>LACP Mode</td>
<td>Specifies the mode in which LACP packets are exchanged between the interfaces. The modes are:</td>
<td>Select from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td>■ None—Indicates that no mode is applicable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Active—Indicates that the interface initiates transmission of LACP packets</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Passive—Indicates that the interface only responds to LACP packets.</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>The description for the LAG.</td>
<td>Enter the description.</td>
</tr>
<tr>
<td>Interface</td>
<td>Indicates that the interfaces available for aggregation.</td>
<td>Click Add to select the interfaces.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Only interfaces that are configured with the same speeds can be selected together for a LAG.</td>
<td></td>
</tr>
<tr>
<td>Speed</td>
<td>Indicates the speed of the interface.</td>
<td></td>
</tr>
<tr>
<td>Enable Log</td>
<td>Specifies whether to enable generation of log entries for LAG.</td>
<td>Select to enable log generation.</td>
</tr>
</tbody>
</table>
Table 174: Edit VLAN Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Mode</td>
<td>Specifies the mode of operation for the port: trunk or access.</td>
<td>If you select Trunk, you can:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Click <strong>Add</strong> to add a VLAN member.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select the VLAN and click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. (Optional) Associate a native VLAN ID with the port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you select Access, you can:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Select the VLAN member to be associated with the port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. (Optional) Associate a VoIP VLAN with the interface. Only a VLAN with a VLAN ID can be associated as a VoIP VLAN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td>VLAN Options</td>
<td>For trunk interfaces, the VLANs for which the interface can carry traffic.</td>
<td>Click <strong>Add</strong> to select VLAN members.</td>
</tr>
<tr>
<td>Native VLAN</td>
<td>VLAN identifier to associate with untagged packets received on the interface.</td>
<td>Select the VLAN identifier.</td>
</tr>
</tbody>
</table>

**Configuring 802.1X Features**

IEEE 802.1X and MAC RADIUS authentication both provide network edge security, protecting Ethernet LANs from unauthorized user access by blocking all traffic to and from devices at the interface until the supplicant’s credential or MAC address is presented and matched on the authentication server (a RADIUS server). When the supplicant is authenticated, the switch stops blocking access and opens the interface to the supplicant.

See the JUNOS Software Documentation for EX Series Switches for detailed examples of configuring 802.1X features.

**Configuring Authentication Features (J-Web)**

To configure 802.1X settings using the J-Web interface:

1. From the **Configure** menu, select **Security > 802.1X**.

   The 802.1X screen displays a list of interfaces, whether 802.1X security has been enabled, and the assigned port role.

   When you select a particular interface, the Details section displays 802.1X details for the selected interface.
NOTE: After you make changes to the configuration, you must commit the changes for them to take effect. To commit all changes to the active configuration, select Commit Options > Commit.

2. Click one:
   - **RADIUS Servers**—specifies the RADIUS server to be used for authentication. Select the check box to select the server. Click Add or Edit to add or modify the RADIUS server settings. Enter information as specified in Table 175 on page 667.
   - **Exclusion List**—implements the authentication bypass option by listing the MAC address of each host to be excluded from 802.1X authentication. Click Add or Edit in the Exclusion list screen to include or modify the MAC address list. Enter information as specified in Table 176 on page 668.
   - **Edit**—specifies 802.1X settings for the selected interface.
     - **Apply 802.1X Profile**—applies a predefined 802.1X profile based on the port role. If a message appears asking if you want to configure a RADIUS server, click Yes and enter information as specified in Table 175 on page 667.
     - **802.1X Configuration**—configures custom 802.1X settings for the selected interface. If a message appears asking if you want to configure a RADIUS server, click Yes and enter information as specified in Table 175 on page 667. To configure 802.1X settings, enter information as specified in Table 177 on page 668.
     - **Delete**—deletes the existing 802.1X authentication configuration on the selected interface.

### Table 175: RADIUS Server Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Specifies the IP address of the server.</td>
<td>Enter the IP address in dotted decimal notation.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the login password.</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Verifies the login password for the server.</td>
<td>Reenter the password.</td>
</tr>
<tr>
<td>Server Port Number</td>
<td>Specifies the port with which the server is associated.</td>
<td>Type the port number.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Specifies the source address of the SRX Series device for communicating with the server.</td>
<td>Type the IP address in dotted decimal notation.</td>
</tr>
<tr>
<td>Retry Attempts</td>
<td>Specifies the number of login retries allowed after a login failure.</td>
<td>Type the number.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Specifies the time interval to wait before the connection to the server is closed.</td>
<td>Type the interval in seconds.</td>
</tr>
</tbody>
</table>
### Table 176: 802.1X Exclusion List

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Specifies the MAC address to be excluded from 802.1X authentication.</td>
<td>Enter the MAC address.</td>
</tr>
<tr>
<td>Exclude if connected</td>
<td>Specifies that a supplicant can bypass authentication if it is connected through a particular interface.</td>
<td>Select to enable the option. Select the port through which the supplicant is connected.</td>
</tr>
<tr>
<td>through the port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Move the host to the VLAN</td>
<td>Moves the host to a specific VLAN once the host is authenticated.</td>
<td>Select to enable the option. Select the VLAN from the list.</td>
</tr>
</tbody>
</table>

### Table 177: 802.1X Port Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplicant Mode</td>
<td>Specifies the mode to be adopted for supplicants:</td>
<td>Select the required mode.</td>
</tr>
<tr>
<td></td>
<td>■ Single—allows only one host for authentication.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Multiple—allows multiple hosts for authentication. Each host is checked before being admitted to the network.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Single authentication for multiple hosts—allows multiple hosts but only the first is authenticated.</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>Specifies enabling reauthentication on the selected interface.</td>
<td>Select to enable reauthentication. Enter the timeout for reauthentication in seconds.</td>
</tr>
<tr>
<td>Enable re-authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action for nonresponsive hosts</td>
<td>Specifies the action to be taken in case a supplicant is non-responsive:</td>
<td>Select the desired action.</td>
</tr>
<tr>
<td></td>
<td>■ Move to the Guest VLAN—moves the supplicant to the specified Guest VLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Deny—does not permit access to the supplicant.</td>
<td></td>
</tr>
<tr>
<td>Timeouts</td>
<td>Specifies timeout values for:</td>
<td>Enter timeout values in seconds for the appropriate options.</td>
</tr>
<tr>
<td></td>
<td>■ Port waiting time after an authentication failure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ EAPOL re-transmitting interval</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Maximum EAPOL requests</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Maximum number of retries</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Port timeout value for a response from the supplicant</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Port timeout value for a response from the RADIUS server</td>
<td></td>
</tr>
</tbody>
</table>
Specifying RADIUS Server Connections on an SRX Series or J Series Device (CLI)

To use 802.1X or MAC RADIUS authentication, you must specify the connections on the SRX Series or J Series device for each RADIUS server to which you will connect.

To configure a RADIUS server:

1. Navigate to the access hierarchy and define the RADIUS server by its IP address and secret password. The secret password on the SRX Series or J Series device must match the secret password on the server.

   ```
   [edit]
   user@host# edit access
   [edit access]
   user@host# set radius-server 10.0.0.100 port 1812 secret abc
   ```

   To define more than one RADIUS server, you need to enter separate `radius-server` commands.

2. (Optional) Specify the IP address that the RADIUS server uses to identify the SRX Series or J Series device.

   By default, the RADIUS server uses the address of the interface sending the RADIUS request to determine the source of a request. If the request has been diverted on an alternate route to the RADIUS server, however, the interface relaying the request might not be an interface on the SRX Series or J Series device. To ensure that the source is identified correctly, specify its IP address explicitly.

   ```
   [edit access]
   user@host# set radius-server 10.0.0.100 source-address 10.93.14.100
   ```

3. Create a profile and configure the authentication order, making `radius` the first method of authentication.

   ```
   [edit access]
   user@host# set profile profile1 authentication-order radius
   ```

4. Specify one or more RADIUS servers to be associated with profile1.

   ```
   [edit access]
   user@host# set profile profile1 radius authentication-server 10.0.0.100
   ```

5. Navigate to the top of the hierarchy and define profile1 as the authentication profile for 802.1X or MAC RADIUS authenticator.

   ```
   [edit access]
   user@host# top
   ```
6. Configure the IP address of the SRX Series or J Series device in the list of clients on the RADIUS server. For specifics on configuring the RADIUS server, consult the documentation for your server.

**Configuring 802.1X Interface Settings (CLI)**

To configure 802.1X authentication on an interface:

1. Navigate to the [edit protocols dot1x] hierarchy and configure the supplicant mode as single (authenticates the first supplicant), single-secure (authenticates only one supplicant), or multiple (authenticates multiple supplicants).

   ```
   [edit]
   user@host# edit protocols dot1x
   [edit protocols dot1x]
   user@host# set authenticator interface ge-0/0/5 supplicant multiple
   ```

2. Enable reauthentication and specify the reauthentication interval.

   ```
   [edit protocols dot1x]
   user@host# set authenticator interface ge-0/0/5/0 reauthentication 120
   ```

3. Configure the interface timeout value for the response from the supplicant.

   ```
   [edit protocols dot1x]
   user@host# set authenticator interface ge-0/0/5 supplicant-timeout 5
   ```

4. Configure the timeout for the interface before it resends an authentication request to the RADIUS server.

   ```
   [edit protocols dot1x]
   user@host# set authenticator interface ge-0/0/5 server-timeout 5
   ```

5. Configure how long, in seconds, the interface waits before retransmitting the initial EAPOL PDUs to the supplicant.

   ```
   [edit protocols dot1x]
   user@host# set authenticator interface ge-0/0/5 transmit-period 60
   ```

6. Configure the maximum number of times an EAPOL request packet is retransmitted to the supplicant before the authentication session times out.

   ```
   [edit protocols dot1x]
   user@host# set authenticator interface ge-0/0/5 maximum-requests 5
   ```

**Example: Configuring a Guest VLAN (CLI)**

802.1X provides LAN access to nonresponsive hosts (hosts where 802.1X is not enabled). These hosts, referred to as guests, typically are provided access only to the Internet.

To create a guest VLAN and to verify the configuration:
1. Configure a VLAN named visitor-vlan.

   [edit]
   user@host# set vlans visitor-vlan vlan-id 300

2. Navigate to the top of the hierarchy to configure visitor-vlan as the guest VLAN.

   top
   [edit]
   user@host# set protocols dot1x authenticator interface all guest-vlan
   visitor-vlan

3. Check the configuration.

   [edit]
   user@host> show configuration

   protocols {
     dot1x {
       authenticator {
         interface {
           all {
             guest-vlan {
               visitor-vlan;
             }
           }
         }
       }
     }
   }

   vlans {
     visitor-vlan {
       vlan-id 300;
     }
   }

4. If you are finished configuring the VLAN, commit the configuration.

---

**Configuring IGMP Snooping—Quick Configuration**

IGMP snooping regulates multicast traffic in a switched network. With IGMP snooping enabled, the Juniper device monitors the IGMP transmissions between a host (a network device) and a multicast router, keeping track of the multicast groups and associated member interfaces. The Juniper device uses that information to make intelligent multicast-forwarding decisions and forward traffic to the intended destination interfaces.

You can use the J-Web Quick Configuration to add a new IGMP snooping configuration or to edit or delete an existing configuration.

To access the IGMP Snooping Quick Configuration:

1. In the J-Web user interface, select **Configure > Switching > IGMP Snooping**.
The VLAN Configuration page displays a list of existing IGMP snooping configurations.

2. Click one:
   - **Add**—Creates an IGMP snooping configuration for the VLAN.
   - **Edit**—Edits an existing IGMP snooping configuration for the VLAN.
   - **Delete**—Deletes member settings for the interface.

   **NOTE:** If you delete a configuration, the VLAN configuration for all the associated interfaces is also deleted.

- **Disable Vlan**—Disables IGMP snooping on the selected VLAN.

When you are adding or editing a VLAN, enter information as described in Table 178 on page 672.

3. Click one:
   - To apply changes to the configuration, click **OK**.
   - To cancel the configuration without saving changes, click **Cancel**.

### Table 178: IGMP Snooping Configuration Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Name</td>
<td>Specifies the VLAN on which to enable IGMP snooping</td>
<td>Select the VLAN from the list.</td>
</tr>
<tr>
<td>Immediate Leave</td>
<td>Immediately removes a multicast group membership from an interface when it receives a leave message from that interface and suppresses the sending of any group-specific queries for the multicast group</td>
<td>To enable the option, select the check box.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To disable the option, clear the check box.</td>
</tr>
<tr>
<td>Query Interval</td>
<td>Configures how frequently the switch sends host-query timeout messages to a multicast group.</td>
<td>Enter a value from 1 through 1024 seconds.</td>
</tr>
<tr>
<td>Query Last Member Interval</td>
<td>Configures the interval between group-specific query timeout messages sent by the switch.</td>
<td>Enter a value from 1 through 1024 seconds.</td>
</tr>
<tr>
<td>Query Response Interval</td>
<td>Configures the length of time the switch waits to receive a response to a specific query message from a host.</td>
<td>Enter a value from 1 through 25 seconds.</td>
</tr>
<tr>
<td>Robust Count</td>
<td>Specifies the number of timeout intervals the switch waits before timing out a multicast group.</td>
<td>Enter a value from 2 through 10.</td>
</tr>
</tbody>
</table>
Table 178: IGMP Snooping Configuration Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces List</td>
<td>Statically configures an interface as a switching interface toward a multicast router (the interface to receive multicast traffic).</td>
<td>1. Click Add.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Select an interface from the list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Select Multicast Router Interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Enter the maximum number of groups an interface can join in Group Limit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. In Static, choose one:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Click Add, type a group IP address, and click OK.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Select a group and click Remove to remove the group membership.</td>
</tr>
</tbody>
</table>

Configuring GVRP—Quick Configuration

As a network expands and the number of clients and VLANs increases, VLAN administration becomes complex, and the task of efficiently configuring VLANs on multiple EX Series switches becomes increasingly difficult. To automate VLAN administration, you can enable GARP VLAN Registration Protocol (GVRP) on the network.

GVRP learns VLANs on a particular 802.1Q trunk port, and adds the corresponding trunk interface to the VLAN if the advertised VLAN is preconfigured or existing already on the switch. For example, a VLAN named “sales” is advertised to trunk interface 1 on the GVRP-enabled switch. The switch adds trunk interface 1 to the sales VLAN if the sales VLAN already exists on the switch.

As individual interfaces become active and send requests to join a VLAN, the VLAN configuration is updated and propagated among the switches. Limiting the VLAN configuration to active participants reduces the network overhead. GVRP also provides the benefit of pruning VLANs to limit the scope of broadcast, unknown unicast, and multicast (BUM) traffic to interested network devices only.

You can use the J-Web Quick Configuration to enable or disable GVRP on an interface.

To access the GVRP Quick Configuration:

1. In the J-Web user interface, select Configure > Switching > GVRP.

   The GVRP Configuration page displays a list of interfaces on which GVRP is enabled.

2. Click one:

   ■ Global Settings—Modifies GVRP timers. Enter the information as described in Table 179 on page 674.

   ■ Add—Enables GVRP on an interface.
- **Disable Port**—Disables an interface.
- **Delete**—Deletes an interface.

3. Click one:
- To apply changes to the configuration, click **OK**.
- To cancel the configuration without saving changes, click **Cancel**.

### Table 179: GVRP Global Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable GVRP</td>
<td>Disables GVRP on all the interfaces.</td>
<td>Click to select.</td>
</tr>
<tr>
<td>Join Timer</td>
<td>Specifies the number of milliseconds an interface must wait before sending VLAN advertisements.</td>
<td>Enter a value from 0 through 4294967295 milliseconds.</td>
</tr>
<tr>
<td>Leave Timer</td>
<td>Specifies the number of milliseconds an interface must wait after receiving a leave message to remove itself from the VLAN specified in the message.</td>
<td>Enter a value from 0 through 4294967295 milliseconds.</td>
</tr>
<tr>
<td>Leave All Timer</td>
<td>Specifies the interval in milliseconds at which Leave All messages are sent on interfaces. Leave All messages help to maintain current GVRP VLAN membership information in the network.</td>
<td>Enter a value from 0 through 4294967295 milliseconds.</td>
</tr>
</tbody>
</table>
For SRX3400, SRX3600, SRX5600, and SRX5800 devices, transparent mode provides
full security services for Layer 2 bridging capabilities. This chapter describes how to
configure bridge domains on SRX Series devices and how to configure Layer 2 security
zones and security policies between these zones.

For information about which devices support the features documented in this chapter,
see the Junos OS Feature Support Reference for SRX Series and J Series Devices.

This chapter contains the following topics:

■ Layer 2 Bridging and Transparent Mode Overview on page 676
■ Understanding Bridge Domains on page 677
■ Understanding Transparent Mode Conditions on page 679
■ Understanding Layer 2 Interfaces on page 680
■ Configuring Bridge Domains on page 680
■ Configuring Layer 2 Logical Interfaces on page 682
■ Understanding Layer 2 Security Zones on page 684
■ Understanding Security Policies in Transparent Mode on page 685
■ Creating Layer 2 Security Zones on page 686
■ Configuring Security Policies for Transparent Mode on page 687
■ Understanding VLAN Retagging on page 689
■ Configuring VLAN Retagging on page 690
■ Changing the Default Forwarding Behavior on page 691
■ Understanding Integrated Routing and Bridging Interfaces on page 692
■ Understanding Firewall User Authentication in Transparent Mode on page 693
■ Configuring an IRB Interface on page 694
■ Understanding Layer 2 Forwarding Tables on page 696
■ Changing the Default Learning for Unknown MAC Addresses on page 698
■ Understanding Layer 2 Transparent Mode Chassis Clusters on page 699
■ Configuring Redundant Ethernet Interfaces for Layer 2 Transparent Mode Chassis
  Clusters on page 700
Layer 2 Bridging and Transparent Mode Overview

On SRX3400, SRX3600, SRX5600, and SRX5800 devices, you can configure one or more bridge domains to perform Layer 2 bridging. A bridge domain is a set of logical interfaces that share the same flooding or broadcast characteristics. Like a virtual LAN (VLAN), a bridge domain spans one or more ports of multiple devices. Thus, the SRX Series device can function as a Layer 2 switch with multiple bridge domains that participate in the same Layer 2 network.

In transparent mode, the SRX Series device filters packets that traverse the device without modifying any of the source or destination information in the IP packet headers. Transparent mode is useful for protecting servers that mainly receive traffic from untrusted sources because there is no need to reconfigure the IP settings of routers or protected servers.

NOTE: Transparent mode is supported only for IPv4 traffic.

In transparent mode, all physical ports on the device are assigned to Layer 2 interfaces. Do not route Layer 3 traffic through the device. Layer 2 zones can be configured to host Layer 2 interfaces, and security policies can be defined between Layer 2 zones. When packets travel between Layer 2 zones, security policies can be enforced on these packets.

NOTE: Not all security features are supported in transparent mode:
- NAT is not supported.
- IPsec VPN is not supported.
- Only DNS, FTP, RTSP, and TFTP ALGs are supported. Other ALGs are not supported in this release.

Related Topics
- Understanding Bridge Domains on page 677
- Understanding Transparent Mode Conditions on page 679
Understanding Bridge Domains

The packets that are forwarded within a bridge domain are determined by the VLAN ID of the packets and the VLAN ID of the bridge domain. Only the packets with VLAN IDs that match the VLAN ID configured for a bridge domain are forwarded within the bridge domain.

When configuring bridge domains, you can specify either a single VLAN ID or a list of specific VLAN IDs. If you specify a list of VLAN IDs, a bridge domain is created for each VLAN ID in the list. Certain bridge domain properties, such as the integrated routing and bridging interface (IRB), are not configurable if bridge domains are created in this manner (see “Understanding Integrated Routing and Bridging Interfaces” on page 692).

Each Layer 2 logical interface configured on the device is implicitly assigned to a bridge domain based on the VLAN ID of the packets accepted by the interface (see “Understanding Layer 2 Interfaces” on page 680). You do not need to explicitly define the logical interfaces when configuring a bridge domain.

You can configure one or more static MAC addresses for a logical interface in a bridge domain; this is only applicable if you specified a single VLAN ID when creating the bridge domain.

**NOTE:** If a static MAC address you configure for a logical interface appears on a different logical interface, packets sent to that interface are dropped.

You can configure the following properties that apply to all bridge domains on the SRX Series device:

- Disable or enable Layer 2 address learning. Layer 2 address learning is enabled by default. A bridge domain learns unicast media access control (MAC) addresses to avoid flooding packets to all interfaces in the bridge domain. Each bridge domain creates a source MAC entry in its forwarding tables for each source MAC address learned from packets received on interfaces that belong to the bridge domain. When you disable MAC learning, source MAC addresses are not dynamically learned, and any packets sent to these source addresses are flooded into a bridge domain.

- Maximum number of MAC addresses learned from all logical interfaces on the SRX Series device. After the MAC address limit is reached, the default is for any incoming packets with a new source MAC address to be forwarded. You can specify that the packets be dropped instead. The default limit is 131,071 MAC addresses. The range that you can configure is 16 through 131,071.

- Timeout interval for MAC table entries. By default, the timeout interval for MAC table entries is 300 seconds. The minimum you can configure is 10 seconds and the maximum is 64,000 seconds. The timeout interval applies only to dynamically learned MAC addresses. This value does not apply to configured static MAC addresses, which never time out.
Layer 2 Bridging Exceptions on SRX Series Devices

The bridging functions on the SRX3400, SRX3600, SRX5600, and SRX5800 devices are similar to the bridging features on Juniper Networks MX Series routers. However, the following Layer 2 networking features on MX Series routers are not supported on SRX Series devices:

- **Layer 2 control protocols**—These protocols are used on MX Series routers for Rapid Spanning Tree Protocol (RSTP) or Multiple Spanning Tree Protocol (MSTP) in customer edge interfaces of a VPLS routing instance.
- **Virtual switch routing instance**—The virtual switching routing instance is used on MX Series routers to group one or more bridge domains.
- **Virtual private LAN services (VPLS) routing instance**—The VPLS routing instance is used on MX Series routers for point-to-multipoint LAN implementations between a set of sites in a VPN.

In addition, the SRX Series devices do not support the following Layer 2 features:

- **Spanning Tree Protocol (STP), RSTP, or MSTP**—It is the user’s responsibility to ensure that no flooding loops exist in the network topology.
- **Internet Group Management Protocol (IGMP) snooping**
- **Double-tagged VLANs, or IEEE 802.1Q VLAN identifiers encapsulated within 802.1Q packets** (also called “Q in Q” VLAN tagging)—Only untagged or single-tagged VLAN identifiers are supported on SRX Series devices.
- **Nonqualified VLAN learning**, where only the MAC address is used for learning within the bridge domain—VLAN learning on SRX Series devices is qualified; that is, both the VLAN identifier and MAC address are used.

Layer 2 Bridging Terms

Before configuring Layer 2 bridge domains, become familiar with the terms defined in Table 180 on page 678.

Table 180: Layer 2 Bridging Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access interface</td>
<td>Logical Layer 2 interface configured to accept untagged packets and to assign a specified VLAN ID to the packets.</td>
</tr>
<tr>
<td>Bridge</td>
<td>A network component defined by the IEEE that forwards frames from one LAN segment or VLAN to another. This bridging function can be contained in a router, LAN switch, or other specialized device.</td>
</tr>
<tr>
<td>Bridge domain</td>
<td>A set of logical interfaces that share the same flooding or broadcast characteristics. As in a VLAN, a bridge domain spans one or more ports of multiple devices. By default, each bridge domain maintains its own forwarding database of MAC addresses learned from packets received on interfaces that belong to that bridge domain.</td>
</tr>
</tbody>
</table>
Table 180: Layer 2 Bridging Terms (continued)

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding Information Base (FIB)</td>
<td>JUNOS Software forwarding information base (also called the forwarding table). The JUNOS routing protocol process installs active routes from its routing tables into the Routing Engine forwarding table. The kernel copies this forwarding table into the Packet Forwarding Engine, which determines the interface that transmits the packets.</td>
</tr>
<tr>
<td>Integrated routing and bridging (IRB) interface</td>
<td>Pseudointerface that contains both routing domain and bridge domain and facilitates simultaneous Layer 2 bridging and Layer 3 routing within the same bridge domain. Packets arriving on an interface of the bridge domain are switched or routed based on the destination MAC address. Packets addressed to the router’s MAC address are routed to other Layer 3 interfaces.</td>
</tr>
<tr>
<td>Learning domain</td>
<td>A MAC address database in the bridge domain where the MAC addresses are added based on VLAN tags.</td>
</tr>
<tr>
<td>Trunk interface</td>
<td>Logical Layer 2 interface that accepts any packets tagged with a VLAN ID that matches a specified list of VLAN IDs.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Defines a broadcast domain, a set of logical ports that share flooding or broadcast characteristics. VLANs span one or more ports on multiple devices. By default, each VLAN maintains its own Layer 2 forwarding database containing MAC addresses learned from packets received on ports belonging to the VLAN.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring Bridge Domains on page 680
- Understanding Integrated Routing and Bridging Interfaces on page 692
- Understanding Layer 2 Forwarding Tables on page 696

**Understanding Transparent Mode Conditions**

A device operates in Layer 2 transparent mode when all physical interfaces on the device are configured as Layer 2 interfaces. A physical interface is a Layer 2 interface if its logical interface is configured with the bridge family.

There is no command to define or enable transparent mode on the device. The device operates in transparent mode when there are interfaces defined as Layer 2 interfaces. The device operates in route mode (the default mode) if there are no physical interfaces configured as Layer 2 interfaces.

**NOTE:** In this release, the SRX Series device can operate at either route mode or transparent mode, but not both modes at the same time. Changing the mode requires a reboot of the device.

You can configure the fxp0 out-of-band management interface on the SRX Series device as a Layer 3 interface, even if Layer 2 interfaces are defined on the device. With the exception of the fxp0 interface, you must not define Layer 2 and Layer 3 interfaces on the device’s network ports.
Related Topics

- Understanding Layer 2 Interfaces on page 680

Understanding Layer 2 Interfaces

Layer 2 logical interfaces are created by defining one or more logical units on a physical interface with the family address type bridge. If a physical interface has a bridge family logical interface, it cannot have any other family type in its logical interfaces. A logical interface can be configured in one of the following modes:

- **Access mode**—Interface accepts untagged packets, assigns the specified VLAN identifier to the packet, and forwards the packet within the bridge domain that is configured with the matching VLAN identifier.

- **Trunk mode**—Interface accepts any packet tagged with a VLAN identifier that matches a specified list of VLAN identifiers. Trunk mode interfaces are generally used to interconnect switches. To configure a VLAN identifier for untagged packets received on the physical interface, use the `native-vlan-id` option. If the `native-vlan-id` option is not configured, untagged packets are dropped.

  Tagged packets arriving on a trunk mode interface can be rewritten or “retagged” with a different VLAN identifier. This allows incoming packets to be selectively redirected to a firewall or other security device. For more information, see “Understanding VLAN Retagging” on page 689.

**NOTE:** Multiple trunk mode logical interfaces can be defined, as long as the VLAN identifiers of a trunk interface do not overlap with those of another trunk interface. The `native-vlan-id` must belong to a VLAN identifier list configured for a trunk interface.

Related Topics

- Configuring Layer 2 Logical Interfaces on page 682

Configuring Bridge Domains

To configure a bridge domain, you must specify one or more VLAN identifiers; only packets that contain a specified VLAN identifier are forwarded within the bridge domain. A logical interface is implicitly assigned to a bridge domain based on the VLAN identifier configured for the interface.

**Before You Begin**

For background information, read “Understanding Bridge Domains” on page 677.
This example configures a bridge domain bd1 for VLANs 1 and 10, and a bridge domain bd2 for VLAN 2. The number of MAC addresses learned on all logical interfaces on the device is limited to 64,000 addresses; when this limit is reached, incoming packets with a new source MAC address will be dropped.

You can use either J-Web or the CLI configuration editor to configure bridge domains.

This topic covers:
- J-Web Configuration on page 681
- CLI Configuration on page 682
- Related Topics on page 682

**J-Web Configuration**

To configure bridge domains:
1. Select Configure > CLI Tools > Point and Click CLI.
   The Configuration page appears.
2. Next to Bridge domains, click Configure or Edit.
3. Next to Domain, click Add new entry.
4. In the Domain name box, type bd1.
5. Next to Domain type, select bridge.
6. Next to Vlan choice, select Vlan id list.
7. In the Vlan id box, type 1,10.
8. Click OK to return to the Configuration page.
9. Select Bridge domains.
10. Next to Domain, click Add new entry.
11. In the Domain box, type bd2
12. Next to Domain type, select bridge.
13. Next to Vlan choice, select Vlan id.
14. Next to Vlan id, select Enter a specific value.
15. In the Vlan id box, type 2.
16. Click OK to return to the Configuration page.

To limit the number of MAC addresses learned on all logical interfaces on the device:
1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Protocols, click Configure or Edit.
3. Next to L2 learning, click Configure.
4. Select Global mac limit, then click Configure.
5. In the Mac limit box, type 64000.
6. Next to packet action, select **Drop**.
7. Click **OK** to return to the L2 learning page.
8. Click **OK** to return to the Protocols page.
9. Click **OK** to return to the Configuration page.

**CLI Configuration**

To configure bridge domains:

```
user@host# set bridge-domains bd1 domain-type bridge vlan-id-list 1,10
user@host# set bridge-domains bd2 domain-type bridge vlan-id 2
```

To limit the number of MAC addresses learned on all logical interfaces on the device:

```
user@host# set protocols l2-learning global-mac-limit 64000 packet-action drop
```

**Related Topics**

- Configuring Layer 2 Logical Interfaces on page 682
- Configuring an IRB Interface on page 694

**Configuring Layer 2 Logical Interfaces**

To configure a Layer 2 logical interface as an access interface, you must specify the VLAN identifier that the interface assigns to untagged packets. To configure a Layer 2 logical interface as a trunk interface, you specify one or more VLAN identifiers accepted by the interface.

**Before You Begin**

For background information, read “Understanding Layer 2 Interfaces” on page 680. Refer to the example configuration in “Configuring Bridge Domains” on page 680.

This example configures logical interface `ge-3/0/0.0` as a trunk port that carries traffic for packets tagged with VLAN identifiers 1 through 10; this interface is implicitly assigned to the previously configured bridge domains `bd1` and `bd2`. Any untagged packets received on the physical interface `ge-3/0/0` are assigned the VLAN identifier 10.

You can use either J-Web or the CLI configuration editor to configure Layer 2 logical interfaces.
This topic covers:

- J-Web Configuration on page 683
- CLI Configuration on page 683
- Related Topics on page 684

**J-Web Configuration**

To configure a Layer 2 logical interface as a trunk port:

1. Select **Configure > CLI Tools > Point and Click CLI**.
2. Next to Interfaces, click **Configure** or **Edit**.
3. In the Interface name column, select **ge-3/0/0**.
4. Under Unit, in the Interface unit number column, click **0**.
5. Next to Family group, select **Bridge** and then click **Configure**.
6. Next to Interface mode, select **trunk**.
7. Next to Vlan list, select **Vlan id list**.
8. In the Vlan id box, type **1–10**.
9. Click **OK** to return to the Family page.
10. Click **OK** to return to the Unit page.
11. Click **OK** to return to the Interface page.
12. Click **OK** to return to the Interfaces page.

To configure a VLAN ID for untagged packets received on a physical interface:

1. Select **Configure > CLI Tools > Point and Click CLI**.
2. Next to Interfaces, click **Configure** or **Edit**.
3. In the Interface name column, select **ge-3/0/0**.
4. In the Native vlan id box, type **10**.
5. Next to Vlan tag mode, select **Vlan tagging**.
6. Click **OK** to return to the Interfaces page.

**CLI Configuration**

To configure a Layer 2 logical interface as a trunk port:

```
user@host# set interfaces ge-3/0/0 unit 0 family bridge interface-mode trunk vlan-id-list 1–10
```

To configure a VLAN identifier for untagged packets received on a physical interface:

```
user@host# set interfaces ge-3/0/0 vlan-tagging native-vlan-id 10
```
Understanding Layer 2 Security Zones

A Layer 2 security zone is a zone that hosts Layer 2 interfaces. A security zone can be either a Layer 2 or Layer 3 zone; it can host either all Layer 2 interfaces or all Layer 3 interfaces, but it cannot contain a mix of Layer 2 and Layer 3 interfaces.

The security zone type—Layer 2 or Layer 3—is implicitly set from the first interface configured for the security zone. Subsequent interfaces configured for the same security zone must be the same type as the first interface.

**NOTE:** In this release, you cannot configure a device with both Layer 2 and Layer 3 security zones.

You can configure the following properties for Layer 2 security zones:

- Interfaces—List of interfaces in the zone.
- Policies—Active security policies that enforce rules for the transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on the traffic as it passes through the firewall.
- Screens—A Juniper Networks stateful firewall secures a network by inspecting, and then allowing or denying, all connection attempts that require passage from one security zone to another. For every security zone, and the MGT zone, you can enable a set of predefined screen options that detect and block various kinds of traffic that the device determines as potentially harmful.

**NOTE:** You can configure the same screen options for a Layer 2 security zone as for a Layer 3 security zone, with the exception of IP spoofing. Detection of IP spoofing is not supported on Layer 2 security zones. For more information about configuring screen options, see the *Junos OS Security Configuration Guide*.

- Address books—IP addresses and address sets that make up an address book to identify its members so that you can apply policies to them.
- TCP-RST—When this feature is enabled, the system sends a TCP segment with the reset flag set when traffic arrives that does not match an existing session and does not have the synchronize flag set.

In addition, you can configure a Layer 2 zone for host-inbound traffic. This allows you to specify the kinds of traffic that can reach the device from systems that are directly connected to the interfaces in the zone. You must specify all expected...
host-inbound traffic because inbound traffic from devices directly connected to the device's interfaces is dropped by default.

For more information about security zones and configuring security zone properties, see the *Junos OS Security Configuration Guide*.

**Related Topics**

- Creating Layer 2 Security Zones on page 686
- Configuring Layer 2 Logical Interfaces on page 682

**Understanding Security Policies in Transparent Mode**

In transparent mode, security policies can be configured only between Layer 2 zones. When packets are forwarded through the bridge domain, the security policies are applied between security zones. A security policy for transparent mode is similar to a policy configured for Layer 3 zones, with the following exceptions:

- NAT is not supported.
- IPsec VPN is not supported.
- Junos-H323 ALGs and IDP are not supported.
- Application ANY is used.

Layer 2 forwarding does not permit any interzone traffic unless there is a policy explicitly configured on the device. By default, Layer 2 forwarding performs the following actions:

- Allows or denies traffic specified by the configured policy.
- Allows Address Resolution Protocol (ARP) and Layer 2 non-IP multicast and broadcast traffic. The device can receive and pass Layer 2 broadcast traffic for STP.
- Continues to block all non-IP and non-ARP unicast traffic.

This default behavior can be changed for bridge packet flow by using either J-Web or the CLI configuration editor:

- Configure the `block-non-ip-all` option to block all Layer 2 non-IP and non-ARP traffic, including multicast and broadcast traffic.
- Configure the `bypass-non-ip-unicast` option to allow all Layer 2 non-IP traffic to pass through the device.

**NOTE:** You cannot configure both options at the same time.

For more information about security policies, see *Junos OS Security Configuration Guide*.
Creating Layer 2 Security Zones

A Layer 2 security zone is a zone that hosts Layer 2 interfaces.

**Before You Begin**

For background information, read “Understanding Layer 2 Security Zones” on page 684.

This example configures the security zone `l2-zone1` to include the previously configured Layer 2 logical interface `ge-3/0/0.0` and security zone `l2-zone2` to include the Layer 2 logical interface `ge-3/0/1.0`. In addition, `l2-zone2` is configured to allow all supported application services (such as SSH, Telnet, SNMP, and other services) as host-inbound traffic.

You can use either J-Web or the CLI configuration editor to configure Layer 2 security zones.

This topic covers:

- J-Web Configuration on page 686
- CLI Configuration on page 687
- Related Topics on page 687

**J-Web Configuration**

To create a Layer 2 security zone:

1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Security, click Configure or Edit.
3. Next to Zones, click Configure.
4. Next to Security zone, click Add new entry.
5. In the Name box, type `l2-zone1`, and then click OK to return to the Security Zones page.

To create a Layer 2 security zone and allow host-bound traffic:

1. Next to Security zone, click Add new entry.
2. In the Name box, type `l2-zone2`.
3. Next to Host inbound traffic, click Configure.
4. To allow the security zone to use all supported application services, next to System services, click **Add new entry**.

5. From the Service name list, select **All**, and then click **OK**.

6. Click **OK** to return to the Security Zones page.

To configure an interface and assign it to the created security zone:

1. On the Security Zones page, next to the newly created security zone l2–zone1, click **Edit**.

2. Next to Interfaces, click **Add new entry**.

3. In the Interface unit box, type `ge-3/0/0.0`, and then click **OK** to return to the Security Zones page.

4. Next to the newly created security zone l2–zone2, click **Edit**.

5. Next to Interfaces, click **Add new entry**.

6. In the Interface unit box, type `ge-3/0/1.0`, and then click **OK** to return to the Security Zones page.

7. Click **OK** to return to the Zones page.

8. Click **OK** to return to the Security page.

**CLI Configuration**

To create a Layer 2 security zone and assign interfaces to the zone:

```shell
user@host# set security zones security-zone l2–zone1 interfaces ge-3/0/0.0
user@host# set security zones security-zone l2–zone2 interfaces ge-3/0/1.0
```

To configure a Layer 2 security zone to allow host-inbound traffic:

```shell
user@host# set security zones security-zone l2–zone2 host-inbound-traffic system-services all
```

**Related Topics**

- Configuring Layer 2 Logical Interfaces on page 682
- Configuring Security Policies for Transparent Mode on page 687

**Configuring Security Policies for Transparent Mode**

In transparent mode, security policies can be configured only between Layer 2 zones.

**Before You Begin**

For background information, read “Understanding Security Policies in Transparent Mode” on page 685.
This example configures a security policy to allow HTTP traffic from the 10.1.1.1/24 subnetwork in the l2–zone1 security zone to the server at 20.1.1.1/32 in l2–zone2.

You can use either J-Web or the CLI configuration editor to configure Layer 2 security zones.

This topic covers:
- J-Web Configuration on page 688
- CLI Configuration on page 689
- Related Topics on page 689

**J-Web Configuration**

To configure Layer 2 security policies:
1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Security, select Configure or Edit.
3. Next to Policy, select the check box, and then click Configure.
4. Next to Policy, click Add new entry.
5. In the From zone name box, type l2–zone1.
6. In the To zone name box, type l2–zone2.
7. Next to Policy, click Add new entry.
8. In the Policy name box, type p1.
9. Select the Match check box, then click Configure.
10. From the Source address choice list, select Source address.
11. Next to Source address, click Add new entry.
12. From the Value keyword list, select Enter specific value.
13. In the Address box, type 10.1.1.1/24, and then click OK.
14. From the Destination address choice list, select Destination address.
15. Next to Destination address, click Add new entry.
16. In the Value keyword list, select Enter specific value.
17. In the Address box, type 20.1.1.1/32, and then click OK.
18. To match the policy to an application set name, from the Application choice list, select Application.
19. Next to Application, click Add new entry.
20. To specify the application set name to match the policy, in the Value keyword list box type http, and then click OK.
21. Select the Then check box, and then click Configure.
22. From the Action list, select Permit, and then click OK.
**CLI Configuration**

To configure Layer 2 security policies:

```
user@host# set security policies from-zone l2-zone1 to-zone l2-zone2 policy p1
    match source-address 10.1.1.1/24
user@host# set security policies from-zone l2-zone1 to-zone l2-zone2 policy p1
    match destination-address 20.1.1.1/32
user@host# set security policies from-zone l2-zone1 to-zone l2-zone2 policy p1
    match application http
user@host# set security policies from-zone l2-zone1 to-zone l2-zone2 policy p1
    then permit
```

**Related Topics**

- Changing the Default Forwarding Behavior on page 691

**Understanding VLAN Retagging**

The VLAN identifier in packets arriving on a Layer 2 trunk port can be rewritten or “retagged” with a different internal VLAN identifier. VLAN retagging is a symmetric operation; upon exiting the same trunk port, the retagged VLAN identifier is replaced with the original VLAN identifier. VLAN retagging provides a way to selectively screen incoming packets and redirect them to a firewall or other security device without affecting other VLAN traffic.

VLAN retagging can be applied only to interfaces configured as Layer 2 trunk interfaces. These interfaces can include redundant Ethernet interfaces in a Layer 2 transparent mode chassis cluster configuration.

**NOTE:** If a trunk port is configured for VLAN retagging, untagged packets received on the port cannot be assigned a VLAN identifier with the VLAN retagging configuration. To configure a VLAN identifier for untagged packets received on the physical interface, use the `native-vlan-id` statement.

To configure VLAN retagging for a Layer 2 trunk interface, specify a one-to-one mapping of the following:

- **Incoming VLAN identifier**—VLAN identifier of the incoming packet that is to be retagged. This VLAN identifier must not be the same VLAN identifier configured with the `native-vlan-id` statement for the trunk port.

- **Internal VLAN identifier**—VLAN identifier for the retagged packet. This VLAN identifier must be in the VLAN identifier list for the trunk port and must not be the same VLAN identifier configured with the `native-vlan-id` statement for the trunk port.
Related Topics

- Configuring VLAN Retagging on page 690

Configuring VLAN Retagging

Configuring VLAN retagging on a Layer 2 trunk interface requires a one-to-one mapping of the incoming and internal VLAN identifiers.

Before You Begin

For background information, read:

- Understanding VLAN Retagging on page 689

In the following example, a Layer 2 trunk interface is configured to receive packets with VLAN identifiers 1 through 10. Packets that arrive on the interface with VLAN identifier 11 are retagged with VLAN identifier 2. Before exiting the trunk interface, VLAN identifier 2 in the retagged packets is replaced with VLAN identifier 11.

You can use either J-Web or the CLI configuration editor to configure VLAN retagging.

This topic covers:

- J-Web Configuration on page 690
- CLI Configuration on page 691
- Related Topics on page 691

J-Web Configuration

To create a Layer 2 trunk interface:

1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Interfaces, click Configure or Edit.
3. In the Interface name column, select ge-3/0/0.
4. Under Unit, in the Interface unit number column, click 0.
5. Next to Family group, select Bridge and then click Configure.
6. Next to Interface mode, select trunk.
7. Next to Vlan list, select Vlan id list.
8. In the Vlan id box, type 1–10.

To configure VLAN retagging:
1. Next to Vlan rewrite, click **Configure**.
2. Next to Translate, click **Add new entry**.
3. In the From vlan id box, type **11**.
4. In the To vlan id box, type **2**.
5. Click **OK** to return to the Vlan rewrite page.
6. Click **OK** to return to the Family page.
7. Click **OK** to return to the Unit page.
8. Click **OK** to return to the Interface page.
9. Click **OK** to return to the Interfaces page.

**CLI Configuration**

To create a Layer 2 trunk interface:

```
user@host# set interface ge-3/0/0 unit 0 family bridge interface-mode trunk
vlan-id-list 1–10
```

To configure VLAN retagging:

```
user@host# set interface xe-9/3/0 unit 0 family bridge vlan-rewrite translate 11 2
```

**Related Topics**

- Configuring Layer 2 Logical Interfaces on page 682

**Changing the Default Forwarding Behavior**

By default, Layer 2 forwarding on the device allows or denies traffic specified by the configured policy and allows ARP and Layer 2 non-IP multicast and broadcast traffic. You can configure the device to block all Layer 2 non-IP and non-ARP traffic.

**Before You Begin**

For background information, read “Understanding Security Policies in Transparent Mode” on page 685.

You can use either J-Web or the CLI configuration editor to change the default forwarding behavior on the device.

This topic covers:

- J-Web Configuration on page 692
- CLI Configuration on page 692
- Related Topics on page 692
**J-Web Configuration**

To block all Layer 2 non-IP and non-ARP traffic:
1. Select **Configure > CLI Tools > Point and Click CLI**.
2. Next to Security, click **Configure** or **Edit**.
3. Next to Flow, click **Configure** or **Edit**.
4. Next to Bridge, click **Configure**.
5. Select **Block non ip all**.
6. Click **OK** to return to the Flow page.
7. Click **OK** to return to the Security page.

To allow all Layer 2 non-IP traffic to pass through the device:
1. Select **Configure > CLI Tools > Point and Click CLI**.
2. Next to Security, click **Configure** or **Edit**.
3. Next to Flow, click **Configure** or **Edit**.
4. Next to Bridge, click **Configure**.
5. Select **Bypass non ip unicast**.
6. Click **OK** to return to the Flow page.
7. Click **OK** to return to the Security page.

**CLI Configuration**

To block all Layer 2 non-IP and non-ARP traffic:

```
user@host# set security flow bridge block-non-ip-all
```

To allow all Layer 2 non-IP traffic to pass through the device:

```
user@host# set security flow bridge bypass-non-ip-unicast
```

**Related Topics**

- Configuring Security Policies for Transparent Mode on page 687

**Understanding Integrated Routing and Bridging Interfaces**

For bridge domains configured with a single VLAN identifier, you can optionally configure an integrated routing and bridging (IRB) interface for management traffic in the bridge domain. An IRB interface acts as a Layer 3 routing interface for a bridge domain.
NOTE: If you specify a VLAN identifier list in the bridge domain configuration, you cannot configure an IRB interface for the bridge domain.

In this release, the IRB interface on the SRX Series device does not support traffic forwarding or routing. In transparent mode, packets arriving on a Layer 2 interface that are destined for the device’s MAC address are classified as Layer 3 traffic while packets that are not destined for the device’s MAC address are classified as Layer 2 traffic. Packets destined for the device’s MAC address are sent to the IRB interface. Packets from the device’s routing engine are sent out the IRB interface.

You create an IRB logical interface in a similar manner as a Layer 3 interface, but the IRB interface does not support traffic forwarding or routing. The IRB interface cannot be assigned to a security zone; however, you can configure certain services on a per-zone basis to allow host-inbound traffic for management of the device. This allows you to control the type of traffic that can reach the device from interfaces bound to a specific zone.

NOTE: You can configure only one IRB logical interface for each bridge domain.

To configure an IRB logical interface:

1. Configure a logical interface by using the `irb` interface in the `[edit interfaces]` hierarchy.
2. Reference the IRB logical interface in the bridge domain configuration.

Related Topics

- Configuring an IRB Interface on page 694

Understanding Firewall User Authentication in Transparent Mode

A firewall user is a network user who must provide a username and password for authentication when initiating a connection across the firewall. Firewall user authentication enables administrators to restrict and permit users accessing protected resources behind a firewall based on their source IP address and other credentials. JUNOS Software supports the following types of firewall user authentication for transparent mode on the SRX Series device:

- Pass-through authentication—A host or a user from one zone tries to access resources on another zone. You must use an FTP, Telnet, or HTTP client to access the IP address of the protected resource and be authenticated by the firewall. The device uses FTP, Telnet, or HTTP to collect username and password information, and subsequent traffic from the user or host is allowed or denied based on the result of this authentication.

- Web authentication—Users try to connect, by using HTTP, to an IP address on the IRB interface that is enabled for Web authentication (see “Configuring an
IRB Interface” on page 694). You are prompted for the username and password that are verified by the device. Subsequent traffic from the user or host to the protected resource is allowed or denied based on the result of this authentication.

For information about configuring pass-through or Web authentication, see the *Junos OS Security Configuration Guide*.

**Related Topics**

- Configuring an IRB Interface on page 694

---

**Configuring an IRB Interface**

To configure an IRB interface, you first create an IRB logical interface, and then reference the interface in the bridge domain configuration. Configure a security zone to control the host-inbound traffic from systems that are directly connected to the interfaces in the zone.

---

**NOTE:** An IRB interface can be configured only for a bridge domain defined with a single VLAN identifier. In a previous example, bridge domain bd1 was configured with a VLAN identifier list; you would not be able to add the IRB interface to the bd1 bridge domain.

---

**Before You Begin**

For background information, read “Understanding Integrated Routing and Bridging Interfaces” on page 692 and “Understanding Firewall User Authentication in Transparent Mode” on page 693.

---

In this example, you configure an IRB logical unit 0 with the family type inet and IP address 10.1.1.1/24, and then reference the IRB interface in the bd2 bridge domain configuration. This example also enables Web authentication on the IRB interface and actives the webserver on the device.

**NOTE:** To complete the Web authentication configuration, you will also need to define the following:

- Access profile and password for a Web authentication client
- Security policy that enables Web authentication for the client

Either the local database or an external authentication server can be used as the Web authentication server. For more information about configuring Web authentication, see the *Junos OS Security Configuration Guide*.

---

You can use either J-Web or the CLI configuration editor to configure an IRB interface.
This topic covers:

- J-Web Configuration on page 695
- CLI Configuration on page 696
- Related Topics on page 696

**J-Web Configuration**

To configure an IRB interface:

1. Select **Configure > CLI Tools > Point and Click CLI**.
2. Next to Interfaces, click **Configure** or **Edit**.
3. In the Interface name column, select **irb**.
4. Under Unit, in the Interface unit number column, click **0**.
5. Next to Family group, select **Inet**, and then click **Configure**.
6. Next to Address, click **Add new entry**.
7. In the Source box, type the address **10.1.1.1/24**.
8. Next to Web authentication, click **Configure**.
9. Select the **Http** check box, and then click **OK**.
10. Click **OK** to return to the Unit page.
11. Click **OK** to return to the Interface page.
12. Click **OK** to return to the Interfaces page.

To reference the IRB interface in a bridge domain:

1. Select **Configure > CLI Tools > Point and Click CLI**.
2. Next to Bridge domains, click **Configure** or **Edit**.
3. Next to Domain, click **bd2**.
4. In the Routing interface box, type **irb.0**.
5. Click **OK** to return to the Configuration page.

To activate the webservice on the device:

1. Select **Configure > CLI Tools > Point and Click CLI**.
2. Next to System, click **Configure**.
3. Next to Services, select the check box, and then click **Configure**.
4. Next to Web management, click **Configure**.
5. Select the **Http** check box, and then click **OK**.
6. Click **OK** to return to the Services page.
7. Click **OK** to return to the System page.
8. Click **OK** to return to the Configuration page.
**CLI Configuration**

To configure an IRB interface:

user@host# set interface irb unit 0 family inet address 10.1.1.1/24
web-authentication http

To reference the IRB interface in a bridge domain:

user@host# set bridge-domains bd2 routing-interface irb.0

To activate the webserver on the device:

user@host# set system services web-management http

**Related Topics**

- Configuring Bridge Domains on page 680
- Creating Layer 2 Security Zones on page 686

**Understanding Layer 2 Forwarding Tables**

The SRX Series device maintains forwarding tables that contain MAC addresses and associated interfaces for each Layer 2 bridge domain. When a packet arrives with a new source MAC address in its frame header, the device adds the MAC address to its forwarding table and tracks the interface at which the packet arrived. The table also contains the corresponding interface through which the device can forward traffic for a particular MAC address.

If the destination MAC address of a packet is unknown to the device (that is, the destination MAC address in the packet does not have an entry in the forwarding table), the device duplicates the packet and floods it on all interfaces in the bridge domain other than the interface on which the packet arrived. This is known as packet flooding and is the default behavior for the device to determine the outgoing interface for an unknown destination MAC address. Packet flooding is performed at two levels: packets are flooded to different zones as permitted by configured Layer 2 security policies, and packets are also flooded to different interfaces with the same VLAN identifier within the same zone. The device learns the forwarding interface for the MAC address when a reply with that MAC address arrives at one of its interfaces.

You can specify that the SRX Series device use ARP queries and trace-route requests (which are ICMP echo requests with the time-to-live values set to 1) instead of packet flooding to locate an unknown destination MAC address. This method is considered more secure than packet flooding because the device floods ARP queries and trace-route packets—not the initial packet—on all interfaces. When ARP or trace-route flooding is used, the original packet is dropped. The device broadcasts an ARP or ICMP query to all other devices on the same subnetwork, requesting the device at the specified destination IP address to send back a reply. Only the device with the specified IP address replies, which provides the requestor with the MAC address of the responder.
ARP allows the device to discover the destination MAC address for a unicast packet if the destination IP address is in the same subnetwork as the ingress IP address. (The ingress IP address refers to the IP address of the last device to send the packet to the device. The device might be the source that sent the packet or a router forwarding the packet.) Trace-route allows the device to discover the destination MAC address even if the destination IP address belongs to a device in a subnetwork beyond that of the ingress IP address.

When you enable ARP queries to locate an unknown destination MAC address, trace-route requests are also enabled. You can also optionally specify that trace-route requests not be used; however, the device can then discover destination MAC addresses for unicast packets only if the destination IP address is in the same subnetwork as the ingress IP address.

Whether you enable ARP queries and trace-route requests or ARP-only queries to locate unknown destination MAC addresses, the SRX Series device performs the following series of actions:

1. The device notes the destination MAC address in the initial packet. The device adds the source MAC address and its corresponding interface to its forwarding table, if they are not already there.
2. The device drops the initial packet.
3. The device generates an ARP query packet and optionally a trace-route packet and floods those packets out all interfaces except the interface on which the initial packet arrived.

ARP packets are sent out with the following field values:
- Source IP address set to the IP address of the IRB
- Destination IP address set to the destination IP address of the original packet
- Source MAC address set to the MAC address of the IRB
- Destination MAC address set to the broadcast MAC address (all Oxf)

Trace-route (ICMP echo request or ping) packets are sent out with the following field values:
- Source IP address set to the IP address of the original packet
- Destination IP address set to the destination IP address of the original packet
- Source MAC address set to the source MAC address of the original packet
- Destination MAC address set to the destination MAC address of the original packet
- Time-to-live (TTL) set to 1

4. Combining the destination MAC address from the initial packet with the interface leading to that MAC address, the device adds a new entry to its forwarding table.
5. The device forwards all subsequent packets it receives for the destination MAC address out the correct interface to the destination.
Related Topics

- Changing the Default Learning for Unknown MAC Addresses on page 698

Changing the Default Learning for Unknown MAC Addresses

By default, the Juniper Networks device uses packet flooding to learn the outgoing interface for an unknown destination MAC address. You can specify that the device use ARP and trace-route packets or only ARP requests to learn this information.

Before You Begin

For background information, read “Understanding Layer 2 Forwarding Tables” on page 696.

This example configures the device to use ARP queries without trace-route requests to learn the outgoing interface for an unknown destination MAC address.

You can use either J-Web or the CLI configuration editor to change the device’s default method for learning unknown MAC addresses.

This topic covers:

- J-Web Configuration on page 698
- CLI Configuration on page 699
- Related Topics on page 699

J-Web Configuration

To enable the device to use only ARP requests to learn unknown destination MAC addresses:

1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Security, click Configure or Edit.
3. Next to Flow, click Configure or Edit.
4. Next to Bridge, click Configure.
5. Select No packet flooding, and select Configure.
6. Select No trace route.
7. Click OK to return to the Bridge page.
8. Click OK to return to the Flow page.
9. Click OK to return to the Security page.
**CLI Configuration**

To enable the device to use only ARP requests to learn unknown destination MAC addresses:

```
user@host# set security flow bridge no-packet-flooding no-trace-route
```

**Related Topics**

- Changing the Default Forwarding Behavior on page 691

**Understanding Layer 2 Transparent Mode Chassis Clusters**

A pair of SRX Series devices in Layer 2 transparent mode can be connected in a chassis cluster to provide network node redundancy. When configured in a chassis cluster, one node acts as the primary device and the other as the secondary device, ensuring stateful failover of processes and services in the event of system or hardware failure. If the primary device fails, the secondary device takes over processing of traffic.

**NOTE:** If the primary device fails in a Layer 2 transparent mode chassis cluster, the physical ports in the failed device become inactive (go down) for a few seconds before they become active (come up) again.

To form a chassis cluster, a pair of the same kind of supported SRX Series devices combines to act as a single system that enforces the same overall security. For more information about chassis clusters and configuring SRX Series devices in chassis cluster formations, see the *Junos OS Security Configuration Guide*.

Devices in Layer 2 transparent mode can be deployed in active/backup and active/active chassis cluster configurations.

The following chassis cluster features are not supported for devices in Layer 2 transparent mode:

- Gratuitous ARP—The newly elected master in a redundancy group cannot send gratuitous ARP requests to notify network devices of a change in mastership on the redundant Ethernet interface links.
- IP address monitoring—Failure of an upstream device cannot be detected.

A redundancy group is a construct that includes a collection of objects on both nodes. A redundancy group is primary on one node and backup on the other. When a redundancy group is primary on a node, its objects on that node are active. When a redundancy group fails over, all its objects fail over together.

You can create one or more redundancy groups numbered 1 through 128 for an active/active chassis cluster configuration. Each redundancy group contains one or more redundant Ethernet interfaces. A redundant Ethernet interface is a...
pseudointerface that contains physical interfaces from each node of the cluster. The physical interfaces in a redundant Ethernet interface must be the same kind—either Fast Ethernet or Gigabit Ethernet. If a redundancy group is active on node 0, then the child links of all associated redundant Ethernet interfaces on node 0 are active. If the redundancy group fails over to the node 1, then the child links of all redundant Ethernet interfaces on node 1 become active.

**NOTE:** The maximum number of redundancy groups is equal to the number of redundant Ethernet interfaces that you configure.

Configuring redundant Ethernet interfaces on a device in Layer 2 transparent mode is similar to configuring redundant Ethernet interfaces on a device in Layer 3 route mode, with the following difference: the redundant Ethernet interface on a device in Layer 2 transparent mode is configured as a Layer 2 logical interface (see “Understanding Layer 2 Interfaces” on page 680 and “Configuring Layer 2 Logical Interfaces” on page 682).

The redundant Ethernet interface may be configured as either an access interface (with a single VLAN ID assigned to untagged packets received on the interface) or as a trunk interface (with a list of VLAN IDs accepted on the interface and, optionally, a native-vlan-id for untagged packets received on the interface). Physical interfaces (one from each node in the chassis cluster) are bound as child interfaces to the parent redundant Ethernet interface.

In Layer 2 transparent mode, MAC learning is based on the redundant Ethernet interface. The MAC table is synchronized across redundant Ethernet interfaces and Services Processing Units (SPUs) between the pair of chassis cluster devices.

In this release, the IRB interface is used only for management traffic, and it cannot be assigned to any redundant Ethernet interface or redundancy group.

All JUNOS screen options that are available for a single, nonclustered device are available for devices in Layer 2 transparent mode chassis clusters.

**Related Topics**

- Configuring Redundant Ethernet Interfaces for Layer 2 Transparent Mode Chassis Clusters on page 700

**Configuring Redundant Ethernet Interfaces for Layer 2 Transparent Mode Chassis Clusters**

On a device in a Layer 2 transparent mode chassis cluster, the redundant Ethernet interface is configured as a Layer 2 logical interface. Physical interfaces are bound to the parent redundant Ethernet interface. This topic describes how to configure the redundant Ethernet interface as a Layer 2 logical interface and how to bind
physical interfaces (one from each node in the chassis cluster) to the redundant Ethernet interface.

### Before You Begin

For background information, read:
- “Chassis Clusters” in the Junos OS Security Configuration Guide
- Understanding Layer 2 Transparent Mode Chassis Clusters on page 699

In this example, you create a redundant Ethernet interface reth0 for redundancy group 1 and configure reth0 as an access interface with the VLAN identifier 1. Physical interfaces are then bound to reth0.

NOTE: Spanning-tree protocols are not supported for Layer 2 transparent mode in this release. You are responsible for ensuring that there are no loop connections in the deployment topology.

You can use either the J-Web or CLI configuration editor to configure a redundant Ethernet interface for a device in Layer 2 transparent mode.

This topic covers:
- J-Web Configuration on page 701
- CLI Configuration on page 702

### J-Web Configuration

To configure a redundant Ethernet interface as a Layer 2 logical interface:

1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Interfaces, click Configure or Edit.
3. Next to Interface, click Add new entry.
4. In the Interface name box, enter reth0.
5. Next to Redundant ether options, click Configure.
6. In the Redundancy group box, enter 1.
7. Click OK to return to the Interface page.
8. Next to Unit, click Add new entry.
9. In the Interface unit number box, enter 0.
10. Under Family, click the Bridge check box, then click Configure.
11. For Interface mode, select Access.
12. From the VLAN ID list, select 1.
13. Click OK.
To assign a child physical interface on a chassis cluster node to the redundant Ethernet interface:

1. Select Configure > CLI Tools > Point and Click CLI.
2. Next to Interfaces, click Configure or Edit.
3. For the physical interface, click Edit.
4. Next to Gigether options, click Configure.
5. Next to Redundant parent, click Configure.
6. In the Parent box, enter reth0.
7. Click OK.

**CLI Configuration**

To configure a redundant Ethernet interface as a Layer 2 logical interface:

```bash
user@host# set interfaces reth0 redundant-ether-options redundancy-group 1
user@host# set interfaces reth0 unit 0 family bridge interface-mode access vlan-id 1
```

To assign a physical interface on a chassis cluster node to the redundant Ethernet interface:

```bash
user@host# set interface ge-2/0/2 gigether-options redundant-parent reth0
```

**Overview of Class of Service Functions in Transparent Mode**

Devices operating in Layer 2 transparent mode support the following Class-of-Service (CoS) functions:

- IEEE 802.1p behavior aggregate (BA) classifiers to determine the forwarding treatment for packets entering the device
  
  Note that only IEEE 802.1p BA classifier types are supported on devices operating in transparent mode.

- Rewrite rules to redefine IEEE 802.1 CoS values in outgoing packets
  
  Note that rewrite rules that redefine IP precedence CoS values and Differentiated Services Code Point (DSCP) CoS values are not supported on devices operating in transparent mode.

- Shapers to apply rate limiting to an interface

- Schedulers that define the properties of an output queue

For more information about CoS components and configuring CoS on SRX Series devices, see *Junos OS Class of Service Configuration Guide for Security Devices*.

You configure BA classifiers and rewrite rules on transparent mode devices in the same way as on devices operating in Layer 3 mode. For transparent mode devices, however, you apply BA classifiers and rewrite rules only to logical interfaces configured
with the `family bridge` configuration statement. For more information about configuring Layer 2 logical interfaces, see “Configuring Layer 2 Logical Interfaces” on page 682.

Related Topics
- Understanding BA Traffic Classification on Transparent Mode Devices on page 703
- Understanding Rewrite of Packet Headers on Transparent Mode Devices on page 704

Understanding BA Traffic Classification on Transparent Mode Devices

A BA classifier checks the header information of an ingress packet. The resulting traffic classification consists of a forwarding class (FC) and packet loss priority (PLP). The FC and PLP associated with a packet specify the CoS behavior of a hop within the system. For example, a hop can place a packet into a priority queue according to its FC, and manage queues by checking the packet’s PLP. JUNOS Software supports up to eight FCs and four PLPs.

NOTE: MPLS EXP bit-based traffic classification is not supported.

BA classification can be applied within one DiffServ domain. BA classification can also be applied between two domains, where each domain honors the CoS results generated by the other domain. JUNOS Software performs BA classification for a packet by examining its Layer 2 and Layer 3 CoS-related parameters. Those parameters include the following:
- Layer 2—IEEE 802.1p: User Priority
- Layer 3—IPv4 Precedence, IPv4 DSCP, IPv6 DSCP

On SRX Series devices in transparent mode, a BA classifier evaluates only Layer 2 parameters. On SRX Series devices in Layer 3 mode, a BA classifier can evaluate Layer 2 and Layer 3 parameters; in that case, classification resulting from Layer 3 parameters overrides that of Layer 2 parameters.

On SRX Series devices in transparent mode, you specify one of four PLP levels—high, medium-high, medium-low, or low—when configuring a BA classifier.

Related Topics
- Configuring and Applying BA Classifiers on Transparent Mode Devices on page 703

Configuring and Applying BA Classifiers on Transparent Mode Devices

In this example, the logical interface `ge-0/0/4.0` is configured as a trunk port that carries traffic for packets tagged with VLAN identifiers 200 through 390. This example creates a BA classifier `c1` for IEEE 802.1 traffic where incoming packets with IEEE
802.1p priority bits 110 are assigned to the forwarding class fc1 with a low loss priority. The BA classifier c1 is applied to interface ge-0/0/4.0.

### Before You Begin

For background information, read:

- Understanding BA Traffic Classification on Transparent Mode Devices on page 703
- “Configuring Layer 2 Logical Interfaces” on page 682

### CLI Configuration

To configure the ge-0/0/4.0 logical interface as a Layer 2 trunk port:

```bash
user@host# set interfaces ge-0/0/0 vlan-tagging unit 0 family bridge interface-mode trunk vlan-id-list 200–390
```

To configure the forwarding classes:

```bash
user@host# set class-of-service forwarding-classes queue 0 fc1
user@host# set class-of-service forwarding-classes queue 1 fc2
user@host# set class-of-service forwarding-classes queue 2 fc3
user@host# set class-of-service forwarding-classes queue 3 fc4
user@host# set class-of-service forwarding-classes queue 4 fc5
user@host# set class-of-service forwarding-classes queue 5 fc6
user@host# set class-of-service forwarding-classes queue 6 fc7
user@host# set class-of-service forwarding-classes queue 7 fc8
user@host# set class-of-service forwarding-classes queue 8 fc7
```

To configure a BA classifier:

```bash
user@host# set class-of-service classifiers ieee-802.1 c1 forwarding-class fc1
        loss-priority low code-points 110
```

To apply the BA classifier to the ge-0/0/4.0 interface:

```bash
user@host# set class-of-service interfaces ge-0/0/4 unit 0 classifiers ieee-802.1 c1
```

### Understanding Rewrite of Packet Headers on Transparent Mode Devices

Before a packet is transmitted from an interface, the CoS fields in the packet’s header can be rewritten for the forwarding class (FC) and packet loss priority (PLP) of the packet. The rewriting function converts a packet’s FC and PLP into corresponding CoS fields in the packet header. In Layer 2 transparent mode, the CoS fields are the IEEE 802.1p priority bits.

You can use either J-Web or the CLI configuration editor to configure the rewrite rules that convert the FC and PLP into IEEE 802.1p priority bits and to apply the rewrite rules to an egress logical interface.
**Related Topics**

- Configuring and Applying Rewrite Rules on Transparent Mode Devices on page 705

---

### Configuring and Applying Rewrite Rules on Transparent Mode Devices

In this example, the logical interface **ge-1/0/3.0** is configured as a trunk port that carries traffic for packets tagged with VLAN identifiers 200 through 390. This example creates a rewrite rule rw1 for IEEE 802.1 traffic. For outgoing packets in the forwarding class fc1 with low loss priority, the IEEE 802.1p priority bits are rewritten as **011**. The rewrite rule rw1 is applied to interface **ge-1/0/3.0**.

### Before You Begin

For background information, read:

- Understanding Rewrite of Packet Headers on Transparent Mode Devices on page 704
- Configuring Layer 2 Logical Interfaces on page 682

### CLI Configuration

To configure the **ge-1/0/3.0** logical interface as a Layer 2 trunk port:

```
user@host# set interfaces ge-1/0/3 vlan-tagging unit 0 family bridge interface mode trunk vlan-id list 200–390
```

To configure the forwarding classes:

```
user@host# set class-of-service forwarding-classes queue 0 fc1
user@host# set class-of-service forwarding-classes queue 1 fc2
user@host# set class-of-service forwarding-classes queue 3 fc4
user@host# set class-of-service forwarding-classes queue 4 fc5
user@host# set class-of-service forwarding-classes queue 5 fc6
user@host# set class-of-service forwarding-classes queue 6 fc7
user@host# set class-of-service forwarding-classes queue 7 fc8
user@host# set class-of-service forwarding-classes queue 2 fc3
```

To configure a rewrite rule:

```
user@host# set class-of-service rewrite-rules ieee-802.1 rw1 forwarding-class fc1 loss-priority low code-point 011
```

To apply the rewrite rule to the **ge-1/0/3.0** interface:

```
user@host# set class-of-service interfaces ge-1/0/3 unit 0 rewrite-rules ieee-802.1 rw1
```
Part 5
MPLS

- MPLS on page 709
- Traffic Engineering on page 719
- MPLS VPNs on page 737
- CLNS VPNs on page 757
- VPLS on page 769
MPLS Overview

Multiprotocol Label Switching (MPLS) is a method for engineering traffic patterns by assigning short labels to network packets that describe how to forward them through the network. MPLS is independent of routing tables or any routing protocol and can be used for unicast packets.

The MPLS framework supports traffic engineering and the creation of virtual private networks (VPNs). Traffic is engineered (controlled) primarily by the use of signaling protocols to establish label-switched paths (LSPs). VPN support includes Layer 2 and Layer 3 VPNs and Layer 2 circuits.

When you enable your device to allow MPLS traffic, the device performs packet-based processing and functions as a standard JUNOS router.

**CAUTION:** When MPLS is enabled on your router, all security features such as security policies, zones, NAT, ALGs, chassis clustering, screens, firewall authentication, and IPSec VPNs are unavailable.

This overview contains the following topics:

- Label Switching on page 710
- Label-Switched Paths on page 710
- Label-Switching Routers on page 711
- Labels on page 712
- Label Operations on page 712
- Penultimate Hop Popping on page 713
- LSP Establishment on page 713
**Label Switching**

In a traditional IP network, packets are transmitted with an IP header that includes a source and destination address. When a router receives such a packet, it examines its forwarding tables for the next-hop address associated with the packet’s destination address and forwards the packet to the next-hop location.

In an MPLS network, each packet is encapsulated with an MPLS header. When a router receives the packet, it copies the header as an index into a separate MPLS forwarding table. The MPLS forwarding table consists of pairs of inbound interfaces and path information. Each pair includes forwarding information that the router uses to forward the traffic and modify, when necessary, the MPLS header.

Because the MPLS forwarding table has far fewer entries than the more general forwarding table, the lookup consumes less processing time and processing power. The resultant savings in time and processing are a significant benefit for traffic that uses the network to transit between outside destinations only.

**Label-Switched Paths**

Label-switched paths (LSPs) are unidirectional routes through a network or autonomous system (AS). In normal IP routing, the packet has no predetermined path. Instead, each router forwards a packet to the next-hop address stored in its forwarding table, based only on the packet’s destination address. Each subsequent router then forwards the packet using its own forwarding table.

In contrast, MPLS routers within an AS determine paths through a network through the exchange of MPLS traffic engineering information. Using these paths, the routers direct traffic through the network along an established route. Rather than selecting the next hop along the path as in IP routing, each router is responsible for forwarding the packet to a predetermined next-hop address.

Figure 84 on page 711 shows a typical LSP topology.
In the topology shown in Figure 84 on page 711, traffic is forwarded from Host C1 to the transit network with standard IP forwarding. When the traffic enters the transit network, it is switched across a preestablished LSP through the network. In this example, an LSP might switch the traffic from Router R4 to Router R2 to Router R1. When the traffic exits the network, it is forwarded to its destination by IP routing protocols.

**Label-Switching Routers**

Routers that are part of the LSP are label-switching routers (LSRs). Each LSR must be configured with MPLS so that it can interpret MPLS headers and perform the MPLS operations required to pass traffic through the network. An LSP can include four types of LSRs:

- **Inbound router**—The only entry point for traffic into MPLS. Native IPv4 packets are encapsulated into the MPLS protocol by the inbound router. Each LSP can have only one inbound router. Inbound routers are also known as ingress routers.

- **Transit router**—Any router in the middle of an LSP. An individual LSP can contain between 0 and 253 transit routers. Transit routers forward MPLS traffic along the LSP, using only the MPLS header to determine how the packet is routed.

- **Penultimate router**—The second-to-last router in the LSP. The penultimate router in an LSP is responsible for stripping the MPLS header from the packet before forwarding it to the outbound router.

- **Outbound router**—The endpoint for the LSP. The outbound router receives MPLS packets from the penultimate router and performs an IP route lookup. The router then forwards the packet to the next hop of the route. Each LSP can have only one outbound router. Outbound routers are also known as egress routers.
**Labels**

To forward traffic through an MPLS network, MPLS routers encapsulate packets and assign and manage headers known as *labels*. A label is a 20–bit unsigned integer in the range 0 through 1,048,575. The routers use the labels to index the MPLS forwarding tables that determine how packets are routed through the network.

When a network's inbound router receives traffic, it inserts an MPLS label between the IP packet and the appropriate Layer 2 header for the physical link. The label contains an index value that identifies a next-hop address for the particular LSP. When the next-hop transit router receives the packet, it uses the index in the MPLS label to determine the next-hop address for the packet and forwards the packet to the next router in the LSP.

As each packet travels through the transit network, every router along the way performs a lookup on the MPLS label and forwards the packet accordingly. When the outbound router receives a packet, it examines the header to determine that it is the final router in the LSP. The outbound router then removes the MPLS header, performs a regular IP route lookup, and forwards the packet with its IP header to the next-hop address.

**Label Operations**

Each LSR along an LSP is responsible for examining the MPLS label, determining the LSP next hop, and performing the required label operations. LSRs can perform five label operations:

- **Push**—Adds a new label to the top of the packet. For IPv4 packets arriving at the inbound router, the new label is the first label in the label stack. For MPLS packets with an existing label, this operation adds a label to the stack and sets the stacking bit to 0, indicating that more MPLS labels follow the first. When it receives the packet, the inbound router performs an IP route lookup on the packet. Because the route lookup yields an LSP next hop, the inbound router performs a label push on the packet, and then forwards the packet to the LSP next hop.

- **Swap**—Replaces the label at the top of the label stack with a new label. When a transit router receives the packet, it performs an MPLS forwarding table lookup. The lookup yields the LSP next hop and the path index of the link between the transit router and the next router in the LSP.

- **Pop**—Removes the label from the top of the label stack. For IPv4 packets arriving at the penultimate router, the entire MPLS label is removed from the label stack. For MPLS packets with an existing label, this operation removes the top label from the label stack and modifies the stacking bit as necessary—sets it to 1, for example, if only a single label remains in the stack. If multiple LSPs terminate at the same outbound router, the router performs MPLS label operations for all outbound traffic on the LSPs. To share the operations among multiple routers, most LSPs use penultimate hop popping (PHP).

- **Multiple push**—Adds multiple labels to the top of the label stack. This action is equivalent to performing multiple push operations.
The multiple push operation is used with label stacking, which is beyond the scope of this topic.

- **Swap and push**—Replaces the top label with a new label and then pushes a new label to the top of the stack.

The swap and push operation is used with label stacking, which is beyond the scope of this topic.

**Penultimate Hop Popping**

Multiple LSPs terminating at a single outbound router load the router with MPLS label operations for all their outbound traffic. Penultimate hop popping (PHP) transfers the operation from the outbound router to penultimate routers.

With PHP, the penultimate router is responsible for popping the MPLS label and forwarding the traffic to the outbound router. The outbound router then performs an IP route lookup and forwards the traffic. For example, if four LSPs terminate at the same outbound router and each has a different penultimate router, label operations are shared across four routers.

**LSP Establishment**

An MPLS LSP is established by one of two methods: static LSPs and dynamic LSPs.

**Static LSPs**

Like a static route, a static LSP requires each router along the path to be configured explicitly. You must manually configure the path and its associated label values. Static LSPs require less processing by the LSRs because no signaling protocol is used. However, because paths are statically configured, they cannot adapt to network conditions. Topology changes and network outages can create black holes in the LSP that exist until you manually reconfigure the LSP.

**Dynamic LSPs**

Dynamic LSPs use signaling protocols to establish themselves and propagate LSP information to other LSRs in the network. You configure the inbound router with LSP information that is transmitted throughout the network when you enable the signaling protocols across the LSRs. Because the LSRs must exchange and process signaling packets and instructions, dynamic LSPs consume more resources than static LSPs. However, dynamic LSPs can avoid the network black holes of static LSPs by detecting topology changes and outages and propagating them throughout the network.

**Related Topics**

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- MPLS Configuration Overview on page 714
- Example: Deleting Security Services on page 715
- Example: Enabling MPLS on page 716
MPLS Configuration Overview

When you first install JUNOS Software on your device, MPLS is disabled by default. You must explicitly configure your device to allow MPLS traffic to pass through. Complete the following steps for all devices in your MPLS network that are running JUNOS software.

To enable MPLS:

1. Delete all configured security services from the device. If you do not complete this step, you will get a commit failure. See “Example: Deleting Security Services” on page 715
2. Enable MPLS on the device. See “Example: Enabling MPLS” on page 716
3. Commit the configuration.
4. Reboot the device.
5. Configure MPLS features such as traffic engineering, VPNs, and VPLS. See:
   - MPLS Traffic Engineering and Signaling Protocols Overview on page 719
   - MPLS VPN Overview on page 737
   - CLNS Overview on page 757
   - VPLS Overview on page 769

**CAUTION:** When MPLS is enabled, all flow-based security features are deactivated and the device performs packet-based processing. Flow-based services such as security policies, zones, NAT, ALGs, chassis clustering, screens, firewall authentication, and IPSec VPNs are unavailable on the router.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- MPLS Overview on page 709
- Example: Deleting Security Services on page 715
- Example: Enabling MPLS on page 716
- Junos MPLS Applications Configuration Guide
- Junos VPNs Configuration Guide
**Example: Deleting Security Services (CLI)**

The following example shows how to save your current configuration to a file called `curfeb08.cfg` before removing all configurations from the **security** level of the configuration hierarchy and deleting all global groups and inherited configurations.

Before you enable MPLS, we recommend that you delete all configured security services.

To delete the configured services in the **security** level of the configuration hierarchy:

1. Save your current configuration in the `var/tmp/` directory with an appropriate filename with the `.cfg` extension—for example, `curfeb08.cfg`.
   
   ```
   [edit]
   user@host# save /var/tmp/curfeb08.cfg
   ```

2. Remove all configurations in the **security** level of the configuration hierarchy.

   ```
   [edit]
   user@host# delete security
   ```

3. Remove all global group and inherited configurations.

   ```
   [edit]
   user@host# delete groups global security
   ```

---

**CAUTION:** Do not commit after deleting the security configurations. A commit without any security configurations leaves the router unreachable through the management port.

---

**Related Topics**

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- MPLS Overview on page 709
- MPLS Configuration Overview on page 714
- Example: Enabling MPLS on page 716
**Example: Enabling MPLS (CLI)**

Before including a device running JUNOS Software in an MPLS network, you must enable MPLS on the device. Perform these tasks on all of the devices running JUNOS Software.

The following example shows how to enable MPLS for packet-based processing. It also shows how to enable the MPLS family and MPLS process on the ge-1/0/0 transit interface.

To enable MPLS:

1. Navigate to the **security forwarding options** level of the configuration hierarchy.
   ```
   [edit]
   user@host# edit security forwarding-options
   ```
2. Enable MPLS for packet-based processing.
   ```
   [edit security forwarding-options]
   user@host# set family mpls mode packet-based
   ```
3. Navigate to the **interfaces** level of the configuration hierarchy.
   ```
   [edit security forwarding-options]
   user@host# top
   [edit]
   user@host# edit interfaces
   ```
4. Enable the MPLS family on each transit interface that you want to include in the MPLS network. For example:
   ```
   [edit interfaces]
   user@host# set interfaces ge-1/0/0 unit 0 family mpls
   ```
5. Navigate to the **protocols mpls** level of the configuration hierarchy.
   ```
   [edit interfaces]
   user@host# top
   [edit]
   user@host# edit protocols mpls
   ```
6. Enable the MPLS process on all of the transit interfaces in the MPLS network. For example:
   ```
   [edit protocols mpls]
   user@host# set interface all
   ```
7. Commit the configuration when you are done configuring the device.
   ```
   [edit]
   user@host# commit
   ```
8. Reboot the device.
**CAUTION:** If you disable MPLS and switch back to using the security services (flow-based processing), we recommend that you restart your router. Management sessions are reset, and transit traffic is interrupted.

**Related Topics**
- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- MPLS Overview on page 709
- MPLS Configuration Overview on page 714
- Example: Deleting Security Services on page 715
Chapter 28
Traffic Engineering

- MPLS Traffic Engineering and Signaling Protocols Overview on page 719
- LDP Signaling Protocol on page 720
- RSVP Signaling Protocol on page 725
- Point-to-Multipoint LSPs on page 733

MPLS Traffic Engineering and Signaling Protocols Overview

Traffic engineering facilitates efficient and reliable network operations while simultaneously optimizing network resources and traffic performance. Traffic engineering provides the ability to move traffic flow away from the shortest path selected by the interior gateway protocol (IGP) to a potentially less congested physical path across a network. To support traffic engineering, besides source routing, the network must do the following:

- Compute a path at the source by taking into account all the constraints, such as bandwidth and administrative requirements.
- Distribute the information about network topology and link attributes throughout the network once the path is computed.
- Reserve network resources and modify link attributes.

When transit traffic is routed through an IP network, MPLS is often used to engineer its passage. Although the exact path through the transit network is of little importance to either the sender or the receiver of the traffic, network administrators often want to route traffic more efficiently between certain source and destination address pairs. By adding a short label with specific routing instructions to each packet, MPLS switches packets from router to router through the network rather than forwarding packets based on next-hop lookups. The resulting routes are called label-switched paths (LSPs). LSPs control the passage of traffic through the network and speed traffic forwarding.

You can create LSPs manually, or through the use of signaling protocols. Signaling protocols are used within an MPLS environment to establish LSPs for traffic across a transit network. JUNOS Software supports two signaling protocols—LDP and the Resource Reservation Protocol (RSVP).
MPLS traffic engineering uses the following components:

- MPLS LSPs for packet forwarding
- IGP extensions for distributing information about the network topology and link attributes
- Constrained Shortest Path First (CSPF) for path computation and path selection
- RSVP extensions to establish the forwarding state along the path and to reserve resources along the path

JUNOS Software also supports traffic engineering across different OSPF regions.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding the LDP Signaling Protocol on page 720
- Understanding the RSVP Signaling Protocol on page 725
- Understanding Point-to-Multipoint LSPs on page 733
- Enabling Interarea Traffic Engineering in the Junos MPLS Applications Configuration Guide

LDP Signaling Protocol

- Understanding the LDP Signaling Protocol on page 720
- Example: Configuring LDP-Signaled LSPs on page 721

Understanding the LDP Signaling Protocol

LDP is a signaling protocol that runs on a device configured for MPLS support. The successful configuration of both MPLS and LDP initiates the exchange of TCP packets across the LDP interfaces. The packets establish TCP-based LDP sessions for the exchange of MPLS information within the network. Enabling both MPLS and LDP on the appropriate interfaces is sufficient to establish LSPs.

LDP is a simple, fast-acting signaling protocol that automatically establishes LSP adjacencies within an MPLS network. Routers then share LSP updates such as hello packets and LSP advertisements across the adjacencies. Because LDP runs on top of an IGP such as IS-IS or OSPF, you must configure LDP and the IGP on the same set of interfaces. After both are configured, LDP begins transmitting and receiving LDP messages through all LDP-enabled interfaces. Because of LDP’s simplicity, it cannot perform the true traffic engineering which RSVP can perform. LDP does not support bandwidth reservation or traffic constraints.

When you configure LDP on a label-switching router (LSR), the router begins sending LDP discovery messages out all LDP-enabled interfaces. When an adjacent LSR receives LDP discovery messages, it establishes an underlying TCP session. An LDP session is then created on top of the TCP session. The TCP three-way handshake ensures that the LDP session has bidirectional connectivity. After they establish the LDP session, the LDP neighbors maintain, and terminate, the session by exchanging...
messages. LDP advertisement messages allow LSRs to exchange label information to determine the next hops within a particular LSP. Any topology changes, such as a router failure, generate LDP notifications that can terminate the LDP session or generate additional LDP advertisements to propagate an LSP change.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- MPLS Traffic Engineering and Signaling Protocols Overview on page 719
- Example: Configuring LDP-Signaled LSPs on page 721

Example: Configuring LDP-Signaled LSPs

This example shows how to create and configure LDP instances within an MPLS network.

- Requirements on page 721
- Overview on page 721
- Configuration on page 722
- Verification on page 723

Requirements

Before you begin:

2. Configure an IGP across your network. (The LDP configuration is added to the existing IGP configuration and included in the MPLS configuration.)
3. Configure a network to use LDP for LSP establishment by enabling MPLS on all transit interfaces in the MPLS network.

NOTE: Because LDP runs on top of an IGP such as IS-IS or OSPF, you must configure LDP and the IGP on the same set of interfaces.

Overview

To configure LDP-signaled RSPs, you must enable the MPLS family on all transit interfaces in the MPLS network, enable the MPLS process on all router interfaces in the MPLS network, and enable an LDP instance on each router. In this example, you enable the MPLS family and create an LDP instance on the ge-0/0/0 interface. Additionally, you enable the MPLS process on all router interfaces in the MPLS network.
Configuration

CLI Quick Configuration  To quickly configure LDP instances within an MPLS network, copy the following commands and paste them into the CLI.

```
[edit]
set interfaces ge-0/0/0 unit 0 family mpls
set protocols mpls interface all
set protocols ldp interface ge-0/0/0.0
```

Step-by-Step Procedure  To enable LDP instances within an MPLS network:

1. Enable the MPLS family on the transit interface.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family mpls
```

2. Enable the MPLS process all interfaces.

```
[edit]
user@host# set protocols mpls interface all
```

3. Create the LDP instance on the transit interface.

```
[edit]
user@host# set protocols ldp interface ge-0/0/0
```

Results  Confirm your configuration by entering the `show` command from configuration mode. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this show output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
user@host# show
...
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        address 10.100.37.20/24;
      }
      family mpls;
    }
  }
}
...
protocols {
  mpls {
    interface all;
  }
}
```
ldp {
    interface ge-0/0/0.0;
}

If you are done configuring the device, enter the commit command from the configuration mode to activate the configuration.

**Verification**

To confirm that the configuration is working properly, perform these tasks:

- Verifying LDP Neighbors on page 723
- Verifying LDP Sessions on page 723
- Verifying the Presence of LDP-Signaled LSPs on page 724
- Verifying Traffic Forwarding over the LDP-Signaled LSP on page 724

**Verifying LDP Neighbors**

**Purpose**
Verify that each router shows the appropriate LDP neighbors.

**Action**
From the CLI, enter the `show ldp neighbor` command.

**Sample Output**

```sh
user@r5> show ldp neighbor
Address     Interface       Label space ID      Hold time
10.0.8.5    ge-0/0/0.0      10.0.9.6:0            14
10.0.8.10   ge-0/0/1.0      10.0.9.7:0            11
```

**Meaning**
The output shows the IP addresses of the neighboring interfaces along with the interface through which the neighbor adjacency is established. Verify the following information:

- Each interface on which LDP is enabled is listed.
- Each neighboring LDP interface address is listed with the appropriate corresponding LDP interface.
- Under Label space ID, the appropriate loopback address for each neighbor appears.

**Verifying LDP Sessions**

**Purpose**
Verify that a TCP-based LDP session has been established between all LDP neighbors. Also, verify that the modified keepalive value is active.

**Action**
From the CLI, enter the `show ldp session detail` command.

**Sample Output**

```sh
user@r5> show ldp session detail
Address: 10.0.9.7, State: Operational, Connection: Open, Hold time: 28
Session ID: 10.0.3.5:0--10.0.9.7:0
Next keepalive in 3 seconds
```
Passive, Maximum PDU: 4096, Hold time: 30, Neighbor count: 1
Keepalive interval: 10, Connect retry interval: 1
Local - Restart: disabled, Helper mode: enabled
Remote - Restart: disabled, Helper mode: disabled
Local maximum recovery time: 240000 msec
Next-hop addresses received:
  10.0.8.10
  10.0.2.17

**Meaning** The output shows the detailed information, including session IDs, keepalive interval, and next-hop addresses, for each established LDP session. Verify the following information:

- Each LDP neighbor address has an entry, listed by loopback address.
- The state for each session is **Operational**, and the connection for each session is **Open**. A state of **Nonexistent** or a connection of **Closed** indicates a problem with one of the following:
  - LDP configuration
  - Passage of traffic between the two devices
  - Physical link between the two routers
- For **Keepalive interval**, the appropriate value, 10, appears.

**Verifying the Presence of LDP-Signaled LSPs**

**Purpose** Verify that each Juniper Networks device’s **inet.3** routing table has an LSP for the loopback address on each of the other routers.

**Action** From the CLI, enter the `show route table inet.3` command.

**Sample Output**

```
user@r5> show route table inet.3
inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.9.6/32         *[LDP/9/0] 00:05:29, metric 1
                   > to 10.0.8.5 via ge-0/0/0.0
10.0.9.7/32         *[LDP/9/0] 00:05:37, metric 1
                   > to 10.0.8.10 via ge-0/0/1.0
```

**Meaning** The output shows the LDP routes that exist in the **inet.3** routing table. Verify that an LDP-signaled LSP is associated with the loopback addresses of the other routers in the MPLS network.

**Verifying Traffic Forwarding over the LDP-Signaled LSP**

**Purpose** Verify that traffic between hosts is forwarded over the LDP-signaled LSP. Because traffic uses any configured gateway address by default, you must explicitly specify that the gateway address is to be bypassed.
Action  From the CLI, enter the `traceroute 220.220.0.0 source 200.200.0.1 bypass-routing gateway 172.16.0.1` command.

Sample Output  
```bash
user@c1> traceroute 220.220.0.0 source 200.200.0.1 bypass-routing gateway 172.16.0.1
traceroute to 220.220.0.1 (172.16.0.1) from 200.200.0.1, 30 hops max, 40 byte packets
1  172.16.0.1 (172.16.0.1)  0.661 ms  0.538 ms  0.449 ms
2  10.0.8.9 (10.0.8.9)  0.511 ms  0.479 ms  0.468 ms
   MPLS Label=100004 CoS=0 TTL=1 S=1
3  10.0.8.5 (10.0.8.5)  0.476 ms  0.512 ms  0.441 ms
4  220.220.0.1 (220.220.0.1) 0.436 ms  0.420 ms  0.416 ms
```

Meaning  The output shows the route that traffic travels between hosts without using the default gateway. In this example, verify that traffic sent from Host C1 to Host C2 travels through Router R7. The `10.0.8.9` address is the interface address for Router R5.

Related Topics  ■ Junos OS Feature Support Reference for SRX Series and J Series Devices
■ Understanding the LDP Signaling Protocol on page 720
■ show ldp neighbor in the Junos Routing Protocols and Policies Command Reference
■ show ldp session in the Junos Routing Protocols and Policies Command Reference
■ show route table in the Junos Routing Protocols and Policies Command Reference
■ traceroute in the Junos System Basics and Services Command Reference

RSVP Signaling Protocol

- Understanding the RSVP Signaling Protocol on page 725
- Example: Configuring RSVP-Signaled LSPs on page 729

Understanding the RSVP Signaling Protocol

RSVP is a signaling protocol that handles bandwidth allocation and true traffic engineering across an MPLS network. Like LDP, RSVP uses discovery messages and advertisements to exchange LSP path information between all hosts. However, RSVP also includes a set of features that control the flow of traffic through an MPLS network. Whereas LDP is restricted to using the configured IGP’s shortest path as the transit path through the network, RSVP uses a combination of the Constrained Shortest Path First (CSPF) algorithm and Explicit Route Objects (EROs) to determine how traffic is routed through the network.

Basic RSVP sessions are established in exactly the same way that LDP sessions are established. By configuring both MPLS and RSVP on the appropriate transit interfaces, you enable the exchange of RSVP packets and the establishment of LSPs. However, RSVP also lets you configure link authentication, explicit LSP paths, and link coloring.
RSVP Fundamentals

RSVP uses unidirectional and simplex flows through the network to perform its function. The inbound router initiates an RSVP path message and sends it downstream to the outbound router. The path message contains information about the resources needed for the connection. Each router along the path begins to maintain information about a reservation.

When the path message reaches the outbound router, resource reservation begins. The outbound router sends a reservation message upstream to the inbound router. Each router along the path receives the reservation message and sends it upstream, following the path of the original path message. When the inbound router receives the reservation message, the unidirectional network path is established.

The established path remains open as long as the RSVP session is active. The session is maintained by the transmission of additional path and reservation messages that report the session state every 30 seconds. If a router does not receive the maintenance messages for 3 minutes, it terminates the RSVP session and reroutes the LSP through another active router.

Bandwidth Reservation Requirement

When a bandwidth reservation is configured, reservation messages propagate the bandwidth value throughout the LSP. Routers must reserve the bandwidth specified across the link for the particular LSP. If the total bandwidth reservation exceeds the available bandwidth for a particular LSP segment, the LSP is rerouted through another LSR. If no segments can support the bandwidth reservation, LSP setup fails and the RSVP session is not established.

Explicit Route Objects

Explicit Route Objects (EROs) limit LSP routing to a specified list of LSRs. By default, RSVP messages follow a path that is determined by the network IGP’s shortest path. However, in the presence of a configured ERO, the RSVP messages follow the path specified.

EROs consist of two types of instructions: loose hops and strict hops. When a loose hop is configured, it identifies one or more transit LSRs through which the LSP must be routed. The network IGP determines the exact route from the inbound router to the first loose hop, or from one loose hop to the next. The loose hop specifies only that a particular LSR be included in the LSP.
When a strict hop is configured, it identifies an exact path through which the LSP must be routed. Strict-hop EROs specify the exact order of the routers through which the RSVP messages are sent.

You can configure loose-hop and strict-hop EROs simultaneously. In this case, the IGP determines the route between loose hops, and the strict-hop configuration specifies the exact path for particular LSP path segments.

Figure 85 on page 727 shows a typical RSVP-signaled LSP that uses EROs.

**Figure 85: Typical RSVP-Signaled LSP with EROs**

In the topology shown in Figure 85 on page 727, traffic is routed from Host C1 to Host C2. The LSP can pass through Routers R4 or Router R7. To force the LSP to use R4, you can set up either a loose-hop or strict-hop ERO that specifies R4 as a hop in the LSP. To force a specific path through Router R4, R3, and R6, configure a strict-hop ERO through the three LSRs.

**Constrained Shortest Path First**

Whereas IGPs use the Shortest Path First (SPF) algorithm to determine how traffic is routed within a network, RSVP uses the Constrained Shortest Path First (CSPF) algorithm to calculate traffic paths that are subject to the following constraints:

- **LSP attributes**—Administrative groups such as link coloring, bandwidth requirements, and EROs
- **Link attributes**—Colors on a particular link and available bandwidth

These constraints are maintained in the traffic engineering database (TED). The database provides CSPF with up-to-date topology information, the current reservable bandwidth of links, and the link colors.

In determining which path to select, CSPF follows these rules:
Computes LSPs one at a time, beginning with the highest priority LSP—the one with the lowest setup priority value. Among LSPs of equal priority, CSPF starts with those that have the highest bandwidth requirement.

Prunes the traffic engineering database of links that are not full duplex and do not have sufficient reservable bandwidth.

If the LSP configuration includes the include statement, prunes all links that do not share any included colors.

If the LSP configuration includes the exclude statement, prunes all links that contain excluded colors. If a link does not have a color, it is accepted.

Finds the shortest path toward the LSP's outbound router, taking into account any EROs. For example, if the path must pass through Router A, two separate SPF algorithms are computed: one from the inbound router to Router A and one from Router A to the outbound router.

If several paths have equal cost, chooses the one with a last-hop address the same as the LSP's destination.

If several equal-cost paths remain, selects the path with the least number of hops.

If several equal-cost paths remain, applies CSPF load-balancing rules configured on the LSP.

### Link Coloring

RSVP allows you to configure administrative groups for CSPF path selection. An administrative group is typically named with a color, assigned a numeric value, and applied to the RSVP interface for the appropriate link. Lower numbers indicate higher priority.

After configuring the administrative group, you can either exclude, include, or ignore links of that color in the TED:

- If you exclude a particular color, all segments with an administrative group of that color are excluded from CSPF path selection.
- If you include a particular color, only those segments with the appropriate color are selected.
- If you neither exclude nor include the color, the metrics associated with the administrative groups and applied on the particular segments determine the path cost for that segment.

The LSP with the lowest total path cost is selected into the TED.

**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- MPLS Traffic Engineering and Signaling Protocols Overview on page 719
- Example: Configuring RSVP-Signaled LSPs on page 729
Example: Configuring RSVP-Signaled LSPs

This example shows how to create an LSP between routers in an IP network using RSVP as the signaling protocol.

- Requirements on page 729
- Overview and Topology on page 729
- Configuration on page 730
- Verification on page 731

Requirements

Before you begin, delete security services from the device. See “Example: Deleting Security Services” on page 715.

Overview and Topology

Using RSVP as a signaling protocol, you can create LSPs between routers in an IP network. In this example, you configure a sample network as shown in Figure 86 on page 729.

Figure 86: Typical RSVP-Signaled LSP

To establish an LSP between routers, you must individually enable the MPLS family and configure RSVP on each of the transit interfaces in the MPLS network. (This example shows how to enable MPLS and configure RSVP on the ge-0/0/0 transit interface). Additionally, you must enable the MPLS process on all of the MPLS interfaces in the network.

This example shows how to define an LSP from R1 to R7 on the ingress router (R1) using R7’s loopback address (10.0.9.7). The configuration reserves 10 Mbps of
bandwidth. Additionally, the configuration disables the CSPF algorithm, ensuring that Hosts C1 and C2 use the RSVP-signaled LSP that correspond to the network IGP’s shortest path.

**Configuration**

**CLI Quick Configuration**

To quickly configure RSVP, copy the following commands and paste them into the CLI.

```
[edit]
set interfaces ge-0/0/0 unit 0 family mpls
set protocols rsvp interface ge-0/0/0.0
set protocols mpls label-switched-path r1-r7 to 10.0.9.7
set protocols mpls label-switched-path r1-r7 bandwidth 10m
set protocols mpls label-switched-path r1-r7 no-cspf
set protocols mpls interface all
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see Using the CLI Editor in Configuration Mode.

To configure RSVP:

1. Enable the MPLS family on all transit interfaces in the MPLS network.

   ```
   [edit]
   user@host# set interfaces ge-0/0/0 unit 0 family mpls
   ```

2. Enable RSVP on each transit interface in the MPLS network.

   ```
   [edit]
   user@host# set protocols rsvp interface ge-0/0/0
   ```

3. Enable the MPLS process on all of the MPLS interfaces in the MPLS network.

   ```
   [edit]
   user@host# set protocols mpls interface all
   ```

4. Define the LSP on the ingress router.

   ```
   [edit protocols mpls]
   user@host# set label-switched-path r1-r7 to 10.0.9.7
   ```

5. Reserve 10 Mbps of bandwidth on the LSP.

   ```
   [edit protocols mpls]
   user@host# set label-switched-path r1-r7 bandwidth 10m
   ```

6. Disable the CSPF algorithm.

   ```
   [edit protocols mpls]
   user@host# set label-switched-path r1-r7 no-cspf
   ```
Confirm your configuration by entering the `show` command from configuration mode. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this `show` command output includes only the configuration that is relevant to this example. Any other configuration on the system has been replaced with ellipses (...).

```
user@host# show
...
interfaces {
  ge-0/0/0 {
    family mpls;
  }
}
...
protocols {
  rsvp {
    interface ge-0/0/0.0;
  }
  mpls {
    label-switched-path r1-r7 {
      to 10.0.9.7;
      bandwidth 10m;
      no-cspf;
    }
    interface all;
  }
}
...
```

If you are done configuring the device, enter `commit` from configuration mode.

**Verification**

To confirm that the configuration is working properly, perform these tasks:

- Verifying RSVP Neighbors on page 731
- Verifying RSVP Sessions on page 732
- Verifying the Presence of RSVP-Signaled LSPs on page 732

**Verifying RSVP Neighbors**

**Purpose**  Verify that each device shows the appropriate RSVP neighbors—for example, that Router R1 in Figure 86 on page 729 lists both Router R3 and Router R2 as RSVP neighbors.

**Action**  From the CLI, enter the `show rsvp neighbor` command.

**Sample Output**

```
user@r1> show rsvp neighbor
RSVP neighbor: 2 learned
Address       Idle Up/Dn LastChange HelloInt HelloTx/Rx
```
Meaning  The output shows the IP addresses of the neighboring routers. Verify that each neighboring RSVP router loopback address is listed.

Verifying RSVP Sessions

Purpose  Verify that an RSVP session has been established between all RSVP neighbors. Also, verify that the bandwidth reservation value is active.

Action  From the CLI, enter the `show rsvp session detail` command.

Sample Output

```
user@r1> show rsvp session detail
Ingress RSVP: 1 sessions
10.0.9.7
  From: 10.0.6.1, LSPstate: Up, ActiveRoute: 0
  LSPname: r1-r7, LSPpath: Primary
  Bidirectional, Upstream label in: -, Upstream label out: -
  Suggested label received: -, Suggested label sent: -
  Recovery label received: -, Recovery label sent: 100000
  Resv style: 1 FF, Label in: -, Label out: 100000
  Time left: -, Since: Thu Jan 26 17:57:45 2002
  Tspec: rate 10Mbps size 10Mbps peak Infbps m 20 M 1500
  Port number: sender 3 receiver 17 protocol 0
  PATH rcvfrom: localclient
  PATH sentto: 10.0.4.13 (ge-0/0/1.0) 1467 pkts
  RESV rcvfrom: 10.0.4.13 (ge-0/0/1.0) 1467 pkts
  Record route: <self> 10.0.4.13 10.0.2.1 10.0.8.10
```

Meaning  The output shows the detailed information, including session IDs, bandwidth reservation, and next-hop addresses, for each established RSVP session. Verify the following information:

- Each RSVP neighbor address has an entry for each neighbor, listed by loopback address.
- The state for each LSP session is `Up`.
- For `Tspec`, the appropriate bandwidth value, `10Mbps`, appears.

Verifying the Presence of RSVP-Signaled LSPs

Purpose  Verify that the routing table of the entry (ingress) router has a configured LSP to the loopback address of the other router. For example, verify that the `inet.3` routing table of the R1 entry router in Figure 86 on page 729 has a configured LSP to the loopback address of Router R7.

Action  From the CLI, enter the `show route table inet.3` command.
Sample Output

user@r1> show route table inet.3
inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.0.9.7/32 *[RSVP/7] 00:05:29, metric 10
> to 10.0.4.17 via ge-0/0/0.0, label-switched-path r1-r7

Meaning
The output shows the RSVP routes that exist in the inet.3 routing table. Verify that an RSVP-signaled LSP is associated with the loopback address of the exit (egress) router, R7, in the MPLS network.

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding the RSVP Signaling Protocol on page 725
- show rsvp neighbor in the Junos Routing Protocols and Policies Command Reference
- show rsvp session in the Junos Routing Protocols and Policies Command Reference

Point-to-Multipoint LSPs

- Understanding Point-to-Multipoint LSPs on page 733
- Point-to-Multipoint LSP Configuration Overview on page 735

Understanding Point-to-Multipoint LSPs

A point-to-multipoint MPLS label-switched path (LSP) is an RSVP-signaled LSP with a single source and multiple destinations. By taking advantage of the MPLS packet replication capability of the network, point-to-multipoint LSPs avoid unnecessary packet replication at the inbound (ingress) router. Packet replication takes place only when packets are forwarded to two or more different destinations requiring different network paths.

This process is illustrated in Figure 87 on page 734. Router PE1 is configured with a point-to-multipoint LSP to Routers PE2, PE3, and PE4. When Router PE1 sends a packet on the point-to-multipoint LSP to Routers P1 and P2, Router P1 replicates the packet and forwards it to Routers PE2 and PE3. Router P2 sends the packet to Router PE4.
The following are some of the properties of point-to-multipoint LSPs:

- A point-to-multipoint LSP allows you to use MPLS for point-to-multipoint data distribution. This functionality is similar to that provided by IP multicast.
- You can add and remove branch LSPs from a main point-to-multipoint LSP without disrupting traffic. The unaffected parts of the point-to-multipoint LSP continue to function normally.
- You can configure a node to be both a transit and an outbound (egress) router for different branch LSPs of the same point-to-multipoint LSP.
- You can enable link protection on a point-to-multipoint LSP. Link protection can provide a bypass LSP for each of the branch LSPs that make up the point-to-multipoint LSP. If any primary paths fail, traffic can be quickly switched to the bypass.
- You can configure sub-paths either statically or dynamically.
- You can enable graceful restart on point-to-multipoint LSPs.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- MPLS Traffic Engineering and Signaling Protocols Overview on page 719
To set up a point-to-multipoint LSP:

1. Configure the primary LSP from the ingress router and the branch LSPs that carry traffic to the egress routers.
2. Specify a path name on the primary LSP and this same path name on each branch LSP.

**NOTE:** By default, the branch LSPs are dynamically signaled by means of CSPF and require no configuration. You can alternatively configure the branch LSPs as a static path.

**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Understanding Point-to-Multipoint LSPs on page 733
- Configuring Primary and Branch LSPs for Point-to-Multipoint LSPs in the Junos MPLS Applications Configuration Guide
Chapter 29
MPLS VPNs

- MPLS VPN Overview on page 737
- MPLS Layer 2 VPNs on page 740
- MPLS Layer 3 VPNs on page 750
- MPLS Layer 2 Circuits on page 753

MPLS VPN Overview

Virtual private networks (VPNs) are private networks that use a public network to connect two or more remote sites. Instead of dedicated connections between networks, VPNs use virtual connections routed (tunneled) through public networks that are typically service provider networks. VPNs are a cost-effective alternative to expensive dedicated lines. The type of VPN is determined by the connections it uses and whether the customer network or the provider network performs the virtual tunneling.

You can configure routers running JUNOS Software to participate in several types of VPNs. This topic discusses MPLS VPNs.

This topic contains the following sections:
- MPLS VPN Topology on page 737
- MPLS VPN Routing on page 738
- VRF Instances on page 738
- Route Distinguishers on page 739

MPLS VPN Topology

There are many ways to set up an MPLS VPN and direct traffic through it. Figure 88 on page 738 shows a typical MPLS VPN topology.
There are three primary types of MPLS VPNs: Layer 2 VPNs, Layer 2 circuits, and Layer 3 VPNs. All types of MPLS VPNs share certain components:

- The provider edge (PE) routers in the provider's network connect to the customer edge (CE) routers located at customer sites. PE routers support VPN and MPLS label functionality. Within a single VPN, pairs of PE routers are connected through a virtual tunnel, typically a label-switched path (LSP).
- Provider routers within the core of the provider's network are not connected to any routers at a customer site but are part of the tunnel between pairs of PE routers. Provider routers support LSP functionality as part of the tunnel support, but do not support VPN functionality.
- CE routers are the routers or switches located at the customer site that connect to the provider's network. CE routers are typically IP routers, but they can also be Asynchronous Transfer Mode (ATM), Frame Relay, or Ethernet switches.

All VPN functions are performed by the PE routers. Neither CE routers nor provider routers are required to perform any VPN functions.

**MPLS VPN Routing**

VPNs tunnel traffic as follows from one customer site to another customer site, using a public network as a transit network, when certain requirements are met:

1. Traffic is forwarded by standard IP forwarding from the CE routers to the PE routers.
2. The PE routers establish an LSP through the provider network.
3. The inbound PE router receives traffic, and it performs a route lookup. The lookup yields an LSP next hop, and the traffic is forwarded along the LSP.
4. The traffic reaches the outbound PE router, and the PE router pops the MPLS label and forwards the traffic with standard IP routing.

**VRF Instances**

A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. The interfaces belong to the routing tables, and the routing protocol
parameters control the information in the routing tables. In the case of MPLS VPNs, each VPN has a VPN routing and forwarding (VRF) instance.

A **VRF instance** consists of one or more routing tables, a derived forwarding table, the interfaces that use the forwarding table, and the policies and routing protocols that determine what goes into the forwarding table. Because each instance is configured for a particular VPN, each VPN has separate tables, rules, and policies that control its operation.

A separate VRF table is created for each VPN that has a connection to a CE router. The VRF table is populated with routes received from directly connected CE sites associated with the VRF instance, and with routes received from other PE routers in the same VPN.

**Route Distinguishers**

Because a typical transit network is configured to handle more than one VPN, the provider routers are likely to have multiple VRF instances configured. As a result, depending on the origin of the traffic and any filtering rules applied to the traffic, the BGP routing tables can contain multiple routes for a particular destination address. Because BGP requires that exactly one BGP route per destination be imported into the forwarding table, BGP must have a way to distinguish between potentially identical network layer reachability information (NLRI) messages received from different VPNs.

A **route distinguisher** is a locally unique number that identifies all route information for a particular VPN. Unique numeric identifiers allow BGP to distinguish between routes that are otherwise identical.

Each routing instance that you configure on a PE router must have a unique route distinguisher. There are two possible formats:

- **as-number:number**, where **as-number** is an autonomous system (AS) number (a 2-byte value) in the range 1 through 65,535, and **number** is any 4-byte value. We recommend that you use an Internet Assigned Numbers Authority (IANA)-assigned, nonprivate AS number, preferably the ISP or the customer AS number.

- **ip-address:number**, where **ip-address** is an IP address (a 4-byte value) and **number** is any 2-byte value. The IP address can be any globally unique unicast address. We recommend that you use the address that you configure in the **router-id** statement, which is a public IP address in your assigned prefix range.

The **route target** defines which route is part of a VPN. A unique route target helps distinguish between different VPN services on the same router. Each VPN also has a policy that defines how routes are imported into the VRF table on the router. A Layer 2 VPN is configured with import and export policies. A Layer 3 VPN uses a unique route target to distinguish between VPN routes.

The PE router then exports the route in IBGP sessions to the other provider routers. Route export is governed by any routing policy that has been applied to the particular VRF table. To propagate the routes through the provider network, the PE router must also convert the route to VPN format, which includes the route distinguisher.
When the outbound PE router receives the route, it strips off the route distinguisher and advertises the route to the connected CE router, typically through standard BGP IPv4 route advertisements.

**Related Topics**

- [Junos OS Feature SupportReference for SRX Series and J Series Devices](#)
- Understanding MPLS Layer 2 VPNs on page 740
- Understanding MPLS Layer 3 VPNs on page 750
- Understanding MPLS Layer 2 Circuits on page 753
- VPN Overview in the [Junos VPNs Configuration Guide](#)

### MPLS Layer 2 VPNs

- Understanding MPLS Layer 2 VPNs on page 740
- MPLS Layer 2 VPN Configuration Overview on page 741
- Configuring Interfaces for MPLS VPNs (CLI Procedure) on page 742
- Configuring MPLS for VPNs (CLI Procedure) on page 744
- Configuring a BGP Session for MPLS VPNs (CLI Procedure) on page 744
- Configuring an IGP and the LDP Signaling Protocol (CLI Procedure) on page 745
- Configuring an IGP and the RSVP Signaling Protocol (CLI Procedure) on page 746
- Configuring Routing Options for MPLS VPNs (CLI Procedure) on page 747
- Configuring a Routing Instance for MPLS VPNs (CLI Procedure) on page 747
- Configuring a Routing Policy for MPLS Layer 2 VPNs (CLI Procedure) on page 748
- Verifying an MPLS Layer 2 VPN Configuration on page 749

### Understanding MPLS Layer 2 VPNs

In an MPLS Layer 2 VPN, traffic is forwarded to the provider edge (PE) router in Layer 2 format, carried by MPLS through an label-switched path (LSP) over the service provider network, and then converted back to Layer 2 format at the receiving customer edge (CE) router.

Routing occurs on the customer routers, typically on the CE router. The CE router connected to a service provider on a Layer 2 VPN must select the appropriate circuit on which to send traffic. The PE router receiving the traffic sends it across the network to the PE router on the outbound side. The PE routers need no information about the customer’s routes or routing topology, and need only to determine the virtual tunnel through which to send the traffic.

Implementing a Layer 2 VPN on the router is similar to implementing a VPN using a Layer 2 technology such as Asynchronous Transfer Mode (ATM) or Frame Relay.
**MPLS Layer 2 VPN Configuration Overview**

To configure MPLS Layer 2 VPN functionality on a router running JUNOS Software, you must enable support on the provider edge (PE) router and configure the PE router to distribute routing information to other routers in the VPN, as explained in the following steps. However, because the tunnel information is maintained at both PE routers, neither the provider core routers nor the customer edge (CE) routers need to maintain any VPN information in their configuration databases.

To configure an MPLS Layer 2 VPN:

1. Determine all of the routers that you want to participate in the VPN, and then complete the initial configuration of their interfaces. See the *Junos OS Interfaces Configuration Guide for Security Devices*.

2. For all of the routers in the VPN configuration, update the interface configurations to enable participation in the Layer 2 VPN. As part of the interface configuration, you must configure the MPLS address family for each interface that uses LDP or RSVP. See “Configuring Interfaces for MPLS VPNs (CLI Procedure)” on page 742.

3. For all of the routers in the VPN configuration, configure the appropriate protocols.
   a. MPLS—For PE routers and provider routers, use MPLS to advertise the Layer 2 VPN interfaces that communicate with other PE routers and provider routers. See “Configuring MPLS for VPNs (CLI Procedure)” on page 744.
   b. BGP and internal BGP (IBGP)—For PE routers, configure a BGP session to enable the routers to exchange information about routes originating and terminating in the VPN. (The PE routers use this information to determine which labels to use for traffic destined to the remote sites. The IBGP session for the VPN runs through the loopback address.) In addition, CE routers require a BGP connection to the PE routers. See “Configuring a BGP Session for MPLS VPNs (CLI Procedure)” on page 744.
   c. IGP and a signaling protocol—For PE routers, configure a signaling protocol (either LDP or RSVP) to dynamically set up label-switched paths (LSPs) through the provider network. (LDP routes traffic using IGP metrics. RSVP has traffic engineering that lets you override IGP metrics as needed.) You must use LDP or RSVP between PE routers and provider routers, but you cannot use them for interfaces between PE routers and CE routers.

In addition, configure an IGP such as OSPF or static routes for PE routers to enable exchanges of routing information between the PE routers and provider routers. Each PE router’s loopback address must appear as a separate route. Do not configure any summarization of the PE router’s loopback addresses at the area boundary. Configure the provider network to run OSPF or IS-IS.
as an IGP, as well as IBGP sessions through either a full mesh or route reflector.

See “Configuring an IGP and the LDP Signaling Protocol (CLI Procedure)” on page 745 and “Configuring an IGP and the RSVP Signaling Protocol (CLI Procedure)” on page 746.

4. For all of the routers in the VPN configuration, configure routing options. The only required routing option for VPNs is the AS number. You must specify it on each router involved in the VPN. See “Configuring Routing Options for MPLS VPNs (CLI Procedure)” on page 747.

5. For each PE router in the VPN configuration, configure a routing instance for each VPN. The routing instance should have the same name on each PE router. Each routing instance must have a unique route distinguisher associated with it. (VPN routing instances need a route distinguisher to help BGP distinguish between potentially identical network layer reachable information [NLRI] messages received from different VPNs.) See “Configuring a Routing Instance for MPLS VPNs (CLI Procedure)” on page 747.

6. For each PE router in the VPN configuration, configure a VPN routing policy if you are not using a route target. Within the policy, describe which packets are sent and received across the VPN and specify how routes are imported into and exported from the router's VRF table. Each advertisement must have an associated route target that uniquely identifies the VPN for which the advertisement is valid. If the routing instance uses a policy for accepting and rejecting packets instead of a route target, you must specify the import and export routing policies and the community on each PE router. See “Configuring a Routing Policy for MPLS Layer 2 VPNs (CLI Procedure)” on page 748.

Related Topics

■ Junos OS Feature Support Reference for SRX Series and J Series Devices
■ Verifying an MPLS Layer 2 VPN Configuration on page 749

Configuring Interfaces for MPLS VPNs (CLI Procedure)

Configuring the router interfaces that participate in the VPN is similar to configuring them for other uses, with a few requirements for the VPN. Perform the following tasks for each interface involved in the VPN, except Layer 3 loopback interfaces, which do not require other configuration.
To configure an interface for an MPLS VPN:

1. Configure IPv4 on all of the routers’ interfaces.
   - For all interfaces except loopback interfaces and Layer 2 VPN interfaces facing a CE router:
     ```
     [edit]
     user@host# edit interfaces interface-name unit logical_interface family inet
     address ipv4_address
     ```
   - For a loopback address on a Layer 2 configuration:
     ```
     [edit]
     user@host# edit interfaces lo0 unit logical_interface family inet address
     ipv4_address primary
     ```
   - For a Layer 2 VPN interface facing a CE router:
     ```
     [edit]
     user@host# set interfaces interface-name vlan-tagging encapsulation
     vlan-ccc unit logical_interface encapsulation vlan-ccc vlan-id id-number
     ```

2. Configure the MPLS address family on the PE router or provider router interfaces that communicate with other PE routers or provider routers (and not loopback addresses).
   ```
   [edit interfaces interface]
   user@host# set unit logical_interface family mpls
   ```

3. Configure encapsulation for the interfaces on the PE routers that communicate with the CE routers in Layer 2 VPNs and Layer 2 circuits. If multiple logical units are configured, the encapsulation type is needed at the interface level only. It is always required at the unit level.
   ```
   [edit interfaces interface]
   user@host# set encapsulation encapsulation_type
   user@host# set unit logical_interface encapsulation encapsulation_type
   ```

4. Commit the configuration if you are finished configuring the device.
   ```
   [edit]
   user@host# commit
   ```

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- MPLS Layer 2 VPN Configuration Overview on page 741
- MPLS Layer 3 VPN Configuration Overview on page 751
- MPLS Layer 2 Circuit Configuration Overview on page 754
Configuring MPLS for VPNs (CLI Procedure)

To configure MPLS for VPNs:

1. Specify the interfaces used for communication between PE routers and between PE routers and provider routers.

   [edit]
   user@host# edit protocols mpls interface interface-name

2. For RSVP only, configure the PE router interface communicating with another PE router.
   a. Configure an MPLS LSP to the destination point on the PE router. The path name is defined on the source router only and is unique between two routers.

      [edit protocols mpls]
      user@host# edit label-switched-path path-name

   b. Specify the IP address of the LSP destination point, which is an address on the remote PE router.

      [edit edit protocols mpls label-switched-path path-name ]
      user@host# set to ip-address

3. Commit the configuration if you are finished configuring the device.

   [edit]
   user@host# commit

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- MPLS Layer 2 VPN Configuration Overview on page 741
- MPLS Layer 3 VPN Configuration Overview on page 751
- MPLS Layer 2 Circuit Configuration Overview on page 754

Configuring a BGP Session for MPLS VPNs (CLI Procedure)

NOTE: This section is valid for Layer 2 VPNs and Layer 3 VPNs, but not Layer 2 circuits.

To configure an IBGP session, perform the following steps on each PE router:

1. Configure BGP.

   [edit]
   user@host# edit protocols bgp group group-name

2. Set the BGP type to internal.

   [edit protocols bgp group group-name]
user@host# set type internal

3. Specify the loopback interface.
   
   [edit protocols bgp group group-name]
   user@host# set local-address loopback-interface-ip-address

4. Set the Layer 2 or Layer 3 VPN family type to unicast.
   
   [edit protocols bgp group group-name]
   user@host# set family family-type unicast

Replace family-type with l2vpn for a Layer 2 VPN or inet-vpn for a Layer 3 VPN.

5. Enter the loopback address of the neighboring PE router.
   
   [edit protocols bgp]
   user@host# set neighbor ip-address

6. Commit the configuration if you are finished configuring the device.
   
   [edit]
   user@host# commit

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- MPLS Layer 2 VPN Configuration Overview on page 741
- MPLS Layer 3 VPN Configuration Overview on page 751

Configuring an IGP and the LDP Signaling Protocol (CLI Procedure)

The following example shows how to configure LDP and OSPF on PE routers and provider routers. Within the example, you specify which interfaces to enable for LDP. Perform this step on each PE router interface and provider router interface that communicates with other PE routers and provider routers. For OSPF, you configure at least one area on at least one of the router's interfaces. (An AS can be divided into multiple areas.) This example uses the backbone area 0.0.0.0. The example also shows how to enable traffic engineering for Layer 2 VPN circuits.

To configure LDP and OSPF:

1. Enable the ldp protocol.
   
   [edit]
   user@host# edit protocols ldp

   NOTE: You must configure the IGP at the [protocols] level of the configuration hierarchy, not within the routing instance at the [routing-instances] level of the configuration hierarchy.

2. Specify which interfaces to enable for LDP.
   
   [edit protocols ldp]
To configure RSVP and OSPF:

1. Configure OSPF with traffic engineering support on the PE routers.
   
   ```
   [edit]
   user@host# edit protocols ospf traffic-engineering shortcuts
   ```

   **NOTE:** You must configure the IGP at the [edit protocols] level, not within the routing instance at the [edit routing-instances] level.

2. Enable RSVP on interfaces that participate in the LSP. For PE routers, enable interfaces on the source and destination points. For provider routers, enable interfaces that connect the LSP between the PE routers.
   
   ```
   [edit]
   user@host# edit protocols rsvp interface interface-name
   ```

3. Commit the configuration if you are finished configuring the device.
   
   ```
   [edit]
   user@host# commit
   ```

**Related Topics**
- [Junos OS Feature Support Reference for SRX Series and J Series Devices](#)
- MPLS Layer 2 VPN Configuration Overview on page 741
- MPLS Layer 3 VPN Configuration Overview on page 751
- MPLS Layer 2 Circuit Configuration Overview on page 754
Configuring Routing Options for MPLS VPNs (CLI Procedure)

To configure routing options for a VPN:
1. Configure the AS number.
   ```
   [edit]
   user@host# set routing-options autonomous-system as-number
   ```

2. Commit the configuration if you are finished configuring the device.
   ```
   [edit]
   user@host# commit
   ```

Configuring a Routing Instance for MPLS VPNs (CLI Procedure)

To configure a VPN routing instance on each PE router:
1. Create the routing instance.
   ```
   [edit]
   user@host# edit routing-instances routing-instance-name
   ```

2. Create a routing instance description. (This text appears in the output of the `show route instance detail` command.)
   ```
   [edit routing-instances routing-instance-name]
   user@host# set description "text"
   ```

3. Specify the instance type, either l2vpn for Layer 2 VPNs or vrf for Layer 3 VPNs.
   ```
   [edit routing-instances routing-instance-name]
   user@host# set instance-type instance-type
   ```

4. Specify the interface of the remote PE router.
   ```
   [edit routing-instances routing-instance-name]
   user@host# set interface interface-name
   ```

5. Specify the route distinguisher using one of the following commands:
   ```
   [edit routing-instances routing-instance-name]
   user@host# set route-distinguisher-as-number:as-number
   ```
6. Specify the policy for the Layer 2 VRF table.

   [edit routing-instances routing-instance-name]
   set route-distinguisher ip-address:number

7. Specify the policy for the Layer 3 VRF table.

   [edit routing-instances routing-instance-name]
   set vrf-import import-policy-name vrf-export export-policy-name

   Where community-id is either as-number:number or ip-address:number.

8. Commit the configuration if you are finished configuring the device.

   [edit]
   user@host# commit

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- MPLS Layer 2 VPN Configuration Overview on page 741
- MPLS Layer 3 VPN Configuration Overview on page 751

Configuring a Routing Policy for MPLS Layer 2 VPNs (CLI Procedure)

This example shows how to configure a Layer 2 VPN routing policy on the PE routers in the VPN.

After configuring an import routing policy for a Layer 2 VPN, configure an export routing policy for the Layer 2 VPN. Configure this export policy on the PE routers in the VPN. The export routing policy defines how routes are exported from the PE router routing table. An export policy is applied to routes sent to other PE routers in the VPN. The export policy must also evaluate all routes received over the routing protocol session with the CE router. The export policy must also contain a second term for rejecting all other routes.

To configure a Layer 2 VPN routing policy on a PE router:

1. Configure the import routing policy.

   [edit]
   user@host# edit policy-options policy-statement import-policy-name

2. Define the import policy’s term for accepting packets.

   [edit edit policy-options policy-statement import-policy-name]
   user@host# set term term-name-accept from protocol bgp community community-name
   user@host# set term term-name-accept then accept

3. Define the import policy’s term for rejecting packets.

   [edit edit policy-options policy-statement import-policy-name]
   user@host# set term term-name-reject then reject
4. Configure the export routing policy.

    [edit]
    user@host# edit policy-options policy-statement export-policy-name

5. Define the export policy’s term for accepting packets.

    [edit policy-options policy-statement export-policy-name]
    user@host# set term term-name-accept from community add community-name
    user@host# set term term-name-accept then accept

6. Define the export policy’s term for rejecting packets.

    [edit policy-options policy-statement export-policy-name]
    user@host# set term term-name-reject from community add community-name
    user@host# set term term-name-reject then reject

7. Define the export policy’s community using one of the following commands.

    [edit policy-options policy-statement export-policy-name]
    user@host# community community-name target: as-number
    user@host# community community-name target: ip-address: number

8. Commit the configuration if you are finished configuring the device.

    [edit]
    user@host# commit

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- MPLS Layer 2 VPN Configuration Overview on page 741
- MPLS Layer 3 VPN Configuration Overview on page 751

Verifying an MPLS Layer 2 VPN Configuration

Purpose

Verify the connectivity of MPLS Layer 2 VPNs using the ping mpls command. This command helps to verify that a VPN has been enabled by testing the integrity of the VPN connection between the PE routers. It does not test the connection between a PE router and CE router.

Action

- To ping an interface configured for the Layer 2 VPN on the PE router, use the following command:
  
  ping mpls l2vpn interface interface-name

- To ping a combination of the Layer 2 VPN routing instance name, the local site identifier, and the remote site identifier to test the integrity of the Layer 2 VPN connection (specified by identifiers) between the two PE routers, use the following command:
  
  ping mpls l2vpn instance l2vpn-instance-name local-site-id local-site-id-number remote-site-id remote-site-id-number
MPLS Layer 3 VPNs

Understanding MPLS Layer 3 VPNs on page 750
MPLS Layer 3 VPN Configuration Overview on page 751
Configuring a Routing Policy for MPLS Layer 3 VPNs (CLI Procedure) on page 752
Verifying an MPLS Layer 3 VPN Configuration on page 753

Understanding MPLS Layer 3 VPNs

An MPLS Layer 3 VPN operates at the Layer 3 level of the OSI model, the Network layer. The VPN is composed of a set of sites that are connected over a service provider’s existing public Internet backbone. The sites share common routing information and the connectivity of the sites is controlled by a collection of policies.

In an MPLS Layer 3 VPN, routing occurs on the service provider’s routers. The provider routers route and forward VPN traffic at the entry and exit points of the transit network. The service provider network must learn the IP addresses of devices sending traffic across the VPN and the routes must be advertised and filtered throughout the provider network. As a result, Layer 3 VPNs require information about customer routes and a more extensive VPN routing and forwarding (VRF) policy configuration than a Layer 2 VPN. This information is used to share and filter routes that originate or terminate in the VPN.

The MPLS Layer 3 VPN requires more processing power on the provider edge (PE) routers than a Layer 2 VPN, because the Layer 3 VPN has larger routing tables for managing network traffic on the customer sites. Route advertisements originate at the customer edge (CE) routers and are shared with the inbound PE routers through standard IP routing protocols, typically BGP. Based on the source address, the PE router filters route advertisements and imports them into the appropriate VRF table.

The provider router uses OSPF and LDP to communicate with the PE routers. For OSPF, the provider router interfaces that communicate with the PE routers are specified, as well as the loopback interface. For the PE routers, the loopback interface is in passive mode, meaning it does not send OSPF packets to perform the control function.
To configure MPLS Layer 3 VPN functionality on a router running JUNOS Software, you must enable support on the provider edge (PE) router and configure the PE router to distribute routing information to other routers in the VPN, as explained in the following steps. However, because the tunnel information is maintained at both PE routers, neither the provider core routers nor the customer edge (CE) routers need to maintain any VPN information in their configuration databases.

To configure an MPLS Layer 3 VPN:

1. Determine all of the routers that you want to participate in the VPN, and then complete the initial configuration of their interfaces. See the Junos OS Interfaces Configuration Guide for Security Devices.

2. For all of the routers in the VPN configuration, update the interface configurations to enable participation in the Layer 3 VPN. As part of the interface configuration, you must configure the MPLS address family for each interface that uses LDP or RSVP. See “Configuring Interfaces for MPLS VPNs (CLI Procedure)” on page 742.

3. For all of the routers in the VPN configuration, configure the appropriate protocols.
   a. MPLS—If you are using RSVP, use MPLS to advertise the Layer 3 VPN interfaces on the PE routers and provider routers that communicate with other PE routers and provider routers. See “Configuring MPLS for VPNs (CLI Procedure)” on page 744.
   b. BGP, EBGP, and internal BGP (IBGP)—For PE routers, configure a BGP session to enable the routers to exchange information about routes originating and terminating in the VPN. (The PE routers use this information to determine which labels to use for traffic destined to the remote sites. The IBGP session for the VPN runs through the loopback address.) In addition, CE routers require a BGP connection to the PE routers. See “Configuring a BGP Session for MPLS VPNs (CLI Procedure)” on page 744.
   c. IGP and a signaling protocol—For PE routers and provider, configure a signaling protocol (either LDP or RSVP) to dynamically set up label-switched paths (LSPs) through the provider network. (LDP routes traffic using IGP metrics. RSVP has traffic engineering that lets you override IGP metrics as needed.) You must use LDP or RSVP between PE routers and provider routers, but cannot use them for interfaces between PE routers and CE routers.

In addition, configure an IGP such as OSPF or static routes on the PE routers in order to enable exchanges of routing information between the PE routers and provider routers. Each PE router’s loopback address must appear as a separate route. Do not configure any summarization of the PE router’s loopback addresses at the area boundary. Configure the provider network to run OSPF or IS-IS as an IGP, as well as IBGP sessions through either a full mesh or route reflector.
See “Configuring an IGP and the LDP Signaling Protocol (CLI Procedure)” on page 745 and “Configuring an IGP and the RSVP Signaling Protocol (CLI Procedure)” on page 746.

4. For all of the routers in the VPN configuration, configure routing options. The only required routing option for VPNs is the autonomous system (AS) number. You must specify it on each router involved in the VPN. See “Configuring Routing Options for MPLS VPNs (CLI Procedure)” on page 747.

5. For each PE router in the VPN configuration, configure a routing instance for each VPN. The routing instance should have the same name on each PE router. Each routing instance must have a unique route distinguisher associated with it. (VPN routing instances need a route distinguisher to help BGP distinguish between potentially identical network layer reachable information [NLRI] messages received from different VPNs.) See “Configuring a Routing Instance for MPLS VPNs (CLI Procedure)” on page 747.

6. For CE routers, configure a routing policy. In addition, if you are not using a route target, configure a VPN routing policy for each PE router in the VPN configuration. Within the policy, describe which packets are sent and received across the VPN and specify how routes are imported into and exported from the router’s VRF table. Each advertisement must have an associated route target that uniquely identifies the VPN for which the advertisement is valid. See “Configuring a Routing Policy for MPLS Layer 3 VPNs (CLI Procedure)” on page 752.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Verifying an MPLS Layer 3 VPN Configuration on page 753

**Configuring a Routing Policy for MPLS Layer 3 VPNs (CLI Procedure)**

To configure a Layer 3 VPN routing policy on a CE router:

1. Configure the routing policy for the loopback interface.

   ```
   [edit]
   user@host# edit policy-options policy-statement policy-name
   ```

2. Define the term for accepting packets.

   ```
   [edit policy-options policy-statement policy-name]
   user@host# set term term-name-accept from protocol direct route-filter
   local-loopback-address/netmask exact
   ```

3. Define the term for rejecting packets.

   ```
   [edit policy-options policy-statement policy-name]
   user@host# set term-term-name-reject then reject
   ```

4. Commit the configuration if you are finished configuring the device.

   ```
   [edit]
   user@host# commit
   ```
**Verifying an MPLS Layer 3 VPN Configuration**

**Purpose**
Verify the connectivity of MPLS Layer 3 VPNs using the `ping mpls` command. This command helps to verify that a VPN has been enabled by testing the integrity of the VPN connection between the source and destination routers. The destination prefix corresponds to a prefix in the Layer 3 VPN. However, ping tests only whether the prefix is present in a PE VRF table.

**Action**
To a combination of a IPv4 destination prefix and a Layer 3 VPN name on the destination PE router, use the following command:

```
ping mpls l3vpn l3vpn-name prefix prefix count count
```

**MPLS Layer 2 Circuits**

**Understanding MPLS Layer 2 Circuits**

An MPLS Layer 2 circuit is a point-to-point Layer 2 connection that transports traffic by means of MPLS or another tunneling technology on the service provider network. The Layer 2 circuit creates a virtual connection to direct traffic between two customer edge (CE) routers across a service provider network. The main difference between a Layer 2 VPN and a Layer 2 circuit is the method of setting up the virtual connection. As with a leased line, a Layer 2 circuit forwards all packets received from the local interface to the remote interface.

Each Layer 2 circuit is represented by the logical interface connecting the local provider edge (PE) router to the local CE router. All Layer 2 circuits using a particular remote PE router neighbor is identified by its IP address and is usually the endpoint destination for the label-switched path (LSP) tunnel transporting the Layer 2 circuit.

Each virtual circuit ID uniquely identifies the Layer 2 circuit among all the Layer 2 circuits to a specific neighbor. The key to identifying a particular Layer 2 circuit on a PE router is the neighbor address and the virtual circuit ID. Based on the virtual
circuit ID and the neighbor relationship, an LDP label is bound to an LDP circuit. LDP uses the binding for sending traffic on that Layer 2 circuit to the remote CE router.

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- MPLS VPN Overview on page 737
- MPLS Layer 2 Circuit Configuration Overview on page 754
- Layer 2 Circuit Overview in the Junos VPNs Configuration Guide

**MPLS Layer 2 Circuit Configuration Overview**

To configure an MPLS Layer 2 circuit:

1. Determine all of the routers that you want to participate in the circuit, and then complete the initial configuration of their interfaces. See the Junos OS Interfaces Configuration Guide for Security Devices.

2. For all of the routers in the circuit configuration, update the interface configurations to enable participation in the Layer 2 circuit.
   a. On the interface communicating with the other provider edge (PE) router, specify MPLS and IPv4, and include the IP address. For the loopback interface, specify `inet`, and include the IP address. For IPv4, designate the loopback interface as primary so it can receive control packets. (Because it is always operational, the loopback interface is best able to perform the control function.)
   b. On the PE router interface facing the customer edge (CE) router, specify a circuit cross-connect (CCC) encapsulation type. The type of encapsulation depends on the interface type. For example, an Ethernet interface uses `ethernet-ccc`. (The encapsulation type determines how the packet is constructed for that interface.)
   c. On the CE router interface that faces the PE router, specify `inet` (for IPv4), and include the IP address. In addition, specify a routing protocol such as Open Shortest Path First (OSPF), which specifies the area and IP address of the router interface.

   See “Configuring Interfaces for MPLS VPNs (CLI Procedure)” on page 742.

3. For all of the routers in the circuit configuration, configure the appropriate protocols.
   a. MPLS—For PE routers and provider routers, use MPLS to advertise the Layer 2 circuit interfaces that communicate with other PE routers and provider routers. See “Configuring MPLS for VPNs (CLI Procedure)” on page 744.
   b. BGP—For PE routers, configure a BGP session.
   c. IGP and a signaling protocol—For PE routers, configure a signaling protocol (either LDP or RSVP) to dynamically set up label-switched paths (LSPs) through the provider network. (LDP routes traffic using IGP metrics. RSVP has traffic engineering that lets you override IGP metrics as needed.) You
must use LDP or RSVP between PE routers and provider routers, but cannot
use them for interfaces between PE routers and CE routers.

In addition, configure an IGP such as OSPF or static routes on the PE routers
to enable exchanges of routing information between the PE routers and
provider routers. Each PE router's loopback address must appear as a
separate route. Do not configure any summarization of the PE router's
loopback addresses at the area boundary. Configure the provider network
to run OSPF or IS-IS as an IGP, as well as IBGP sessions through either a full
mesh or route reflector.

See “Configuring an IGP and the LDP Signaling Protocol (CLI Procedure)” on
page 745 and “Configuring an IGP and the RSVP Signaling Protocol (CLI
Procedure)” on page 746.

4. For all of the routers in the circuit configuration, configure routing options. The
only required routing option for circuits is the autonomous system (AS) number.
You must specify it on each router involved in the circuit. See “Configuring
Routing Options for MPLS VPNs (CLI Procedure)” on page 747.

5. For PE routers, configure Layer 2 circuits on the appropriate interfaces. See
“Configuring an MPLS Layer 2 Circuit (CLI Procedure)” on page 755.

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Verifying an MPLS Layer 2 Circuit Configuration on page 756

**Configuring an MPLS Layer 2 Circuit (CLI Procedure)**

To configure a Layer 2 circuit on a PE router:

1. Enable a Layer 2 circuit on the appropriate interface.

   ```
   [edit]
   user@host# edit protocols l2circuit neighbor interface-name interface
   interface-name
   ```

2. Enter the circuit ID number.

   ```
   [edit protocols l2circuit neighbor interface-name interface interface-name]
   user@host# set virtual-circuit-id id-number
   ```

   For **neighbor**, specify the local loopback address, and for **interface**, specify the
   interface name of the remote PE router.

3. Commit the configuration if you are finished configuring the device.

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

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- MPLS Layer 2 Circuit Configuration Overview on page 754
Verifying an MPLS Layer 2 Circuit Configuration

**Purpose**  
To verify the connectivity of MPLS Layer 2 circuits, use the `ping mpls` command. This command helps to verify that the circuit has been enabled by testing the integrity of the Layer 2 circuit between the source and destination routers.

**Action**  
- To ping an interface configured for the Layer 2 circuit on the PE router, enter the following command:
  
  ```
  ping mpls l2circuit interface interface-name
  ```

- To ping a combination of the IPv4 prefix and the virtual circuit ID on the destination PE router, enter the following command:
  
  ```
  ping mpls l2circuit virtual-circuit prefix virtual-circuit-id
  ```

**Related Topics**  
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- MPLS Layer 2 Circuit Configuration Overview on page 754
Chapter 30

CLNS VPNs

- CLNS Overview on page 757
- CLNS Configuration Overview on page 758
- Example: Configuring a VPN Routing Instance for CLNS (CLI) on page 759
- ES-IS for CLNS on page 760
- IS-IS for CLNS on page 761
- Static Routes for CLNS on page 763
- BGP for CLNS VPNs on page 764
- Verifying a CLNS VPN Configuration on page 765

CLNS Overview

Connectionless Network Service (CLNS) is a Layer 3 protocol similar to IP version 4 (IPv4) for linking hosts (end systems) with routers (intermediate systems) in an Open Systems Interconnection (OSI) network. CLNS and its related OSI protocols, Intermediate System-to-Intermediate System (IS-IS) and End System-to-Intermediate System (ES-IS), are International Organization for Standardization (ISO) standards.

You can configure devices running JUNOS Software as provider edge (PE) routers within a CLNS network. CLNS networks can be connected over an IP MPLS network core using Border Gateway Protocol (BGP) and MPLS Layer 3 virtual private networks (VPNs). See RFC 2547, BGP/MPLS VPNs.

CLNS uses network service access points (NSAPs), similar to IP addresses found in IPv4, to identify end systems (hosts) and intermediate systems (routers). ES-IS enables the hosts and routers to discover each other. IS-IS is the interior gateway protocol (IGP) that carries ISO CLNS routes through a network.

For more information about CLNS, see the ISO 8473 standards.

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- CLNS Configuration Overview on page 758
- Understanding ES-IS for CLNS on page 760
- Understanding IS-IS for CLNS on page 762
**CLNS Configuration Overview**

To configure CLNS:

1. Configure the network interfaces. See the *Junos OS Interfaces Configuration Guide for Security Devices*.

2. If applicable, configure BGP and VPNs. See:
   - Example: Configuring BGP for CLNS VPNs on page 764
   - MPLS Layer 2 VPN Configuration Overview on page 741
   - MPLS Layer 3 VPN Configuration Overview on page 751


4. Configure one or more of the following protocols for CLNS (depending on your network).
   - **ES-IS**—If a device is a PE router within a CLNS island that contains any end systems, you must configure ES-IS on the device. If a CLNS island does not contain any end systems, you do not need to configure ES-IS on a device. See “Example: Configuring ES-IS for CLNS” on page 761.

   **NOTE:** ES-IS is enabled only if either ES-IS or IS-IS is configured on the router. ES-IS must not be disabled. If ES-IS is not explicitly configured, the interface sends and receives only intermediate system hello (ISH) messages. If ES-IS is explicitly configured and disabled, the interface does not send or receive ES-IS packets. If ES-IS is explicitly configured and not disabled, the interface sends and receives ISH messages as well as ES-IS packets.

   One of the interfaces that is configured for ES-IS must be configured with an ISO address for hello messages. The ISO address family must be configured on an interface to support ES-IS on that interface.

   - **IS-IS**—You can configure IS-IS to exchange CLNS routes within a CLNS island. See “Example: Configuring IS-IS for CLNS” on page 762.

   **NOTE:** If you have a pure CLNS island—an island that does not contain any IP devices—you must disable IPv4 and IPv6 routing. Also, to export BGP routes into IS-IS, you must configure and apply an export policy.
Static routes—If some devices in your network do not support IS-IS, you must configure CLNS static routes. You can use static routing with or without IS-IS. You might also consider using static routes if your network is simple. See “Example: Configuring Static Routes for CLNS” on page 763.

BGP—See “Example: Configuring BGP for CLNS VPNs” on page 764.

NOTE: Many of the configuration statements used to configure CLNS and routing protocols can be included at different hierarchy levels in the configuration. For more information, see the Junos Routing Protocols Configuration Guide.

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- CLNS Overview on page 757
- Verifying a CLNS VPN Configuration on page 765

Example: Configuring a VPN Routing Instance for CLNS (CLI)

The following example shows how to create a CLNS routing instance called aaaa and set the instance type to VRF for Layer 3 VPNs. Within the example, you specify that the lo0.1 interface, e1–2/0/0.0 interface, and t1–3/0/0.0 interface all belong to the routing instance. The route distinguisher is set as 10.255.245.1:1 and the policy for the Layer 3 VRF table is set as target:11111:1.

To configure a VPN routing instance:

1. Create the routing instance.
   
   [edit]
   user@host# edit routing-instances aaaa

2. Specify the routing instance type.
   
   [edit routing-instances aaaa]
   user@host# set instance-type vrf

3. Specify the interfaces that belong to the routing instance.
   
   [edit routing-instances aaaa]
   user@host# set interface lo0.1
   user@host# set interface e1–2/0/0.0
   user@host# set interface t1–3/0/0.0

4. Specify the route distinguisher.
   
   [edit routing-instances aaaa]
   user@host# set route-distinguisher 10.255.245.1:1

5. Specify the policy for the Layer 3 VRF table.
   
   [edit routing-instances aaaa]
   user@host# set vrf-target target:11111:1
6. Commit the configuration if you are done configuring the device.

   [edit]
   user@host# commit

---

**ES-IS for CLNS**

- Understanding ES-IS for CLNS on page 760
- Example: Configuring ES-IS for CLNS (CLI) on page 761

**Understanding ES-IS for CLNS**

End System-to-Intermediate System (ES-IS) is a protocol that resolves Layer 3 ISO network service access points (NSAP) to Layer 2 addresses. ES-IS has an equivalent role as Address Resolution Protocol (ARP) in IP version 4 (IPv4).

ES-IS provides the basic interaction between Connectionless Network Service (CLNS) hosts (end systems) and routers (intermediate systems). ES-IS allows hosts to advertise NSAP addresses to other routers and hosts attached to the network. Those routers can then advertise the address to the rest of the network by using Intermediate System-to-Intermediate System (IS-IS). Routers use ES-IS to advertise their network entity title (NET) to hosts and routers that are attached to that network.

ES-IS routes are exported to Layer 1 IS-IS by default. You can also export ES-IS routes into Layer 2 IS-IS by configuring a routing policy. ES-IS generates and receives end system hello (ESH) hello messages when the protocol is configured on an interface. ES-IS is a resolution protocol that allows a network to be fully ISO integrated at both the network layer and the data layer.

The resolution of Layer 3 ISO NSAPs to Layer 2 subnetwork point of attachments (SNPAs) by ES-IS is equivalent to ARP within an IPv4 network. If a device is a provider edge (PE) router within a CLNS island that contains any end systems, you must configure ES-IS on the device.

For more information about ES-IS, see the ISO 9542 standard.
**Example: Configuring ES-IS for CLNS (CLI)**

In the following example, you create a routing instance called aaaa and enable ES-IS on all interfaces. You set the end system configuration timer for the interfaces to 180, set the graceful restart duration to 180, and set a preference value for ES-IS.

To configure ES-IS:

1. Create the routing instance.
   ```
   [edit]
   user@host# edit routing-instances aaaa
   ```

2. Enable ES-IS on all interfaces.
   ```
   [edit routing-instances aaaa]
   user@host# set protocols esis interface all
   ```

3. Configure the end system configuration timer.
   ```
   [edit routing-instances aaaa]
   user@host# set protocols esis interface all end-system-configuration-timer 180
   ```

4. Configure graceful restart.
   ```
   [edit routing-instances aaaa]
   user@host# set protocols esis graceful-restart restart-duration 180
   ```

5. Configure the preference value.
   ```
   [edit routing-instances aaaa]
   user@host# set protocols esis preference value
   ```

6. Commit the configuration if you are done configuring the device.
   ```
   [edit]
   user@host# commit
   ```

**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- CLNS Configuration Overview on page 758
- Understanding ES-IS for CLNS on page 760
- Verifying a CLNS VPN Configuration on page 765

**IS-IS for CLNS**

- Understanding IS-IS for CLNS on page 762
- Example: Configuring IS-IS for CLNS (CLI) on page 762
Understanding IS-IS for CLNS

Intermediate System-to-Intermediate System (IS-IS) extensions provide the basic interior gateway protocol (IGP) support for collecting intradomain routing information for Connectionless Network Service (CLNS) destinations within a CLNS network. Routers that learn host addresses through End System-to-Intermediate System (ES-IS) can advertise the addresses to other routers (intermediate systems) by using IS-IS.

For more information about IS-IS, see the ISO 10589 standard.

Example: Configuring IS-IS for CLNS (CLI)

To configure IS-IS for CLNS:

1. Configure the routing instance.
   
   ```
   [edit]
   user@host# edit routing-instances aaaa
   ```

2. Enable CLNS routing.
   
   ```
   [edit routing-instances aaaa]
   user@host# set protocols isis clns-routing
   ```

3. Enable IS-IS on all interfaces.
   
   ```
   [edit routing-instances aaaa]
   user@host# set protocols isis interface all
   ```

4. (Optional) Disable IPv4 and IPv6 routing to configure a pure CLNS network.
   
   ```
   [edit routing-instances aaaa]
   user@host# set protocols isis no-ipv4-routing no-ipv6-routing
   ```

5. Define the BGP export policy name—for example, dist-bgp—and the family and protocol.
   
   ```
   [edit]
   user@host# set policy-options policy-statement dist-bgp from family iso protocol bgp
   ```

6. Define the action for the export policy.
   
   ```
   [edit]
   user@host# set policy-options policy-statement dist-bgp then accept
   ```

7. Apply the export policy to IS-IS.
   
   ```
   [edit]
   user@host# set routing-instances aaaa protocols isis export dist-bgp
   ```
8. Commit the configuration if you are done configuring the device.

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

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- CLNS Configuration Overview on page 758
- Understanding IS-IS for CLNS on page 762
- Configuring CLNS for IS-IS in the Junos Routing Protocols Configuration Guide
- clns-routing in the Junos Routing Protocols Configuration Guide
- Verifying a CLNS VPN Configuration on page 765

**Static Routes for CLNS**

- Understanding Static Routes for CLNS on page 763
- Example: Configuring Static Routes for CLNS (CLI) on page 763

**Understanding Static Routes for CLNS**

You can configure static routes to exchange Connectionless Network Service (CLNS) routes within a CLNS island. A **CLNS island** is typically an IS-IS level 1 area that is part of a single IGP routing domain. An island can contain more than one area. CLNS islands can be connected by VPNs.

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- CLNS Overview on page 757
- Example: Configuring Static Routes for CLNS on page 763

**Example: Configuring Static Routes for CLNS (CLI)**

This procedure uses the following ISO NET address and NSAP prefix:

- `47.0005.80ff.f800.0000.aaaa.1000.1921.6800.4196.00`
- `47.0005.80ff.f800.0000.bbbb.1022/104`

To configure CLNS static routes:
1. Configure the routing instance.
   ```
   [edit]
   user@host# edit routing-instances aaaa
   ```
2. Configure the next-hop ISO NET address for an NSAP prefix.
   ```
   [edit routing-instances aaaa]
   ```
user@host# set routing-options iso-route
47.0005.80ff.f800.0000.bbbb.1022/104 next-hop
47.0005.80ff.f800.0000.aaaa.1000.1921.6800.4196.00

3. Commit the configuration if you are done configuring the device.

[edit]
user@host# commit

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- CLNS Configuration Overview on page 758
- Understanding Static Routes for CLNS on page 763
- Configuring CLNS Static Routes in the Junos Routing Protocols Configuration Guide
- Verifying a CLNS VPN Configuration on page 765

BGP for CLNS VPNs

- Understanding BGP for CLNS VPNs on page 764
- Example: Configuring BGP for CLNS VPNs (CLI) on page 764

Understanding BGP for CLNS VPNs

Border Gateway Protocol (BGP) extensions allow BGP to carry Connectionless Network Service (CLNS) virtual private network (VPN) network layer reachability information (NLRI) between provider edge (PE) routers. Each CLNS route is encapsulated into a CLNS VPN NLRI and propagated between remote sites in a VPN.

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- CLNS Overview on page 757
- Example: Configuring BGP for CLNS VPNs on page 764

Example: Configuring BGP for CLNS VPNs (CLI)

In this example, you create a BGP group called pedge-pedge, define the 10.255.245.215 BGP peer neighbor address for the group, and define the family.

To configure BGP to carry CLNS VPN NLRI:
1. Configure BGP.

[edit]
user@host# set protocols bgp group pedge-pedge neighbor 10.255.245.215 family iso-vpn unicast
2. Commit the configuration if you are done configuring the device.

   [edit]
   user@host# commit

Verifying a CLNS VPN Configuration

**Purpose**  Verify that the device is configured correctly for CLNS VPNs.

**Action**  From configuration mode in the CLI, enter the `show` command.

   [edit]
   user@host# show
   interfaces {
     e1–2/0/0.0 {
       unit 0 {
         family inet {
           address 192.168.37.51/31;
         }
         family iso;
         family mpls;
       }
     }
     t1–3/0/0.0 {
       unit 0 {
         family inet {
           address 192.168.37.24/32;
         }
         family iso;
         family mpls;
       }
     }
     lo0 {
       unit 0 {
         family inet {
           address 127.0.0.1/32;
           address 10.255.245.215/32;
         }
         family iso {
           address 47.0005.80ff.f800.0000.0108.0001.1921.6800.4215.00;
         }
       }
     }
   }

Related Topics

- *Junos OS Feature Support Reference for SRX Series and J Series Devices*
- CLNS Configuration Overview on page 758
- Understanding BGP for CLNS VPNs on page 764
- Enabling BGP to Carry CLNS Routes in the *Junos Routing Protocols Configuration Guide*
- iso-vpn in the *Junos Routing Protocols Configuration Guide*
- Verifying a CLNS VPN Configuration on page 765
unit 1 {
    family iso {
        address 47.0005.80ff.f800.0000.0108.aaa2.1921.6800.4215.00;
    }
}

routing-options {
    autonomous-system 230;
}

protocols {
    bgp {
        group pedge-pedge {
            type internal;
            local-address 10.255.245.215;
            neighbor 10.255.245.212 {
                family iso-vpn {
                    unicast;
                }
            }
        }
    }
}

policy-options {
    policy-statement dist-bgp {
        from {
            protocol bgp;
            family iso;
        }
        then accept;
    }
}

routing-instances {
    aaaa {
        instance-type vrf;
        interface lo0.1;
        interface e1–2/0/0.0;
        interface t1–3/0/0.0;
        route-distinguisher 10.255.245.1:1;
        vrf-target target:11111:1;
        routing-options {
            rib aaaa.iso.0 {
                static {
                    iso-route 47.0005.80ff.f800.0000.bbbb.1022/104
                    next-hop 47.0005.80ff.f800.0000.aaa2.1921.6800.4196.00;
                }
            }
        }
        protocols {
            esis {
                interface all;
            }
            isis {
                export dist-bgp;
                no-ipv4–routing;
            }
        }
    }
}
no-ip64-routing;
clns-routing;
interface all;
}
}
}

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- CLNS Configuration Overview on page 758
- show bgp neighbor in the Junos Routing Protocols and Policies Command Reference
- show bgp summary in the Junos Routing Protocols and Policies Command Reference
- show isis backup coverage in the Junos Routing Protocols and Policies Command Reference
- show isis database in the Junos Routing Protocols and Policies Command Reference
- show isis overview in the Junos Routing Protocols and Policies Command Reference
- show isis route in the Junos Routing Protocols and Policies Command Reference
- show isis spf in the Junos Routing Protocols and Policies Command Reference
Chapter 31
VPLS

VPLS Overview

Virtual private LAN service (VPLS) is an Ethernet-based point-to-multipoint Layer 2 VPN. It allows you to connect geographically dispersed Ethernet LAN sites to each other across an MPLS backbone. For customers who implement VPLS, all sites appear to be in the same Ethernet LAN even though traffic travels across the service provider’s network.

VPLS, in its implementation and configuration, has much in common with an MPLS Layer 2 VPN. In a VPLS topology, a packet originating within a customer’s network is sent first to a customer edge (CE) device (for example, a router or Ethernet switch). It is then sent to a provider edge (PE) router within the service provider’s network. The packet traverses the service provider’s network over an MPLS label-switched path (LSP). It arrives at the egress PE router, which then forwards the traffic to the CE device at the destination customer site.

The difference is that for VPLS, packets can traverse the service provider’s network in point-to-multipoint fashion, meaning that a packet originating from a CE device can be broadcast to all the PE routers participating in a VPLS routing instance. In contrast, a Layer 2 VPN forwards packets in point-to-point fashion only. The paths carrying VPLS traffic between each PE router participating in a routing instance are signaled using BGP.
This topic contains the following sections:
- Sample VPLS Topology on page 770
- VPLS on PE Routers on page 770
- Using an Ethernet Switch as the VPLS CE Device on page 772
- VPLS Exceptions on J Series and SRX Series Devices on page 772

**Sample VPLS Topology**

Figure 89 on page 770 shows a basic VPLS topology.

![Figure 89: Basic VPLS Topology](image)

In this sample, the PE routers use the same autonomous system (AS). Within the AS, routing information is communicated through an interior gateway protocol (IGP). Outside the AS, routing information is shared with other ASs through BGP. The PE routers must use the same signaling protocols to communicate.

**VPLS on PE Routers**

Within a VPLS configuration, a device running JUNOS Software can act as a PE router. JUNOS Software passes the VPLS traffic through the following ports and PIMs on the Juniper Networks device to CE routers in the VPLS network:
- Built-in Ethernet ports on front panel
- Gigabit Ethernet uPIMs
- Gigabit Ethernet ePIMs
- Fast Ethernet PIMs
- Fast Ethernet ePIMs

**NOTE:** Ports on uPIMs and ePIMs must be in routing mode before you can configure the corresponding interfaces for VPLS.
Because a VPLS carries Ethernet traffic across a service provider network, it must mimic an Ethernet network in some ways. When a PE router configured with a VPLS routing instance receives a packet from a CE device, it first determines whether it has the destination of the VPLS packet in the appropriate routing table. If it does, it forwards the packet to the appropriate PE router or CE device. If it does not, it broadcasts the packet to all other PE routers and CE devices that are members of that VPLS routing instance. In both cases, the CE device receiving the packet must be different from the one sending the packet.

When a PE router receives a packet from another PE router, it first determines whether it has the destination of the VPLS packet in the appropriate routing table. If it does, the PE router either forwards the packet or drops it depending on whether the destination is a local or remote CE device:

- If the destination is a local CE device, the PE router forwards the packet to it.
- If the destination is a remote CE device (connected to another PE router), the PE router discards the packet.

If the PE router cannot determine the destination of the VPLS packet, it floods the packet to all attached CE devices. Figure 90 on page 771 illustrates this process.

**Figure 90: Flooding a Packet with an Unknown Destination**

A VPLS can be directly connected to an Ethernet switch. Layer 2 information gathered by an Ethernet switch, for example, MAC addresses and interface ports, is included in the VPLS routing instance table.

An MPLS label-switched interface (LSI) label is used as the inner label for VPLS. This label maps to a VPLS routing instance. On the PE router, the LSI label is stripped and then mapped to a logical LSI interface. The Layer 2 Ethernet frame is then forwarded using the LSI interface to the correct VPLS routing instance.

One restriction on flooding behavior in VPLS is that traffic received from remote PE routers is never forwarded to other PE routers. This restriction helps prevent loops in the core network. However, if a CE Ethernet switch has two or more connections
to the same PE router, you must enable the Spanning Tree Protocol (STP) on the CE switch to prevent loops.

**NOTE:** Under certain circumstances, VPLS PE routers might duplicate an Internet Control Message Protocol (ICMP) reply from a CE device when a PE router has to flood an ICMP request because the destination MAC address has not yet been learned. The duplicate ICMP reply can be triggered when a CE device with promiscuous mode enabled is connected to a PE router. The PE router automatically floods the promiscuous mode enabled CE device, which then returns the ICMP request to the VPLS PE routers. The VPLS PE routers consider the ICMP request to be new and flood the request again, creating a duplicate ping reply.

---

**Using an Ethernet Switch as the VPLS CE Device**

For VPLS configurations, the CE device does not necessarily need to be a router. You can link the PE routers directly to Ethernet switches. However, be aware of the following configuration issues:

- When you configure VPLS routing instances and establish two or more connections between a CE Ethernet switch and a PE router, you must enable the Spanning Tree Protocol (STP) on the switch to prevent loops.
- JUNOS Software allows standard bridge protocol data unit (BPDU) frames to pass through emulated Layer 2 connections, such as those configured with Layer 2 VPNs, Layer 2 circuits, and VPLS instances. However, CE Ethernet switches that generate proprietary BPDU frames might not be able to run STP across Juniper Networks routing platforms configured for these emulated Layer 2 connections.

---

**VPLS Exceptions on J Series and SRX Series Devices**

The VPLS implementation on a J Series or SRX Series device is similar to VPLS implementations on M Series, T Series, and MX Series routers, with the following exceptions:

- J Series or SRX Series devices do not support aggregated Ethernet interfaces. Therefore, aggregated Ethernet interfaces between CE devices and PE routers are not supported for VPLS routing instances on J Series or SRX Series devices.
- VPLS routing instances on J Series or SRX Series devices use BGP to send signals to other PE routers. LDP signaling is not supported.
- VPLS multihoming, which allows connecting a CE device to multiple PE routers to provide redundant connectivity, is not supported on J Series or SRX Series devices.
- J Series or SRX Series devices do not support BGP mesh groups.
- J Series or SRX Series devices support only the following encapsulation types on VPLS interfaces that face CE devices: extended VLAN VPLS, Ethernet VPLS, and VLAN VPLS. Ethernet VPLS over ATM LLC encapsulation is not supported.
Virtual ports are generated dynamically on a Tunnel Services PIC on some Juniper Networks routing platforms. J Series or SRX Series devices do not support Tunnel Services modules or virtual ports.

The VPLS implementation on J Series or SRX Series devices does not support dual-tagged frames. Therefore, VLAN rewrite operations are not supported on dual-tagged frames. VLAN rewrite operations such as pop-pop, pop-swap, push-push, swap-push, and swap-swap, which are supported on M Series and T Series routing platforms, are not supported on J Series or SRX Series devices.

Firewall filters for VPLS are not supported.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- MPLS Layer 2 VPN Configuration Overview on page 741
- Understanding VPLS Interfaces on page 774
- Understanding VPLS Routing Instances on page 777
- Understanding VPLS VLAN Encapsulation on page 783
- Understanding VPLS VLAN Encapsulation on a Logical Interface on page 785
- VPLS Configuration Overview on page 773

VPLS Configuration Overview

To configure VPLS functionality, you must enable VPLS support on the provider edge (PE) routers. You must also configure PE routers to distribute routing information to the other PE routers in the VPLS and configure the circuits between the PE routers and the customer edge (CE) devices, as explained in the steps that follow.

NOTE: Many configuration procedures for VPLS are identical to the procedures for Layer 2 and Layer 3 VPNs.

To configure VPLS:

1. Determine which uPIM and ePIM ports correspond to the interfaces that will carry the VPLS traffic and enable routing mode on those ports.

2. Configure the interfaces that will carry the VPLS traffic between the PE router and CE devices. On the PE router interfaces that are facing the CE devices, specify a VPLS encapsulation type. The type of encapsulation depends on the interface type. See “Example: Configuring Routing Interfaces on the VPLS PE Router (CLI)” on page 776 and “Example: Configuring the Interface to the VPLS CE Device” on page 777.

3. Create a VPLS routing instance on each PE router that is participating in the VPLS. For each VPLS routing instance, specify which interfaces will carry the VPLS traffic between the PE and CE devices. On the CE device interface that faces the PE router, you must specify inet (for IPv4), and include the IP address. Additionally, each routing instance must have a unique route distinguisher.
associated with it. (VPN routing instances need a route distinguisher to help BGP identify overlapping network layer reachability information (NLRI) messages from different VPNs.) See “Example: Configuring the VPLS Routing Instance” on page 780.


5. Configure MPLS LSPs between the PE routers. See “Example: Configuring MPLS on the VPLS PE Router” on page 781.

6. Configure RSVP on the PE routers. Enable RSVP for all connections that participate in the MPLS LSP. See “Example: Configuring RSVP on the VPLS PE Router” on page 782.

7. Configure an IBGP session between PE routers so that the routers can exchange information about routes originating and terminating in the VPLS. See “Example: Configuring BGP on the VPLS PE Router” on page 782.

8. Configure an IGP on the PE routers to exchange routing information. See “Example: Configuring OSPF on the VPLS PE Router” on page 783.


**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- MPLS Layer 2 VPN Configuration Overview on page 741
- Example: Configuring MPLS on the VPLS PE Router on page 781
- Example: Configuring RSVP on the VPLS PE Router on page 782
- Example: Configuring BGP on the VPLS PE Router on page 782
- Example: Configuring OSPF on the VPLS PE Router on page 783

**VPLS Interfaces**

- Understanding VPLS Interfaces on page 774
- Example: Configuring Routing Interfaces on the VPLS PE Router (CLI) on page 776
- Example: Configuring the Interface to the VPLS CE Device (CLI) on page 777

**Understanding VPLS Interfaces**

For each VPLS routing instance on a PE router, you specify which interfaces are to be used to carry VPLS traffic between the PE and CE devices.
This topic contains the following sections:

- Interface Name on page 775
- Encapsulation Type on page 775
- Flexible VLAN Tagging on page 776
- VLAN Rewrite on page 776

**Interface Name**

Specify both the physical and logical portions of the interface name, in the following format:

`physical.logical`

For example, in `ge-1/2/1.2`, `ge-1/2/1` is the physical portion of the interface name and `2` is the logical portion. If you do not specify the logical portion of the interface name, `0` is set by default. A logical interface can be associated with only one routing instance.

**Encapsulation Type**

The physical link-layer encapsulation type for a VPLS interface can be one of the following:

- **ethernet-vpls**—Use Ethernet VPLS encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard Tag Protocol Identifier (TPID) values.

- **extended-vlan-vpls**—Use extended virtual LAN (VLAN) VPLS encapsulation on Ethernet interfaces that have VLAN 802.1Q tagging and VPLS enabled and that must accept packets carrying TPIDs 0x8100, 0x9100, and 0x9901. All VLAN IDs from 1 through 1023 are valid for VPLS VLANs on Fast Ethernet interfaces, and all VLAN IDs from 1 through 4094 are valid for VPLS VLANs on Gigabit Ethernet interfaces.

- **vlan-vpls**—Use VLAN VPLS encapsulation on Ethernet interfaces with VLAN tagging and VPLS enabled. Interfaces with VLAN VPLS encapsulation accept packets carrying standard TPID values only. You must configure this encapsulation type on both the physical interface and the logical interface. VLAN IDs 1 through 511 are reserved for normal Ethernet VLANs, IDs 512 through 1023 are reserved for VPLS VLANs on Fast Ethernet interfaces, and IDs 512 through 4094 are reserved for VPLS VLANs on Gigabit Ethernet interfaces.

- **flexible-ethernet-services**—Use flexible Ethernet services encapsulation when you want to configure multiple per-unit Ethernet encapsulations. This encapsulation type allows you to configure any combination of route, TCC, CCC, and VPLS encapsulations on a single physical port. Aggregated Ethernet bundles cannot use this encapsulation type.

For flexible Ethernet services encapsulation, VLAN IDs from 1 through 511 are no longer reserved for normal VLANs.
Flexible VLAN Tagging

For untagged packets to be accepted on an 802.1Q VLAN-tagged port, specify the native VLAN ID with the flexible VLAN tagging option. (No other flexible VLAN tagging features are supported.)

VLAN Rewrite

You can rewrite VLAN tags on VPLS interfaces. Rewriting VLAN tags allows you to use an additional (outer) VLAN tag to differentiate between CE devices that share a VLAN ID.

You can configure rewrite operations to stack (push), remove (pop), or rewrite (swap) tags on single-tagged frames. If a port is not configured for VLAN tagging, rewrite operations are not supported on any logical interface on that port.

You can configure the following VLAN rewrite operations:

- **pop**—Remove a VLAN tag from the top of the VLAN tag stack. The outer VLAN tag of the frame is removed.
- **push**—Add a new VLAN tag to the top of the VLAN stack. An outer VLAN tag is pushed in front of the existing VLAN tag.
- **swap**—Replace the VLAN tag at the top of the VLAN tag stack with a user-specified VLAN tag value.

You perform VLAN rewrite operations by applying input and output VLAN maps at the ingress and egress, respectively, of the interface. For incoming frames, use the input-vlan-map; for outgoing frames, use the output-vlan-map.

The VPLS implementation on J Series or SRX Series devices does not support dual-tagged frames. Therefore, VLAN rewrite operations are not supported on dual-tagged frames. VLAN rewrite operations such as pop-pop, pop-swap, push-push, swap-push, and swap-swap, which are supported on M Series and T Series routing platforms, are not supported on J Series or SRX Series devices.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Example: Configuring Routing Interfaces on the VPLS PE Router (CLI) on page 776
- Example: Configuring the Interface to the VPLS CE Device on page 777
- VPLS Configuration Overview on page 773
- VPLS Overview on page 769
- Understanding VPLS VLAN Encapsulation on page 783

Example: Configuring Routing Interfaces on the VPLS PE Router (CLI)

This example shows how to configure the PE1 router loopback and the interface to the PE2 router (so-2/0/1).
To configure the loopback interface on the VPLS PE router:

```bash
user@host# set interfaces lo0 unit 0 family inet address 127.0.0.1/32
user@host# set interfaces lo0 unit 0 family inet address 10.255.7.168/32 primary
user@host# set interfaces lo0 unit 0 family iso address 47.0005.80ff.f800.0000.0102.5500.7168.00
user@host# set interfaces lo0 unit 0 family inet6 address abcd::10:255:7:168/128 primary
```

To configure the interface to the PE2 router on the VPLS PE router:

```bash
user@host# set interfaces so-2/0/1 unit 0 family inet address 10.1.1.1/30
user@host# set interfaces so-2/0/1 unit 0 family mpls
```

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- VPLS Configuration Overview on page 773
- Understanding VPLS Interfaces on page 774

### Example: Configuring the Interface to the VPLS CE Device (CLI)

This example shows how to configure the PE1 router interface that is connected to the CE device to include VPLS encapsulation.

To configure VPLS encapsulation for the interface facing the CE router:

```bash
user@host# set interfaces ge-1/2/1 encapsulation ethernet-vpls
```

To configure the interface for the vpls family group:

```bash
user@host# set interfaces ge-1/2/1 unit 0 family vpls
```

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- VPLS Configuration Overview on page 773
- Understanding VPLS Interfaces on page 774

### VPLS Routing Instances

- Understanding VPLS Routing Instances on page 777
- Example: Configuring the VPLS Routing Instance (CLI) on page 780

### Understanding VPLS Routing Instances

To configure VPLS functionality, you must enable VPLS support on the PE router. You must also configure PE routers to distribute routing information to the other PE routers in the VPLS and configure the circuits between the PE routers and the CE devices.
You create a VPLS routing instance on each PE router that is participating in the VPLS. The routing instance has the same name on each PE router. To configure the VPLS routing instance, you specify the following:

- **Route distinguisher**—Helps BGP distinguish between potentially identical network layer reachability information (NLRI) messages received from different VPLS instances. Each routing instance that you configure on a PE router must have a unique route distinguisher.
- **Route target**—Defines which route is part of a VPLS. A unique route target helps distinguish between different VPLS services on the same router.
- **Site name**—Provides unique name for the VPLS site.
- **Site identifier**—Provides unique numerical identifier for the VPLS site.
- **Site range**—Specifies total number of sites in the VPLS. The site range must be greater than the site identifier.
- **Interface to the CE router**—Specifies the physical interface to the CE router that carries VPLS traffic. The interface must be configured for a VPLS encapsulation type.

**NOTE:** In addition to the VPLS routing instance, you must configure MPLS label-switched paths (LSPs) between the PE routers, internal BGP (IBGP) sessions between the PE routers, and an interior gateway protocol (IGP) on the PE routers.

**CAUTION:** MPLS is disabled by default on J Series and SRX Series devices. You must explicitly configure your router to allow MPLS traffic. However, when MPLS is enabled, all flow-based security features are deactivated and the router performs packet-based processing. Flow-based services such as security policies, zones, NAT, ALGs, chassis clustering, screens, firewall authentication, and IPSec VPNs are unavailable on the router.

This topic contains the following sections:

- **BGP Signaling** on page 778
- **VPLS Routing Table** on page 779
- **Trace Options** on page 780

**BGP Signaling**

BGP is used to signal the paths between each of the PE routers participating in the VPLS routing instance. These paths carry VPLS traffic across the service provider's network between the VPLS sites.

**NOTE:** LDP signaling is not supported for the VPLS routing instance.
To configure BGP signaling, you specify the following:

- **VPLS site name and site identifier**—When you configure BGP signaling for the VPLS routing instance, you must specify each VPLS site that has a connection to the router. For each VPLS site, you must configure a site name and site identifier (a numerical identifier between 1 to 65,534 that uniquely identifies the VPLS site).

- **Site range**—When you enable BGP signaling for the VPLS routing instance, you need to configure a site range. The site range specifies the total number of sites in the VPLS.

**NOTE:** The site range value must be greater than the largest site identifier.

- **Site preference**—You can specify the preference value advertised for a particular VPLS site. The site preference value is encoded in the BGP local preference attribute. When a PE router receives multiple advertisements with the same VPLS edge (VE) device identifier, the advertisement with the highest local preference value is preferred.

**VPLS Routing Table**

The VPLS routing table contains MAC addresses and interface information for both physical and virtual ports. You can configure the following characteristics for the table:

- **Table size**—You can modify the size of the VPLS MAC address table. The default table size is 512 MAC addresses; the minimum is 16 addresses, and the maximum is 65,536 addresses.

  If the MAC table limit is reached, new MAC addresses can no longer be added to the table. Eventually the oldest MAC addresses are removed from the MAC address table automatically. This frees space in the table, allowing new entries to be added. However, as long as the table is full, new MAC addresses are dropped.

  The interfaces affected include all of the interfaces within the VPLS routing instance, including the local interfaces and the LSI interfaces.

- **Timeout interval**—You can modify the timeout interval for the VPLS table. The default timeout interval is 300 seconds; the minimum is 10 seconds, and the maximum is 1,000,000 seconds. We recommend you configure longer values for small, stable VPLS networks and shorter values for large, dynamic VPLS networks. If the VPLS table does not receive any updates during the timeout interval, the router waits one additional interval before automatically clearing the MAC address entries from the VPLS table.

- **Number of addresses learned from an interface**—You can configure a limit on the number of MAC addresses learned by a VPLS routing instance by setting the MAC table size. The default is 512 addresses; the minimum is 16, and the maximum is 65,536 addresses. If the MAC table limit is reached, new MAC addresses can no longer be added to the table. Eventually the oldest MAC addresses are removed from the MAC address table automatically. This frees
space in the table, allowing new entries to be added. However, as long as the table is full, new MAC addresses are dropped.

Because this limit applies to each VPLS routing instance, the MAC addresses of a single interface can consume all the available space in the table, preventing the routing instance from acquiring addresses from other interfaces. You can limit the number of MAC addresses learned from all interfaces configured for a VPLS routing instance, as well as limit the number of MAC addresses learned from a specific interface.

The MAC limit configured for an individual interface overrides the limit configured for all interfaces for the VPLS routing instance. Also, the table limit can override the limits configured for the interfaces.

The MAC address limit applies only to interfaces to CE devices.

Trace Options

The following trace flags display operations associated with VPLS:

- **all**—All VPLS tracing options
- **connections**—VPLS connections (events and state changes)
- **error**—Error conditions
- **nlri**—VPLS advertisements received or sent using BGP
- **route**—Trace-routing information
- **topology**—VPLS topology changes caused by reconsideration or advertisements received from other PE routers using BGP

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Example: Configuring the VPLS Routing Instance on page 780
- Example: Configuring Routing Options on the VPLS PE Router on page 781
- VPLS Configuration Overview on page 773
- VPLS Overview on page 769
- Understanding VPLS VLAN Encapsulation on page 783

Example: Configuring the VPLS Routing Instance (CLI)

Create a VPLS routing instance on each PE router that is participating in the VPLS.

> **NOTE:** You must specify no-tunnel-services in the VPLS routing instance configuration, as J Series and SRX Series devices do not support tunnel serial PICs.

To create a VPLS routing instance:

```
user@host# set routing-instances green instance-type vpls
```
To configure the VPLS site identifier and range for the VPLS routing instance:

```
user@host# set routing-instances green protocols vpls site-range 10 site R3 site-identifier 2
```

To configure the no-tunnel-services option for the VPLS routing instance green:

```
user@host# set routing-instances green protocols vpls no-tunnel-services
```

To configure the route distinguisher and route target for the VPLS routing instance:

```
user@host# set routing-instances green route-distinguisher 10.255.7.1:1
user@host# set routing-instances green vrf-target target:11111:1
```

To specify the VPLS interface to the CE router:

```
user@host# set routing-instances green instance-type vpls interface ge-1/2/1.0
```

**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- VPLS Configuration Overview on page 773
- Understanding VPLS Routing Instances on page 777

**Example: Configuring Routing Options on the VPLS PE Router (CLI)**

For each router involved in the VPLS, specify the router ID and autonomous system (AS) number. In this sample, PE1 and PE2 use the same AS number (100).

To configure the router ID on the VPLS PE router:

```
user@host# set routing-options router-id 10.255.7.168
```

To configure the AS number on the VPLS PE router:

```
user@host# set routing-options autonomous-system 100
```

**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- VPLS Configuration Overview on page 773
- VPLS Overview on page 769

**Example: Configuring MPLS on the VPLS PE Router (CLI)**

Configure MPLS on the PE1 router to advertise the Layer 2 VPN interface that communicates with the PE2 router.

**CAUTION:** MPLS is disabled by default on J Series and SRX Series devices. You must explicitly configure your router to allow MPLS traffic. However, when MPLS is enabled, all flow-based security features are deactivated and the router performs packet-based processing. Flow-based services such as security policies, zones, NAT, ALGs, chassis...
clustering, screens, firewall authentication, and IPSec VPNs are unavailable on the router.

To configure the interface to the PE2 router for MPLS:

```
user@host# set protocols mpls interface so-2/0/1.0
```

To configure the loopback for MPLS:

```
user@host# set protocols mpls interface lo0.0
```

To configure the path to destination 10.255.7.164:

```
user@host# set protocols mpls label-switched-path chelsea-sagar to 10.255.7.164
```

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- VPLS Configuration Overview on page 773
- VPLS Overview on page 769

---

**Example: Configuring RSVP on the VPLS PE Router (CLI)**

Enable RSVP for all connections that participate in the label-switched path (LSP) on the PE1 router.

To configure the interface to the PE2 router for RSVP:

```
user@host# set protocols rsvp interface so-2/0/1.0
```

To configure the loopback interface for RSVP:

```
user@host# set protocols rsvp interface lo0.0
```

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- VPLS Configuration Overview on page 773
- VPLS Overview on page 769

---

**Example: Configuring BGP on the VPLS PE Router (CLI)**

You configure an internal BGP (IBGP) session between PE routers so that the routers can exchange information about routes originating and terminating in the VPLS. The PE routers use this information to determine which labels to use for traffic destined for remote sites.

To configure the BGP internal group on the VPLS PE router:

```
user@host# set protocols bgp group ibgp type internal local-address 10.255.7.168 neighbor 10.255.7.164
```
To configure the BGP family L2vpn and specify NLRI signaling:

```
user@host# set protocols bgp family l2vpn signaling
```

**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- VPLS Configuration Overview on page 773
- VPLS Overview on page 769

---

**Example: Configuring OSPF on the VPLS PE Router (CLI)**

The PE routers exchange routing information using an IGP such as OSPF.

To configure OSPF area 0.0.0.0 on the VPLS PE router:

```
user@host# set protocols ospf area 0.0.0.0 interface so-2/0/1.0
user@host# set protocols ospf area 0.0.0.0 interface lo0.0
```

To configure traffic engineering for OSPF:

```
user@host# set protocols ospf traffic-engineering
```

**Related Topics**

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- VPLS Configuration Overview on page 773
- VPLS Overview on page 769

---

**VPLS VLAN Encapsulation**

- Understanding VPLS VLAN Encapsulation on page 783
- Example: Configuring VPLS VLAN Encapsulation on a Gigabit Ethernet Interface (CLI) on page 784
- Example: Configuring VPLS VLAN Encapsulation on an Aggregated Ethernet Interface (CLI) on page 785
- Configuring VPLS VLAN Encapsulation for a VLAN Circuit (CLI Procedure) on page 785
- Understanding VPLS VLAN Encapsulation on a Logical Interface on page 785

**Understanding VPLS VLAN Encapsulation**

Gigabit Ethernet IQ, Gigabit Ethernet PIMs with small form-factor pluggable optics (SFPs), SRX Series devices with Gigabit Ethernet, J Series devices with Gigabit Ethernet, Tri-Rate Ethernet copper, and 10-Gigabit Ethernet interfaces with VLAN tagging enabled can use flexible Ethernet services, VLAN CCC, or VLAN virtual private LAN service (VPLS) encapsulation.
NOTE: VLAN encapsulation is not supported on SRX100 devices because there is no Gigabit Ethernet port.

Aggregated Ethernet interfaces configured for VPLS can use Ethernet VPLS or VLAN VPLS.

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- Example: Configuring VPLS VLAN Encapsulation on a Gigabit Ethernet Interface (CLI) on page 784
- Example: Configuring VPLS VLAN Encapsulation on an Aggregated Ethernet Interface (CLI) on page 785
- Configuring VPLS VLAN Encapsulation for a VLAN Circuit (CLI Procedure) on page 785
- Understanding VPLS VLAN Encapsulation on a Logical Interface on page 785
- VPLS Overview on page 769

**Example: Configuring VPLS VLAN Encapsulation on a Gigabit Ethernet Interface (CLI)**

To configure the encapsulation on a Gigabit Ethernet IQ or Gigabit Ethernet physical interface, include the `encapsulation` statement at the `[edit interfaces interface-name]` hierarchy level, specifying `flexible-ethernet-services`, `vlan-ccc`, or `vlan-vpls`:

```
[edit interfaces interface-name]
encapsulation (flexible-ethernet-services | vlan-ccc | vlan-vpls);
```

The following example shows VLAN CCC encapsulation configured on the Gigabit Ethernet interface.

```
interfaces ge-2/1/0 {
  vlan-tagging;
  encapsulation vlan-ccc;
  unit 0 {
    encapsulation vlan-ccc;
    vlan-id 600;
  }
}
```

Related Topics
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- VPLS Configuration Overview on page 773
- Understanding VPLS VLAN Encapsulation on page 783
Example: Configuring VPLS VLAN Encapsulation on an Aggregated Ethernet Interface (CLI)

To configure the encapsulation on an aggregated Ethernet interface, include the 
\texttt{encapsulation} statement at the \texttt{[edit interfaces interface-name]} hierarchy level, specifying \texttt{flexible-ethernet-services}, \texttt{ethernet-vpls}, or \texttt{vlan-vpls}:

\begin{verbatim}
[edit interfaces interface-name]
encapsulation (flexible-ethernet-services | ethernet-vpls | vlan-vpls);
\end{verbatim}

The following example shows VLAN CCC encapsulation configured on an aggregated Gigabit Ethernet interface.

\begin{verbatim}
interfaces ae0 {
  vlan-tagging;
  encapsulation vlan-vpls;
  unit 0 {
    vlan-id 100;
  }
}
\end{verbatim}

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- VPLS Configuration Overview on page 773
- Understanding VPLS VLAN Encapsulation on page 783

Configuring VPLS VLAN Encapsulation for a VLAN Circuit (CLI Procedure)

In general, you configure an interface’s encapsulation at the \texttt{[edit interfaces interface-name]} hierarchy level. However, for some encapsulation types, including flexible Ethernet services, Ethernet VLAN CCC and VLAN VPLS, you can also configure the encapsulation type that is used inside the VLAN circuit itself. To do this, include the \texttt{encapsulation} statement:

\begin{verbatim}
encapsulation (vlan-ccc | vlan-tcc | vlan-vpls);
\end{verbatim}

You can include this statement at the \texttt{[edit interfaces interface-name unit logical-unit-number]} hierarchy level.

Related Topics

- Junos OS Feature Support Reference for SRX Series and J Series Devices
- VPLS Configuration Overview on page 773
- Understanding VPLS VLAN Encapsulation on page 783

Understanding VPLS VLAN Encapsulation on a Logical Interface

You cannot configure a logical interface with VLAN CCC or VLAN VPLS encapsulation unless you also configure the physical device with the same encapsulation or with flexible Ethernet services encapsulation. In general, the logical interface must have a VLAN ID of 512 or higher; if the VLAN ID is 511 or lower, it will be subject to the
normal destination filter lookups in addition to source address filtering. However if you configure flexible Ethernet services encapsulation, this VLAN ID restriction is removed.

Ethernet interfaces in VLAN mode can have multiple logical interfaces. In CCC and VPLS modes, VLAN IDs from 1 through 511 are reserved for normal VLANs, and VLAN IDs 512 through 4094 are reserved for CCC or VPLS VLANs. For 4-port Fast Ethernet interfaces, you can use VLAN IDs 512 through 1024 for CCC or VPLS VLANs.

For encapsulation type `flexible-ethernet-services`, all VLAN IDs are valid.

**Related Topics**
- Junos OS Feature Support Reference for SRX Series and J Series Devices
- VPLS Configuration Overview on page 773
- Understanding VPLS VLAN Encapsulation on page 783
Part 6
Configuring Class of Service

- Class of Service Overview on page 789
- Configuring Class of Service on page 815
Chapter 32
Class of Service Overview

When a network experiences congestion and delay, some packets must be dropped. JUNOS Software class of service (CoS) allows you to divide traffic into classes and offer various levels of throughput and packet loss when congestion occurs. This allows packet loss to happen according to the rules you configure.

For interfaces that carry IPv4, IPv6, or MPLS traffic, you can configure the JUNOS Software CoS features to provide multiple classes of service for different applications. On the device, you can configure multiple forwarding classes for transmitting packets, define which packets are placed into each output queue, schedule the transmission service level for each queue, and manage congestion using a random early detection (RED) algorithm.

Traffic shaping is the allocation of the appropriate amount of network bandwidth to every user and application on an interface. The appropriate amount of bandwidth is defined as cost-effective carrying capacity at a guaranteed CoS. You can use a J Series Services Router or an SRX Series Services Gateway to control traffic rate by applying classifiers and shapers.

The CoS features provide a set of mechanisms that you can use to provide differentiated services when best-effort delivery is insufficient.

Using JUNOS CoS features, you can assign service levels with different delay, jitter (delay variation), and packet loss characteristics to particular applications served by specific traffic flows. CoS is especially useful for networks supporting time-sensitive video and audio applications. To configure CoS features on a device, see “Configuring Class of Service” on page 815.

NOTE: Policing, scheduling, and shaping CoS services are not supported for pre-encryption and post-encryption packets going into and coming out of an IPsec VPN tunnel.

JUNOS Software supports the following RFCs for traffic classification and policing:
- RFC 2474, Definition of the Differentiated Services Field in the IPv4 and IPv6
- RFC 2475, An Architecture for Differentiated Services
- RFC 2579, Assured Forwarding PHB Group
- RFC 2598, An Expedited Forwarding PHB
CoS Terms

Before configuring CoS, become familiar with the terms defined in Table 181 on page 790.

Table 181: CoS Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>assured forwarding (AF)</td>
<td>CoS packet forwarding class that provides a group of values you can define and includes four subclasses, AF1, AF2, AF3, and AF4, each with three drop probabilities, low, medium, and high.</td>
</tr>
<tr>
<td>behavior aggregate (BA)</td>
<td>Feature that can be used to determine the forwarding treatment for each packet. The behavior aggregate classifier maps a code point to a forwarding class and loss priority. The loss priority is used later in the workflow to select one of the two drop profiles used by random early detection (RED).</td>
</tr>
<tr>
<td>best effort (BE)</td>
<td>CoS packet forwarding class that provides no service profile. For the BE forwarding class, loss priority is typically not carried in a code point, and random early detection (RED) drop profiles are more aggressive.</td>
</tr>
<tr>
<td>class of service (CoS)</td>
<td>Method of classifying traffic on a packet-by-packet basis, using information in the type-of-service (ToS) byte to assign traffic flows to different service levels.</td>
</tr>
<tr>
<td>Differentiated Services (DiffServ)</td>
<td>Services based on RFC 2474, <em>Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers</em>. For IPv4, the DiffServ method of CoS uses the type-of-service (ToS) byte to identify different packet flows on a packet-by-packet basis. For IPv6, DiffServ uses the first six bits of the 8-bit Traffic Class field of the IPv6 header. DiffServ adds a Class Selector code point (CSCP) and a DiffServ code point (DSCP).</td>
</tr>
</tbody>
</table>
Table 181: CoS Terms (continued)

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DiffServ code point (DSCP) values</td>
<td>Values for a 6-bit field defined in IP packet headers that can be used to enforce class-of-service (CoS) distinctions.</td>
</tr>
<tr>
<td>drop profile</td>
<td>Drop probabilities for different levels of buffer fullness that are used by random early detection (RED) to determine when to drop packets from a given J Series or SRX Series device scheduling queue.</td>
</tr>
<tr>
<td>expedited forwarding (EF)</td>
<td>CoS packet forwarding class that provides end-to-end service with low loss, low latency, low jitter, and assured bandwidth.</td>
</tr>
<tr>
<td>multifield (MF) classifier</td>
<td>Firewall filter that scans through a variety of packet fields to determine the forwarding class and loss priority for a packet and polices traffic to a specific bandwidth and burst size. Typically, a classifier performs matching operations on the selected fields against a configured value.</td>
</tr>
<tr>
<td>network control (NC)</td>
<td>CoS packet forwarding class that is typically high priority because it supports protocol control.</td>
</tr>
<tr>
<td>PLP bit</td>
<td>Packet loss priority bit. Used to identify packets that have experienced congestion or are from a transmission that exceeded a service provider’s customer service license agreement. A J Series or SRX Series device can use the PLP bit as part of a congestion control strategy. The bit can be configured on an interface or in a filter.</td>
</tr>
<tr>
<td>policer</td>
<td>Feature that limits the amount of traffic passing into or out of an interface. It is an essential component of firewall filters that is designed to thwart denial-of-service (DoS) attacks. A policer applies rate limits on bandwidth and burst size for traffic on a particular J Series device interface.</td>
</tr>
<tr>
<td>policing</td>
<td>Applying rate and burst size limits to traffic on an interface.</td>
</tr>
<tr>
<td>random early detection (RED)</td>
<td>Gradual drop profile for a given class, used for congestion avoidance. RED attempts to anticipate congestion and reacts by dropping a small percentage of packets from the tail of the queue to prevent congestion.</td>
</tr>
<tr>
<td>rule</td>
<td>Guide that the device follows when applying services. A rule consists of a match direction and one or more terms.</td>
</tr>
</tbody>
</table>

**Benefits of CoS**

IP routers normally forward packets independently, without controlling throughput or delay. This type of packet forwarding, known as best-effort service, is as good as your network equipment and links allow. Best-effort service is sufficient for many traditional IP data delivery applications, such as e-mail or Web browsing. However, newer IP applications such as real-time video and audio (or voice) require lower delay, jitter, and packet loss than simple best-effort networks can provide.

CoS features allow a J Series or SRX Series device to improve its processing of critical packets while maintaining best-effort traffic flows, even during periods of congestion. Network throughput is determined by a combination of available bandwidth and delay. CoS dedicates a guaranteed minimum bandwidth to a particular service class by reducing forwarding queue delays. (The other two elements of overall network delay, serial transmission delays determined by link speeds and propagation delays determined by media type, are not affected by CoS settings.)
Normally, packets are queued for output in their order of arrival, regardless of service class. Queuing delays increase with network congestion and often result in lost packets when queue buffers overflow. CoS packet classification assigns packets to forwarding queues by service class.

Because CoS must be implemented consistently end-to-end through the network, the CoS features on the Juniper Networks device are based on IETF Differentiated Services (DiffServ) standards, to interoperate with other vendors’ CoS implementations.

## CoS Across the Network

CoS works by examining traffic entering at the edge of your network. The edge devices classify traffic into defined service groups, which allow for the special treatment of traffic across the network. For example, voice traffic can be sent across certain links, and data traffic can use other links. In addition, the data traffic streams can be serviced differently along the network path to ensure that higher-paying customers receive better service. As the traffic leaves the network at the far edge, you can reclassify the traffic.

To support CoS, you must configure each device in the network. Generally, each device examines the packets that enter it to determine their CoS settings. These settings then dictate which packets are first transmitted to the next downstream device. In addition, the devices at the edges of your network might be required to alter the CoS settings of the packets transmitting to the neighboring network.

Figure 91 on page 792 shows an example of CoS operating across an Internet Service Provider (ISP) network.

![Figure 91: CoS Across the Network](image)

In the ISP network shown in Figure 91 on page 792, Device A is receiving traffic from your network. As each packet enters, Device A examines the packet’s current CoS settings and classifies the traffic into one of the groupings defined by the ISP. This definition allows Device A to prioritize its resources for servicing the traffic streams it is receiving. In addition, Device A might alter the CoS settings (forwarding class and loss priority) of the packets to better match the ISP’s traffic groups. When Device B receives the packets, it examines the CoS settings, determines the appropriate traffic group, and processes the packet according to those settings. Device B then transmits the packets to Device C, which performs the same actions. Device D also examines the packets and determines the appropriate group. Because it sits at the far end of the network, the ISP might decide once again to alter the CoS settings of the packets before Device D transmits them to the neighboring network.
JUNOS CoS Components

JUNOS Software supports CoS on J Series and SRX Series devices as indicated in the following topics:

- Code-Point Aliases on page 793
- Classifiers on page 793
- Forwarding Classes on page 796
- Loss Priorities on page 796
- Forwarding Policy Options on page 797
- Transmission Queues on page 797
- Schedulers on page 797
- Virtual Channels on page 800
- Policers for Traffic Classes on page 801
- Rewrite Rules on page 801

Code-Point Aliases

A code-point alias assigns a name to a pattern of code-point bits. You can use this name, instead of the bit pattern, when you configure other CoS components such as classifiers, drop-profile maps, and rewrite rules.

Classifiers

Packet classification refers to the examination of an incoming packet. This function associates the packet with a particular CoS servicing level. Two general types of classifiers are supported—behavior aggregate (BA) classifiers and multifield (MF) classifiers. When both BA and MF classifications are performed on a packet, the MF classification has higher precedence.

In JUNOS Software, classifiers associate incoming packets with a forwarding class (FC) and packet loss priority (PLP) and, based on the associated forwarding class, assign packets to output queues. FC and PLP associated with a packet specify the behavior of a hop, within the system, to process the packet. The per hop behavior (PHB) comprises packet forwarding, policing, scheduling, shaping, and marking. For example, a hop can put a packet in one of the priority queues according to its FC and then manage the queues by checking a packet’s PLP. JUNOS Software supports up to eight FCs and four PLPs.

Behavior Aggregate Classifiers

A behavior aggregate (BA) classifier operates on a packet as it enters the device. Using behavior aggregate classifiers, the device aggregates different types of traffic into a single forwarding class to receive the same forwarding treatment. The CoS value in the packet header is the single field that determines the CoS settings applied to the packet. Behavior aggregate classifiers allow you to set the forwarding class and loss priority of a packet based on the Differentiated Services (DiffServ) code
point (DSCP) value, DSCP IPv4 value, DSCP IPv6 value, IP precedence value, MPLS EXP bits, or IEEE 802.1p value. The default classifier is based on the IP precedence value. For more information, see “Default Behavior Aggregate Classifiers” on page 807.

JUNOS Software performs BA classification for a packet by examining its layer 2, layer 3, and CoS-related parameters as shown in Table 182 on page 794.

### Table 182: BA Classification

<table>
<thead>
<tr>
<th>Layer</th>
<th>CoS Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2</td>
<td>IEEE 802 1p value: User Priority</td>
</tr>
<tr>
<td>Layer 3</td>
<td>IPv4 precedence</td>
</tr>
<tr>
<td></td>
<td>IPv4 Differentiated Services code point (DSCP) value</td>
</tr>
<tr>
<td></td>
<td>IPv6 DSCP value</td>
</tr>
</tbody>
</table>

**NOTE:** A BA classifier evaluates Layer 2 and Layer 3 parameters independently; the results that generate from Layer 2 parameters override the results that generate from the Layer 3 parameters.

### Default IP Precedence Classifier

With JUNOS Software, all logical interface are automatically assigned a default IP precedence classifier when the logical interface is configured. This default traffic classifier maps IP precedence values to a forwarding class and packet loss priority as shown in Table 183 on page 794. These mapping results take effect for an ingress packet until it is further processed by another classification method.

### Table 183: Default IP Precedence Classifier

<table>
<thead>
<tr>
<th>IP Precedence CoS Values</th>
<th>Forwarding Class</th>
<th>Packet Loss Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>001</td>
<td>best-effort</td>
<td>high</td>
</tr>
<tr>
<td>010</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>011</td>
<td>best-effort</td>
<td>high</td>
</tr>
<tr>
<td>100</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>101</td>
<td>best-effort</td>
<td>high</td>
</tr>
<tr>
<td>110</td>
<td>network-control</td>
<td>low</td>
</tr>
<tr>
<td>111</td>
<td>network-control</td>
<td>high</td>
</tr>
</tbody>
</table>
Multifield Classifiers

A multifield (MF) classifier is a second method for classifying traffic flows. Unlike the behavior aggregate classifier, a multifield classifier can examine multiple fields in the packet—for example, the source and destination address of the packet or the source and destination port numbers of the packet. With multifield classifiers, you set the forwarding class and loss priority of a packet based on firewall filter rules.

**NOTE:** For a specified interface, you can configure both an MF classifier and a BA classifier without conflicts. Because the classifiers are always applied in sequential order, the BA classifier followed by the MF classifier, any BA classification result is overridden by an MF classifier, if they conflict.

JUNOS Software performs MF traffic classification by directly scrutinizing multiple fields of a packet to classify a packet without having to rely upon the output of the previous BA traffic classification. JUNOS Software can simultaneously check a packet’s data ranging from layer 2 to layer 7 as shown in Table 184 on page 795.

**Table 184: MF Classification**

<table>
<thead>
<tr>
<th>Layer</th>
<th>CoS Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2</td>
<td>IEEE 802.1Q: VLAN ID</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.1p: User Priority</td>
</tr>
<tr>
<td>Layer 3</td>
<td>IP Precedence value</td>
</tr>
<tr>
<td></td>
<td>DSCP or DSCP IPv6 value</td>
</tr>
<tr>
<td></td>
<td>Source IP address</td>
</tr>
<tr>
<td></td>
<td>Destination IP address</td>
</tr>
<tr>
<td></td>
<td>Protocol</td>
</tr>
<tr>
<td></td>
<td>ICMP: Code and type</td>
</tr>
<tr>
<td>Layer 4</td>
<td>TCP/UDP: Source port</td>
</tr>
<tr>
<td></td>
<td>TCP/UDP: Destination port</td>
</tr>
<tr>
<td></td>
<td>TCP: Flags</td>
</tr>
<tr>
<td></td>
<td>AH/ESP: SPI</td>
</tr>
<tr>
<td>Layer 7</td>
<td>Not supported for this release.</td>
</tr>
</tbody>
</table>

Using JUNOS Software, you configure an MF classifier with a firewall filter and its associated match conditions. This enables you to use any filter match criteria to
locate packets that require classification. For more information on firewall filters and policies, see the JUNOS Software Security Configuration Guide.

**Forwarding Classes**

Forwarding classes allow you to group packets for transmission. Based on forwarding classes, you assign packets to output queues. The forwarding class plus the loss priority define the per-hop behavior (PHB in DiffServ) of a packet. J Series Services Routers and SRX Series Services Gateways support eight queues (0 through 7). For a classifier to assign an output queue (default queues 0 through 3) to each packet, it must associate the packet with one of the following forwarding classes:

- **Expedited forwarding (EF)**—Provides a low loss, low latency, low jitter, assured bandwidth, end-to-end service.
- **Assured forwarding (AF)**—Provides a group of values you can define and includes four subclasses: AF1, AF2, AF3, and AF4, each with three drop probabilities: low, medium, and high.
- **Best effort (BE)**—Provides no service profile. For the BE forwarding class, loss priority is typically not carried in a class-of-service (CoS) value, and random early detection (RED) drop profiles are more aggressive.
- **Network Control (NC)**—This class is typically high priority because it supports protocol control.

The SRX Series devices support eight queues.

---

**NOTE:** Queues 4 through 7 are not mapped to forwarding classes. To use queues 4 through 7, you must create custom forwarding class names and map them to the queues. For more information, see “Forwarding Class Queue Assignments” on page 806.

In addition to BA and MF classification, the forwarding class (FC) of a packet can be directly determined by the logical interface that receives the packet. This FC of a packet can be configured using CLI commands, and if configured, this FC overrides the FC from any BA classification that was previously performed on the logical interface.

The following CLI commands can assign a forwarding class directly to packets received at a logical interface:

```cli
[edit class-of-service interfaces interface-name unit logical-unit-number]
forwarding-class class-name;
```

**Loss Priorities**

Loss priorities allow you to set the priority of dropping a packet. You can use the loss priority setting to identify packets that have experienced congestion. Typically, you mark packets exceeding some service level with a high loss priority—a greater likelihood of being dropped. You set loss priority by configuring a classifier or a
The loss priority is used later in the workflow to select one of the drop profiles used by random early detection (RED).

You can configure the packet loss priority (PLP) bit as part of a congestion control strategy. The PLP bit can be configured on an interface or in a filter. A packet for which the PLP bit is set has an increased probability of being dropped during congestion.

**Forwarding Policy Options**

CoS-based forwarding (CBF) enables you to control next-hop selection based on a packet’s class of service and, in particular, the value of the IP packet’s precedence bits. For example, you can specify a particular interface or next hop to carry high-priority traffic while all best-effort traffic takes some other path. CBF allows path selection based on class. When a routing protocol discovers equal-cost paths, it can pick a path at random or load-balance across the paths through either hash selection or round-robin selection.

Forwarding policy also allows you to create CoS classification overrides. You can override the incoming CoS classification and assign the packets to a forwarding class based on their input interface, input precedence bits, or destination address. When you override the classification of incoming packets, any mappings you configured for associated precedence bits or incoming interfaces to output transmission queues are ignored.

**Transmission Queues**

After a packet is sent to the outgoing interface on a device, it is queued for transmission on the physical media. The amount of time a packet is queued on the device is determined by the availability of the outgoing physical media as well as the amount of traffic using the interface.

J Series Services Routers and SRX Series Services Gateways support queues 0 through 7. If you configure more than eight queues on a device, the commit operation fails and the device displays a detailed message stating the total number of queues available.

**Schedulers**

An individual device interface has multiple queues assigned to store packets temporarily before transmission. To determine the order to service the queues, the device uses a round-robin scheduling method based on priority and the queue’s weighted round-robin (WRR) credits. JUNOS schedulers allow you to define the priority, bandwidth, delay buffer size, rate control status, and RED drop profiles to be applied to a particular queue for packet transmission. For more information, see “Scheduler Settings” on page 807.

You can configure per-unit scheduling (also called logical interface scheduling). Per-unit scheduling allows you to enable multiple output queues on a logical interface and associate an output scheduler with each queue.
Transmit Rate

The transmission rate determines the traffic transmission bandwidth for each forwarding class you configure. The rate is specified in bits per second (bps). Each queue is allocated some portion of the bandwidth of the outgoing interface.

This bandwidth amount can be a fixed value, such as 1 megabit per second (Mbps), a percentage of the total available bandwidth, or the rest of the available bandwidth. You can limit the transmission bandwidth to the exact value you configure, or allow it to exceed the configured rate if additional bandwidth is available from other queues (SRX3600, SRX3800, SRX5600, and SRX5800 devices do not support an exact value transmit rate). This property helps ensure that each queue receives the amount of bandwidth appropriate to its level of service.

The minimum transmit rate supported on high-speed interfaces is one-tenth thousandth of the speed of that interface. For example, on a Gigabit Ethernet interface with a speed of 1000 Mbps, the minimum transmit rate is 100 Kbps (1000 Mbps x 1/10000). You can configure transmit rates in the range 3200 bps through 160,000,000,000 bps. When the configured rate is less than the minimum transmit rate, the minimum transmit rate is used instead.

NOTE: Interfaces with slower interface speeds, like T1, E1, or channelized T1/E1/ISDN PRI, cannot support minimum transmit rates because the minimum transmit rate supported on a Services Router is 3200 bps.

Transmit rate assigns the weighted round-robin (WRR) priority values within a given priority level and not between priorities. For more information, see “Transmission Scheduling” on page 811.

Delay Buffer Size

You can configure the delay buffer size to control congestion at the output stage. A delay buffer provides packet buffer space to absorb burst traffic up to a specified duration of delay. When the buffer is full, all packets are dropped.

The system calculates the buffer size for a queue based on the buffer allocation method you specify for it in the scheduler. See “Delay Buffer Size Allocation Methods” on page 901 for different buffer allocation methods and “Specifying Delay Buffer Sizes for Queues” on page 902 for buffer size calculations.

By default, all J Series device interfaces other than channelized T1/E1 interfaces support a delay buffer time of 100,000 microseconds. On channelized T1/E1 interfaces, the default delay buffer time is 500,000 microseconds for clear-channel interfaces, and 1,200,000 microseconds for NxDS0 interfaces.

On J Series devices, you can configure larger delay buffers on channelized T1/E1 interfaces. Larger delay buffers help these slower interfaces to avoid congestion and packet dropping when they receive large bursts of traffic. For more information, see “Configuring Large Delay Buffers with a Configuration Editor” on page 900.
NOTE: For a J Series Services Router, if the buffer size percentage is set to zero for T1 interfaces, traffic does not pass.

Scheduling Priority

Scheduling priority determines the order in which an output interface transmits traffic from the queues, thus ensuring that queues containing important traffic are provided better access to the outgoing interface.

The queues for an interface are divided into sets based on their priority. Each set contains queues of the same priority. The device examines the sets in descending order of priority. If at least one queue in a set has a packet to transmit, the device selects that set. If multiple queues in the set have packets to transmit, the device selects a queue from the set according to the weighted round-robin (WRR) algorithm that operates within the set.

The packets in a queue are transmitted based on the configured scheduling priority, the transmit rate, and the available bandwidth. For more information, see “Transmission Scheduling” on page 811.

Shaping Rate

Shaping rates control the maximum rate of traffic transmitted on an interface. You can configure the shaping rate so that the interface transmits less traffic than it is physically capable of carrying.

You can configure shaping rates on logical interfaces. By default, output scheduling is not enabled on logical interfaces. Logical interface scheduling (also called per-unit scheduling) allows you to enable multiple output queues on a logical interface and associate an output scheduler and shaping rate with the queues.

By default, the logical interface bandwidth is the average of unused bandwidth for the number of logical interfaces that require default bandwidth treatment. You can specify a peak bandwidth rate in bits per second (bps), either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). The range is from 1000 through 32,000,000,000 bps.

For low-speed interfaces, the queue-limit values might become lower than the interface MTU so that traffic with large packets can no longer pass through some of the queues. If you want larger-sized packets to flow through, set the buffer-size configuration in the scheduler to a larger value. For more accuracy, the 100-ms queue-limit values are calculated based on shaper rates and not on interface rates.

RED Drop Profiles

A drop profile is a feature of the random early detection (RED) process that allows packets to be dropped before queues are full. Drop profiles are composed of two main values—the queue fullness and the drop probability. The queue fullness represents percentage of memory used to store packets in relation to the total amount that has been allocated for that queue. The drop probability is a percentage value
that correlates to the likelihood that an individual packet is dropped from the network. These two variables are combined in a graph-like format.

When a packet reaches the head of the queue, a random number between 0 and 100 is calculated by the device. This random number is plotted against the drop profile having the current queue fullness of that particular queue. When the random number falls above the graph line, the packet is transmitted onto the physical media. When the number falls below the graph line, the packet is dropped from the network.

When you configure the RED drop profile on an interface, the queue no longer drops packets from the tail of the queue (the default). Rather, packets are dropped after they reach the head of the queue.

You specify drop probabilities in the drop profile section of the class-of-service (CoS) configuration hierarchy and reference them in each scheduler configuration. For each scheduler, you can configure multiple separate drop profiles, one for each combination of loss priority (low, medium-low, medium-high, or high) and IP transport protocol (TCP or non-TCP or any).

**NOTE:** For J Series devices and SRX210, SRX240, and SRX650 devices, tcp and non-tcp values are not supported, only the value “any” is supported.

You can configure a maximum of 32 different drop profiles.

To configure RED drop profiles, include the following statements at the [edit class-of-service] hierarchy level of the configuration:

```
[edit class-of-service]
drop-profiles {
  profile-name {
    fill-level percentage drop-probability percentage;
    interpolate {
      drop-probability [ values ];
      fill-level [ values ];
    }
  }
}
```

**Default Drop Profiles**

By default, if you configure no drop profiles, RED is still in effect and functions as the primary mechanism for managing congestion. In the default RED drop profile, when the fill level is 0 percent, the drop probability is 0 percent. When the fill level is 100 percent, the drop probability is 100 percent.

**Virtual Channels**

On J Series devices, you can configure virtual channels to limit traffic sent from a corporate headquarters to branch offices. Virtual channels might be required when the headquarters site has an expected aggregate bandwidth higher than that of the
individual branch offices. The router at the headquarters site must limit the traffic sent to each branch office router to avoid oversubscribing their links.

You configure virtual channels on a logical interface. Each virtual channel has a set of eight queues with a scheduler and an optional shaper. You can use an output firewall filter to direct traffic to a particular virtual channel. For example, a filter can direct all traffic with a destination address for branch office 1 to virtual channel 1, and all traffic with a destination address for branch office 2 to virtual channel 2.

Although a virtual channel group is assigned to a logical interface, a virtual channel is not the same as a logical interface. The only features supported on a virtual channel are queuing, packet scheduling, and accounting. Rewrite rules and routing protocols apply to the entire logical interface.

**Policers for Traffic Classes**

Policers allow you to limit traffic of a certain class to a specified bandwidth and burst size. Packets exceeding the policer limits can be discarded, or can be assigned to a different forwarding class, a different loss priority, or both. You define policers with firewall filters that can be associated with input or output interfaces.

**Rewrite Rules**

A rewrite rule modifies the appropriate CoS bits in an outgoing packet. Modification of CoS bits allows the next downstream device to classify the packet into the appropriate service group. Rewriting or marking outbound packets is useful when the device is at the border of a network and must alter the CoS values to meet the policies of the targeted peer.

**How CoS Components Work**

On J Series and SRX Series devices, you configure CoS functions using different components. These components are configured individually or in a combination to define particular CoS services. Figure 92 on page 802 displays the relationship of different CoS components to each other and illustrates the sequence in which they interact. “JUNOS CoS Components” on page 793 defines the components and explains their use.
Each box in Figure 92 on page 802 represents a CoS component. The solid lines show the direction of packet flow in a device. The upper row indicates an incoming packet, and the lower row an outgoing packet. The dotted lines show the inputs and outputs of particular CoS components. For example, the forwarding class and loss priority are outputs of behavior aggregate classifiers and multifield classifiers and inputs for rewrite markers and schedulers.

Typically, only a combination of some components shown in Figure 92 on page 802 (not all) is used to define a CoS service offering. For example, if a packet’s class is determined by a behavior aggregate classifier, it is associated with a forwarding class and loss priority and does not need further classification by the multifield classifier.

**CoS Process on Incoming Packets**

Classifiers and policers perform the following operations on incoming packets:

1. A classifier examines an incoming packet and assigns a forwarding class and loss priority to it.
2. Based on the forwarding class, the packet is assigned to an outbound transmission queue.
3. Input policers meter traffic to see if traffic flow exceeds its service level. Policers might discard, change the forwarding class and loss priority, or set the PLP bit of a packet. A packet for which the PLP bit is set has an increased probability of being dropped during congestion.
CoS Process on Outgoing Packets

The scheduler map and rewrite rules perform the following operations on outgoing packets:

1. Scheduler maps are applied to interfaces and associate the outgoing packets with a scheduler and a forwarding class.
2. The scheduler defines how the packet is treated in the output transmission queue based on the configured transmit rate, buffer size, priority, and drop profile.
   - The buffer size defines the period for which the packet is stored during congestion.
   - The scheduling priority and transmit rate determine the order in which the packet is transmitted.
   - The drop profile defines how aggressively to drop packets that are using a particular scheduler.
3. Output policers meter traffic and might change the forwarding class and loss priority of a packet if a traffic flow exceeds its service level.
4. The rewrite rule writes information to the packet (for example, EXP or DSCP bits) according to the forwarding class and loss priority of the packet.

Default CoS Settings

Even when you do not configure any CoS settings on your routing platform, the software performs some CoS functions to ensure that user traffic and protocol packets are forwarded with minimum delay when the network is experiencing congestion. Some default mappings are automatically applied to each logical interface that you configure. Other default mappings, such as explicit default classifiers and rewrite rules, are in operation only if you explicitly associate them with an interface.

You can display default CoS settings by running the show class-of-service operational mode command.

This section contains the following topics:

- Default CoS Values and Aliases on page 804
- Forwarding Class Queue Assignments on page 806
- Scheduler Settings on page 807
- Default Behavior Aggregate Classifiers on page 807
- CoS Value Rewrites on page 810
- Sample Behavior Aggregate Classification on page 810
**Default CoS Values and Aliases**

Table 185 on page 804 shows the default mappings between the bit values and standard aliases.

**Table 185: Well-Known CoS Aliases and Default CoS Values**

<table>
<thead>
<tr>
<th>CoS Value Type</th>
<th>Alias</th>
<th>CoS Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP and DSCP IPv6</td>
<td>ef</td>
<td>101110</td>
</tr>
<tr>
<td></td>
<td>af11</td>
<td>001010</td>
</tr>
<tr>
<td></td>
<td>af12</td>
<td>001100</td>
</tr>
<tr>
<td></td>
<td>af13</td>
<td>001110</td>
</tr>
<tr>
<td></td>
<td>af21</td>
<td>010010</td>
</tr>
<tr>
<td></td>
<td>af22</td>
<td>010100</td>
</tr>
<tr>
<td></td>
<td>af23</td>
<td>010110</td>
</tr>
<tr>
<td></td>
<td>af31</td>
<td>011010</td>
</tr>
<tr>
<td></td>
<td>af32</td>
<td>011100</td>
</tr>
<tr>
<td></td>
<td>af33</td>
<td>011110</td>
</tr>
<tr>
<td></td>
<td>af41</td>
<td>100010</td>
</tr>
<tr>
<td></td>
<td>af42</td>
<td>100100</td>
</tr>
<tr>
<td></td>
<td>af43</td>
<td>100110</td>
</tr>
<tr>
<td></td>
<td>be</td>
<td>000000</td>
</tr>
<tr>
<td></td>
<td>cs1</td>
<td>001000</td>
</tr>
<tr>
<td></td>
<td>cs2</td>
<td>010000</td>
</tr>
<tr>
<td></td>
<td>cs3</td>
<td>011000</td>
</tr>
<tr>
<td></td>
<td>cs4</td>
<td>100000</td>
</tr>
<tr>
<td></td>
<td>cs5</td>
<td>101000</td>
</tr>
<tr>
<td></td>
<td>nc1/cs6</td>
<td>110000</td>
</tr>
<tr>
<td></td>
<td>nc2/cs7</td>
<td>111000</td>
</tr>
<tr>
<td>CoS Value Type</td>
<td>Alias</td>
<td>CoS Value</td>
</tr>
<tr>
<td>---------------</td>
<td>-------</td>
<td>-----------</td>
</tr>
<tr>
<td>MPLS EXP</td>
<td>be</td>
<td>000</td>
</tr>
<tr>
<td></td>
<td>be1</td>
<td>001</td>
</tr>
<tr>
<td></td>
<td>ef</td>
<td>010</td>
</tr>
<tr>
<td></td>
<td>ef1</td>
<td>011</td>
</tr>
<tr>
<td></td>
<td>af11</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>af12</td>
<td>101</td>
</tr>
<tr>
<td></td>
<td>nc1/cs6</td>
<td>110</td>
</tr>
<tr>
<td></td>
<td>nc2/cs7</td>
<td>111</td>
</tr>
<tr>
<td>IEEE 802.1</td>
<td>be</td>
<td>000</td>
</tr>
<tr>
<td></td>
<td>be1</td>
<td>001</td>
</tr>
<tr>
<td></td>
<td>ef</td>
<td>010</td>
</tr>
<tr>
<td></td>
<td>ef1</td>
<td>011</td>
</tr>
<tr>
<td></td>
<td>af11</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>af12</td>
<td>101</td>
</tr>
<tr>
<td></td>
<td>nc1/cs6</td>
<td>110</td>
</tr>
<tr>
<td></td>
<td>nc2/cs7</td>
<td>111</td>
</tr>
<tr>
<td>IP precedence</td>
<td>be</td>
<td>000</td>
</tr>
<tr>
<td></td>
<td>be1</td>
<td>001</td>
</tr>
<tr>
<td></td>
<td>ef</td>
<td>010</td>
</tr>
<tr>
<td></td>
<td>ef1</td>
<td>011</td>
</tr>
<tr>
<td></td>
<td>af11</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>af12</td>
<td>101</td>
</tr>
<tr>
<td></td>
<td>nc1/cs6</td>
<td>110</td>
</tr>
<tr>
<td></td>
<td>nc2/cs7</td>
<td>111</td>
</tr>
</tbody>
</table>
**Forwarding Class Queue Assignments**

J Series and SRX Series devices have eight queues built into the hardware. By default, four queues are assigned to four forwarding classes. Table 186 on page 806 shows the four default forwarding classes and queues that Juniper Networks classifiers assign to packets based on the CoS values in arriving packet headers. Queues 4 through 7 have no default assignments to forwarding classes. To use queues 4 through 7, you must create custom forwarding class names and assign them to the queues. For more information about how to assign queues to forwarding classes, see “Configuring Class of Service” on page 815.

By default, all incoming packets, except the IP protocol control packets, are assigned to the forwarding class associated with queue 0. All IP protocol control packets are assigned to the forwarding class associated with queue 3.

Table 186 on page 806 displays the default assignments of forwarding classes to queues.

<table>
<thead>
<tr>
<th>Forwarding Queue</th>
<th>Forwarding Class</th>
<th>Forwarding Class Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue 0</td>
<td>best-effort (BE)</td>
<td>The Juniper Networks device does not apply any special CoS handling to packets with 000000 in the DiffServ field, a backward compatibility feature. These packets are usually dropped under congested network conditions.</td>
</tr>
<tr>
<td>Queue 1</td>
<td>expedited-forwarding (EF)</td>
<td>The Juniper Networks device delivers assured bandwidth, low loss, low delay, and low delay variation (jitter) end-to-end for packets in this service class. Devices accept excess traffic in this class, but in contrast to assured forwarding, out-of-profile expedited-forwarding packets can be forwarded out of sequence or dropped.</td>
</tr>
<tr>
<td>Queue 2</td>
<td>assured-forwarding (AF)</td>
<td>The Juniper Networks device offers a high level of assurance that the packets are delivered as long as the packet flow from the customer stays within a certain service profile that you define. The device accepts excess traffic, but applies a random early detection (RED) drop profile to determine whether the excess packets are dropped and not forwarded. Three drop probabilities (low, medium, and high) are defined for this service class.</td>
</tr>
<tr>
<td>Queue 3</td>
<td>network-control (NC)</td>
<td>The Juniper Networks device delivers packets in this service class with a low priority. (These packets are not delay sensitive.) Typically, these packets represent routing protocol hello or keepalive messages. Because loss of these packets jeopardizes proper network operation, delay is preferable to discard.</td>
</tr>
</tbody>
</table>
Scheduler Settings

Each forwarding class has an associated scheduler priority. Only two forwarding classes, **best-effort** and **network-control** (queue 0 and queue 3), are used in the JUNOS default scheduler configuration.

By default, the **best-effort** forwarding class (queue 0) receives 95 percent, and the **network-control** (queue 3) receives 5 percent of the bandwidth and buffer space for the output link. The default drop profile causes the buffer to fill and then discard all packets until it again has space.

The **expedited-forwarding** and **assured-forwarding** classes have no schedulers, because by default no resources are assigned to queue 1 and queue 2. However, you can manually configure resources for **expedited-forwarding** and **assured-forwarding**.

By default, each queue can exceed the assigned bandwidth if additional bandwidth is available from other queues. When a forwarding class does not fully use the allocated transmission bandwidth, the remaining bandwidth can be used by other forwarding classes if they receive a larger amount of offered load than the bandwidth allocated. If you do not want a queue to use any leftover bandwidth, you must configure it for strict allocation. For more information, see “Configuring Strict High Priority for Queuing with a Configuration Editor” on page 893.

The device uses the following default scheduler settings. You can modify these settings through configuration. For instructions, see “Configuring Class of Service” on page 815.

```
[edit class-of-service]
schedulers {
  network-control {
    transmit-rate percent 5;
    buffer-size percent 5;
    priority low;
    drop-profile-map loss-priority any protocol any drop-profile terminal;
  }
  best-effort {
    transmit-rate percent 95;
    buffer-size percent 95;
    priority low;
    drop-profile-map loss-priority any protocol any drop-profile terminal;
  }
}
drop-profiles {
  terminal {
    fill-level 100 drop-probability 100;
  }
}
```

Default Behavior Aggregate Classifiers

Table 187 on page 808 shows the forwarding class and packet loss priority (PLP) that are assigned by default to each well-known DSCP. Although several DSCPs map to the **expedited-forwarding** (**ef**) and **assured-forwarding** (**af**) classes, by default no resources
are assigned to these forwarding classes. All af classes other than af1x are mapped to best-effort, because RFC 2597, Assured Forwarding PHB Group, prohibits a node from aggregating classes. Assignment to best-effort implies that the node does not support that class.

You can modify the default settings through configuration. For instructions, see “Configuring Class of Service” on page 815.

<table>
<thead>
<tr>
<th>DSCP and DSCP IPv6 Alias</th>
<th>Forwarding Class</th>
<th>Packet Loss Priority (PLP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ef</td>
<td>expedited-forwarding</td>
<td>low</td>
</tr>
<tr>
<td>af11</td>
<td>assured-forwarding</td>
<td>low</td>
</tr>
<tr>
<td>af12</td>
<td>assured-forwarding</td>
<td>high</td>
</tr>
<tr>
<td>af13</td>
<td>assured-forwarding</td>
<td>high</td>
</tr>
<tr>
<td>af21</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>af22</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>af23</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>af31</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>af32</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>af33</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>af41</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>af42</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>af43</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>be</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>cs1</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>cs2</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>cs3</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>cs4</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>cs5</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>nc1/cs6</td>
<td>network-control</td>
<td>low</td>
</tr>
<tr>
<td>nc2/cs7</td>
<td>network-control</td>
<td>low</td>
</tr>
<tr>
<td>other</td>
<td>best-effort</td>
<td>low</td>
</tr>
</tbody>
</table>
Defining BA Classifiers

You can override the default IP precedence classifier by defining a classifier and applying it to a logical interface. To define new classifiers for all code point types, include the classifiers statement at the [edit class-of-service] hierarchy level:

```
[edit class-of-service]
classifiers {
  (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence) classifier-name {
    import [classifier-name | default];
    forwarding-class class-name {
      loss-priority level {
        code-points [ aliases ] [ 6-bit-patterns ];
      }
    }
  }
}
```

The map sets the forwarding class and PLP for a specific set of code-point aliases and bit patterns. The inputs of the map are code-point aliases and bit patterns. The outputs of the map are the forwarding class and the PLP.

The classifiers work as follows:
- **dscp**—Handles incoming IPv4 packets.
- **dscp-ipv6**—Handles incoming IPv6 packets.
- **exp**—Handles MPLS packets using Layer 2 headers.
- **ieee-802.1**—Handles Layer 2 CoS.
- **inet-precedence**—Handles incoming IPv4 packets. IP precedence mapping requires only the upper three bits of the DSCP field.

A classifier takes a specified bit pattern as either the literal pattern or as a defined alias and attempts to match it to the type of packet arriving on the interface. If the information in the packet’s header matches the specified pattern, the packet is sent to the appropriate queue, defined by the forwarding class associated with the classifier.

The code-point aliases and bit patterns are the input for the map. The loss priority and forwarding class are outputs of the map. In other words, the map sets the PLP and forwarding class for a given set of code-point aliases and bit patterns.

Applying a BA Classifier to a Logical Interface

You can apply the classification map to a logical interface by including the classifiers statement at the [edit class-of-service interfaces interface-name unit logical-unit-number] hierarchy level:

```
[edit class-of-service interfaces interface-name interface-name unit logical-unit-number]
classifiers (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence) (classifier-name | default);
```
You can use interface wildcards for interface-name and logical-unit-number.

**CoS Value Rewrites**

Typically, a device rewrites CoS values in outgoing packets on the outbound interfaces of an edge device, to meet the policies of the targeted peer. After reading the current forwarding class and loss priority information associated with the packet, the transmitting device locates the chosen CoS value from a table, and writes this CoS value into the packet header.

For instructions for configuring rewrite rules, see “Configuring and Applying Rewrite Rules” on page 845.

**Sample Behavior Aggregate Classification**

Table 188 on page 810 shows the device forwarding classes associated with each well-known DSCP code point and the resources assigned to their output queues for a sample DiffServ CoS implementation. This example assigns expedited forwarding to queue 1 and a subset of the assured forwarding classes (af1x) to queue 2, and distributes resources among all four forwarding classes.

Other DiffServ-based implementations are possible. For configuration information, see “Configuring Class of Service” on page 815.

**Table 188: Sample Behavior Aggregate Classification Forwarding Classes and Queues**

<table>
<thead>
<tr>
<th>DSCP and DSCP IPv6 Alias</th>
<th>DSCP and DSCP IPv6 Bits</th>
<th>Forwarding Class</th>
<th>PLP</th>
<th>Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>ef</td>
<td>101110</td>
<td>expedited-forwarding</td>
<td>low</td>
<td>1</td>
</tr>
<tr>
<td>af11</td>
<td>001010</td>
<td>assured-forwarding</td>
<td>low</td>
<td>2</td>
</tr>
<tr>
<td>af12</td>
<td>001100</td>
<td>assured-forwarding</td>
<td>high</td>
<td>2</td>
</tr>
<tr>
<td>af13</td>
<td>001110</td>
<td>assured-forwarding</td>
<td>high</td>
<td>2</td>
</tr>
<tr>
<td>af21</td>
<td>010010</td>
<td>best-effort</td>
<td>low</td>
<td>0</td>
</tr>
<tr>
<td>af22</td>
<td>010100</td>
<td>best-effort</td>
<td>low</td>
<td>0</td>
</tr>
<tr>
<td>af23</td>
<td>010110</td>
<td>best-effort</td>
<td>low</td>
<td>0</td>
</tr>
<tr>
<td>af31</td>
<td>011010</td>
<td>best-effort</td>
<td>low</td>
<td>0</td>
</tr>
<tr>
<td>af32</td>
<td>011100</td>
<td>best-effort</td>
<td>low</td>
<td>0</td>
</tr>
<tr>
<td>af33</td>
<td>011110</td>
<td>best-effort</td>
<td>low</td>
<td>0</td>
</tr>
<tr>
<td>af41</td>
<td>100010</td>
<td>best-effort</td>
<td>low</td>
<td>0</td>
</tr>
<tr>
<td>af42</td>
<td>100100</td>
<td>best-effort</td>
<td>low</td>
<td>0</td>
</tr>
<tr>
<td>af43</td>
<td>100110</td>
<td>best-effort</td>
<td>low</td>
<td>0</td>
</tr>
</tbody>
</table>
Table 188: Sample Behavior Aggregate Classification Forwarding Classes and Queues (continued)

<table>
<thead>
<tr>
<th>DSCP and DSCP IPv6 Alias</th>
<th>DSCP and DSCP IPv6 Bits</th>
<th>Forwarding Class</th>
<th>PLP</th>
<th>Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>be</td>
<td>000000</td>
<td>best-effort</td>
<td>low</td>
<td>0</td>
</tr>
<tr>
<td>cs1</td>
<td>001000</td>
<td>best-effort</td>
<td>low</td>
<td>0</td>
</tr>
<tr>
<td>cs2</td>
<td>010000</td>
<td>best-effort</td>
<td>low</td>
<td>0</td>
</tr>
<tr>
<td>cs3</td>
<td>011000</td>
<td>best-effort</td>
<td>low</td>
<td>0</td>
</tr>
<tr>
<td>cs4</td>
<td>100000</td>
<td>best-effort</td>
<td>low</td>
<td>0</td>
</tr>
<tr>
<td>cs5</td>
<td>101000</td>
<td>best-effort</td>
<td>low</td>
<td>0</td>
</tr>
<tr>
<td>nc1/cs6</td>
<td>110000</td>
<td>network-control</td>
<td>low</td>
<td>3</td>
</tr>
<tr>
<td>nc2/cs7</td>
<td>111000</td>
<td>network-control</td>
<td>low</td>
<td>3</td>
</tr>
<tr>
<td>other</td>
<td>—</td>
<td>best-effort</td>
<td>low</td>
<td>0</td>
</tr>
</tbody>
</table>

Transmission Scheduling

The packets in a queue are transmitted based on their transmission priority, transmit rate, and the available bandwidth.

By default, each queue can exceed the assigned bandwidth if additional bandwidth is available from other queues. When a forwarding class does not fully use the allocated transmission bandwidth, the remaining bandwidth can be used by other forwarding classes if they receive a larger amount of offered load than the bandwidth allocated. A queue receiving traffic within its bandwidth configuration is considered to have positive bandwidth credit, and a queue receiving traffic in excess of its bandwidth allocation is considered to have negative bandwidth credit.

A queue with positive credit does not need to use leftover bandwidth, because it can use its own allocation. For such queues, packets are transmitted based on the priority of the queue, with packets from higher-priority queues transmitting first. The transmit rate is not considered during transmission. In contrast, a queue with negative credit needs a share of the available leftover bandwidth.

The leftover bandwidth is allocated to queues with negative credit in proportion to the configured transmit rate of the queues within a given priority set. The queues for an interface are divided into sets based on their priority. For more information, see "Scheduling Priority" on page 799. If no transmit rate is configured, each queue in the set receives an equal percentage of the leftover bandwidth. However, if a transmit rate is configured, each queue in the set receives the configured percentage of the leftover bandwidth.

Table 189 on page 812 shows a sample configuration of priority and transmit rate on six queues. The total available bandwidth on the interface is 100 Mbps.
Table 189: Sample Transmission Scheduling

<table>
<thead>
<tr>
<th>Queue</th>
<th>Scheduling Priority</th>
<th>Transmit Rate</th>
<th>Incoming Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Low</td>
<td>10%</td>
<td>20 Mbps</td>
</tr>
<tr>
<td>1</td>
<td>High</td>
<td>20%</td>
<td>20 Mbps</td>
</tr>
<tr>
<td>2</td>
<td>High</td>
<td>30%</td>
<td>20 Mbps</td>
</tr>
<tr>
<td>3</td>
<td>Low</td>
<td>30%</td>
<td>20 Mbps</td>
</tr>
<tr>
<td>4</td>
<td>Medium-high</td>
<td>No transmit rate configured</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>5</td>
<td>Medium-high</td>
<td>No transmit rate configured</td>
<td>20 Mbps</td>
</tr>
</tbody>
</table>

In this example, queues are divided into three sets based on their priority:

- High priority set—Consists of queue 1 and queue 2. Packets use 40 Mbps (20 + 20) of the available bandwidth (100 Mbps) and are transmitted first. Because of positive credit, the configured transmit rate is not considered.

- Medium-high priority set—Consists of queue 4 and queue 5. Packets use 30 Mbps (10 + 20) of the remaining 60 Mbps bandwidth. Because of positive credit, the transmit rate is not considered. If the queues had negative credit, they would receive an equal share of the leftover bandwidth because no transmit rate is configured.

- Low priority set—Consists of queue 0 and queue 3. Packets share the 20 Mbps of leftover bandwidth based on the configured transmit rate. The distribution of bandwidth is in proportion to the assigned percentages. Because the total assigned percentage is 40 (10 + 30), each queue receives a share of bandwidth accordingly. Thus queue 0 receives 5 Mbps (10/40 x 20), and queue 3 receives 15 Mbps (30/40 x 20).

CoS Queuing for Tunnels

A tunnel interface in a J Series device running JUNOS Software supports many of the same CoS features as a physical interface. A tunnel interface is a virtual or logical interface on a J Series device. It creates a virtual point-to-point link between two J Series devices at remote points over an IP network.

For example, you can configure CoS features for generic routing encapsulation (GRE) and IP-IP tunnel interfaces. Tunneling protocols encapsulate packets inside a transport protocol.

GRE or IP-IP tunnels are used with services like IPsec and NAT to set up point-to-point VPNs. JUNOS Software allows you to enable CoS queuing, scheduling, and shaping for traffic exiting through these tunnel interfaces. For an example of configuring CoS Queuing for GRE tunnels, see “Example: Configuring CoS for GRE/IPIP tunnels” on page 888.
Benefits of CoS Queuing on Tunnel Interfaces

On a J Series device, CoS queuing enabled for tunnel interfaces allows you to

■ Segregate tunnel traffic.
  
  Each tunnel can be shaped so that a tunnel with low-priority traffic cannot swamp other tunnels that carry high-priority traffic.
  
  Traffic for one tunnel does not impact traffic on other tunnels.

■ Control tunnel bandwidth.
  
  Traffic through various tunnels is limited to not exceed a certain bandwidth.
  
  For example, suppose you have three tunnels to three remote sites through a single WAN interface. You can select CoS parameters for each tunnel such that traffic to some sites gets more bandwidth than traffic to other sites.

■ Customize CoS policies.
  
  You can apply different queuing, scheduling, and shaping policies to different tunnels based on user requirements. Each tunnel can be configured with different scheduler maps, different queue depths, and so on. Customization allows you to configure granular CoS policy providing for better control over tunnel traffic.

■ Prioritize traffic before it enters a tunnel.
  
  For example, CoS queuing avoids having low-priority packets scheduled ahead of high-priority packets when the interface speed is higher than the tunnel traffic speed. This feature is most useful when combined with IPsec. Typically, IPsec processes packets in a FIFO manner. However, with CoS queuing each tunnel can prioritize high-priority packets over low-priority packets. Also, each tunnel can be shaped, so that a tunnel with low-priority traffic does not swamp tunnels carrying high-priority traffic.

How CoS Queuing Works

Figure 93 on page 814 shows CoS-related processing that occurs for traffic entering and exiting a tunnel. For information on flow-based packet processing, see the Junos OS Security Configuration Guide.
Limitations on CoS Shapers for Tunnel Interfaces

On a J Series device, when defining a CoS shaping rate on a tunnel interface, be aware of the following restrictions:

- The shaping rate on the tunnel interface must be less than that of the physical egress interface.
- The shaping rate only measures the packet size that includes the Layer 3 packet with GRE or IP-IP encapsulation. The Layer 2 encapsulation added by the physical interface is not factored into the shaping rate measurement.
- The CoS behavior works as expected only when the physical interface carries the shaped GRE or IP-IP tunnel traffic alone. If physical interface carries other traffic, thereby lowering the available bandwidth for tunnel interface traffic, the CoS features do not work as expected.
- You cannot configure a logical interface shaper and a virtual circuit shaper simultaneously on the router. If virtual circuit shaping is desired, do not define a logical interface shaper. Instead, define a shaping rate for all the virtual circuits.
You configure class of service (CoS) when you need to override the default packet forwarding behavior of a J Series or SRX Series device—especially in the three areas identified in Table 190 on page 815.

Table 190: Reasons to Configure Class of Service (Cos)

<table>
<thead>
<tr>
<th>Default Behavior to Override with CoS</th>
<th>CoS Configuration Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet classification—By default, the J Series or SRX Series device does not use behavior aggregate (BA) classifiers to classify packets. Packet classification applies to incoming traffic.</td>
<td>Classifiers</td>
</tr>
<tr>
<td>Scheduling queues—By default, the J Series or SRX Series device has only two queues enabled. Scheduling queues apply to outgoing traffic.</td>
<td>Schedulers</td>
</tr>
<tr>
<td>Packet headers—By default, the J Series or SRX Series device does not rewrite CoS bits in packet headers. Rewriting packet headers applies to outgoing traffic.</td>
<td>Rewrite rules</td>
</tr>
</tbody>
</table>

You can use either J-Web Quick Configuration or a configuration editor to configure CoS. This chapter contains the following topics. For more information about CoS, see the Junos Class of Service Configuration Guide.

For information about which devices support the features documented in this chapter, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.

This chapter contains the following topics:

- Before You Begin on page 816
- Configuring CoS (J-Web Procedure) on page 816
- Configuring CoS Components with a Configuration Editor on page 833
- Configuring Virtual Channels on page 869
- Configuring Adaptive Shaping for Frame Relay on page 875
- Classifying Frame Relay Traffic on page 876
- Rewriting Frame Relay Headers on page 878
- Configuring Strict-High Priority on page 879
Before You Begin

Before you begin configuring a J Series or SRX Series device for CoS, complete the following tasks:

- If you do not already have a basic understanding of CoS, read “Class of Service Overview” on page 789.
- Determine whether the device needs to support different traffic streams, such as voice or video. If so, CoS helps to make sure this traffic receives more than basic best-effort packet delivery service.
- Determine whether the device is directly attached to any applications that send CoS-classified packets. If no sources are enabled for CoS, you must configure and apply rewrite rules on the interfaces facing the sources.
- Determine whether the device must support assured forwarding (AF) classes. Assured forwarding usually requires random early detection (RED) drop profiles to be configured and applied.
- Determine whether the device must support expedited forwarding (EF) classes with a policer. Policers require you to apply a burst size and bandwidth limit to the traffic flow, and set a consequence for packets that exceed these limits—usually a high loss priority, so that packets exceeding the policer limits are discarded first.

Configuring CoS (J-Web Procedure)

The Class of Service menu allows you to configure most of the JUNOS CoS components for the IPv4 and MPLS traffic on a J Series or an SRX Series device. You can configure forwarding classes for transmitting packets, define which packets are placed into each output queue, schedule the transmission service level for each queue, and manage congestion using a random early detection (RED) algorithm. After defining the CoS components, you must assign classifiers to the required physical and logical interfaces.

This section contains the following topics:

- Defining CoS Value Aliases on page 817
- Defining Forwarding Classes on page 819
Defining CoS Value Aliases

A code-point alias assigns a name to a pattern of code-point bits. You can use this name, instead of the bit pattern, when you configure other CoS components such as classifiers, drop-profile maps, and rewrite rules. For more information about code point aliases, see “Code-Point Aliases” on page 793.

To define CoS value aliases using the J-Web configuration editor:

2. Fill in the options as shown in Table 191 on page 817.
3. Click one of the following buttons:
   - To apply the configuration and return to the main configuration page, click OK.
   - To cancel your entries and return to the main page, click Cancel.

Table 191: CoS Value Aliases Configuration Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Code Point Alias Summary</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alias name</td>
<td>Displays the name given to CoS values—for example, af11 or be.</td>
<td>None</td>
</tr>
</tbody>
</table>
### Table 191: CoS Value Aliases Configuration Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias type</td>
<td>Displays the code point type. The following type of code points are supported:</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>■ DSCP—Defines aliases for DiffServ code point (DSCP) IPv4 values.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can refer to these aliases when you configure classes and define classifiers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ DSCP-IPv6—Defines aliases for DSCP IPv6 values.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can refer to these aliases when you configure classes and define classifiers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ EXP—Defines aliases for MPLS experimental (EXP) bits.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can map MPLS EXP bits to the device forwarding classes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ inet-precedence—Defines aliases for IPv4 precedence values.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Precedence values are modified in the IPv4 type-of-service (TOS) field and mapped to values that correspond to levels of service.</td>
<td></td>
</tr>
<tr>
<td>CoS value bits</td>
<td>Displays the CoS value for which an alias is defined.</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Changing this value alters the behavior of all classifiers that refer to this alias.</td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Opens a page that allows you to create a new code point alias.</td>
<td>Click <strong>Add</strong> to create a new code point alias.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens a page that allows you to edit a selected code point alias.</td>
<td>To edit an existing code point alias, select the alias in the summary page, and click <strong>Edit</strong>.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes a specified code point alias.</td>
<td>To delete an existing code point alias, select the alias and click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>

**Add Code Point Alias/Edit Code Point Alias**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code point name</td>
<td>Name given to CoS values—for example, af11 or be.</td>
<td>Specify a name for the CoS point alias.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> If you create a new alias with the same name that is available in the default list, then the default alias name is overwritten with the user-configured name.</td>
</tr>
<tr>
<td>Code point type</td>
<td>Code point type: DSCP, DSCP-IPv6, EXP, or inet-precedence</td>
<td>Select the alias value you want to configure: DSCP, DSCP-IPv6, EXP, or inet-precedence.</td>
</tr>
</tbody>
</table>
Table 191: CoS Value Aliases Configuration Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code point value</td>
<td>Specifies a CoS value for which an alias is</td>
<td>To specify a CoS value, type it in an appropriate format:</td>
</tr>
<tr>
<td>value bits</td>
<td>defined</td>
<td>■ For DSCP and DSCP IPv6 CoS values, use the format xxxxxx, where x is 1 or 0—for example, 101110.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ For MPLS EXP and IP precedence CoS values, use the format xxx, where x is 1 or 0—for example, 111.</td>
</tr>
</tbody>
</table>

Defining Forwarding Classes

By assigning a forwarding class to a queue number, you affect the scheduling and marking of a packet as it transits a J Series or an SRX Series device. For more information about forwarding classes and queues, see the “Forwarding Classes” on page 796 and “Transmission Queues” on page 797.

To define forwarding classes using the J-Web configuration editor:

1. Select Configure > Class of Service > Forwarding Classes.
   The Forwarding Class Configuration summary page appears.
2. Fill in the options as shown in Table 192 on page 819.
3. Click one of the following buttons:
   ■ To apply the configuration and return to the main configuration page, click OK.
   ■ To cancel your entries and return to the main page, click Cancel.

Table 192: Forwarding Classes Configuration Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding Classes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forwarding class name</td>
<td>Displays the forwarding class name assigned to the internal queue number.</td>
<td>None</td>
</tr>
</tbody>
</table>

By default, four forwarding classes are assigned to queue numbers 0 (best-effort), 1 (assured-forwarding), 5 (expedited-forwarding), and 7 (network-connect).
### Table 192: Forwarding Classes Configuration Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue number</td>
<td>Displays internal queue numbers to which forwarding classes are assigned. By assigning a forwarding class to a queue number, you affect the scheduling and marking of a packet as it transits a J Series or an SRX Series device. By default, if a packet is not classified, it is assigned to the class associated with queue 0. You can have more than one forwarding class to a queue number.</td>
<td>None</td>
</tr>
<tr>
<td>Queue characteristics</td>
<td>Displays the queue characteristics, for example, video or voice.</td>
<td>None</td>
</tr>
<tr>
<td>Add</td>
<td>Opens a page that allows you to create a new forwarding class.</td>
<td>Click <strong>Add</strong> to create a new forwarding class.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens a page that allows you to edit a selected forwarding class.</td>
<td>To edit a forwarding class, select a forwarding class in the summary page, and click <strong>Edit</strong>.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes a specified forwarding class.</td>
<td>To delete a forwarding class, select the forwarding class and click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>

**Add Forwarding Class/Edit Forwarding Class**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue number</td>
<td>Specifies the internal queue number to which a forwarding class is assigned.</td>
<td>To specify an internal queue number, type an integer from 0 through 7, as supported by your device. <strong>NOTE:</strong> If you create a new forwarding class that overrides the default queue number, the default forwarding class is deleted after a commit.</td>
</tr>
<tr>
<td>Forwarding class name</td>
<td>Specifies the forwarding class name assigned to the internal queue number.</td>
<td>To assign a forwarding class name to a queue, type the name—for example, be-class.</td>
</tr>
</tbody>
</table>

### Defining Classifiers

Classifiers examine the CoS value or alias of an incoming packet and assign it a level of service by setting its forwarding class and loss priority. For more information about classifiers, see the “Classifiers” on page 793.

To define classifiers using the J-Web configuration editor:

1. Select **Configure > Class of Service > Classifiers**.
   
   The Classifier Configuration summary page appears.

2. Fill in the options as shown in Table 193 on page 821.

3. Click one of the following buttons:
   - To apply the configuration and return to the main configuration page, click **OK**.
To cancel your entries and return to the main page, click **Cancel**.

### Table 193: Classifiers Configuration Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Classifier Configuration Summary</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Classifier name</td>
<td>Displays the names of classifiers.</td>
<td>None</td>
</tr>
<tr>
<td>Classifier type</td>
<td>Displays the classifier type. The following type of classifiers are supported:</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>J Series (J6350), SRX650:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ dscp-default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ dscp-ipv6-default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ dscp-ipv6-compatibility</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ exp-default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ ieee8021p-default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ ipprec-default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ ipprec-compatibility</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ ieee8021ad-default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SRX210, SRX240:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ dscp-default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ dscp-ipv6-default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ dscp-ipv6-compatibility</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ exp-default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ ieee8021p-default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ ipprec-default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ ipprec-compatibility</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ ieee8021ad-default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ ieee8021p-compatibility</td>
<td></td>
</tr>
<tr>
<td><strong>Details of Classifiers</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incoming code point</td>
<td>Displays CoS values and aliases to which forwarding class and loss priority are mapped.</td>
<td>None</td>
</tr>
<tr>
<td>Forwarding class name</td>
<td>Displays forwarding class names that are assigned to specific CoS values and aliases of a classifier.</td>
<td>None</td>
</tr>
<tr>
<td>Loss priority</td>
<td>Displays loss priorities that are assigned to specific CoS values and aliases of a classifier.</td>
<td>None</td>
</tr>
<tr>
<td>Add</td>
<td>Opens a page that allows you to define classifiers.</td>
<td>To add a classifier, click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens a page that allows you to edit a selected classifier.</td>
<td>To edit a classifier, select a classifier in the summary page and click <strong>Edit</strong>.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes a specified classifier.</td>
<td>To delete a classifier, select the classifier and click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>
Table 193: Classifiers Configuration Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classifier name</td>
<td>Specifies the name for a classifier.</td>
<td>To name a classifier, type the name—for example, ba-classifier.</td>
</tr>
<tr>
<td>Classifier type</td>
<td>Specify a classifier type.</td>
<td>Select a classifier type from the drop-down list, for example, dscp, ieee-802.1, or inet-precedence.</td>
</tr>
<tr>
<td>Add</td>
<td>Opens a page that allows you to assign a forwarding class and loss priority to the specified CoS value and alias.</td>
<td>To assign a code point, forwarding class, and loss priority to a specific CoS classifier, click Add.</td>
</tr>
</tbody>
</table>

Add Code Point Mapping/Edit Code Point Mapping

<table>
<thead>
<tr>
<th>Code point</th>
<th>Specifies the CoS value in bits and the alias of a classifier.</th>
<th>To specify a CoS value and alias, either select preconfigured ones from the list or type new ones.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding class</td>
<td>Assigns the forwarding class to the specified CoS value and alias.</td>
<td>To assign a forwarding class, select either one of the following default forwarding classes or one that you have configured:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- expedited-forwarding—Provides low loss, low delay, low jitter, assured bandwidth, and end-to-end service. Packets can be forwarded out of sequence or dropped.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- best-effort—Provides no special CoS handling of packets. Typically, RED drop profile is aggressive and no loss priority is defined.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- assured-forwarding—Provides high assurance for packets within the specified service profile. Excess packets are dropped.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- network-control—Packets can be delayed but not dropped.</td>
</tr>
<tr>
<td>Loss priority</td>
<td>Assigns a loss priority to the specified CoS value and alias.</td>
<td>To assign a loss priority, select one:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- high—Packet has a high loss priority.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- low—Packet has a low loss priority.</td>
</tr>
</tbody>
</table>

Defining Rewrite Rules

Use the rewrite rules to alter the CoS values in outgoing packets to meet the requirements of the targeted peer. A rewrite rule examines the forwarding class and loss priority of a packet and sets its bits to a corresponding value specified in the rule. For more information about rewrite rules, see the “Rewrite Rules” on page 801.
To define rewrite rules using the J-Web configuration editor:

1. Select **Configure > Class of Service > Rewrite Rules**.
The Configure Rewrite Rule summary page appears.
2. Fill in the options as shown in Table 194 on page 823.
3. Click one of the following buttons:
   - To apply the configuration and return to the main configuration page, click **OK**.
   - To cancel your entries and return to the main page, click **Cancel**.

### Table 194: Rewrite Rules Configuration Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure Rewrite Rule Summary</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rewrite rule name</td>
<td>Displays names of defined rewrite rules.</td>
<td>None</td>
</tr>
<tr>
<td>Rewrite rule type</td>
<td>Displays the rewrite rule type. The following types are supported for J6350, SRX210, SRX240, and SRX650 devices:</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>■ dscp—Defines the differentiated services code point rewrite rule.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ dscp-ipv6—Defines the differentiated services code point rewrite rule IPv6.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ exp—Defines the MPLS EXP rewrite rule.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ frame-relay-de—Defines the frame relay discard eligible bit rewrite rule.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ ieee-802.1—Defines the IEEE-802.1 rewrite rule.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ inet-precedence—Defines the IPv4 precedence rewrite rule.</td>
<td></td>
</tr>
<tr>
<td><strong>Code Point Details</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incoming code point</td>
<td>Displays the CoS values and aliases that a specific rewrite rule has set for a specific forwarding class and loss priority.</td>
<td>None</td>
</tr>
<tr>
<td>Forwarding class name</td>
<td>Displays forwarding classes associated with a specific rewrite rule.</td>
<td>None</td>
</tr>
<tr>
<td>Loss priority</td>
<td>Displays loss priority values associated with a specific rewrite rule.</td>
<td>None</td>
</tr>
<tr>
<td>Add</td>
<td>Opens a page that allows you to define a new rewrite rule.</td>
<td>To add a rewrite rule, click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens a page that allows you to edit a selected rewrite rule.</td>
<td>To edit a rewrite rule, select a rewrite rule in the summary page and click <strong>Edit</strong>.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes selected rewrite rules.</td>
<td>To remove a rule, select the rewrite rule and click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>
### Table 194: Rewrite Rules Configuration Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add Rewrite Rule/Edit Rewrite Rule</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rewrite rule name</td>
<td>Specifies a rewrite rule name.</td>
<td>To name a rule, type the name—for example, rewrite-dscps.</td>
</tr>
<tr>
<td>Rewrite rule type</td>
<td>Specify a rewrite rule type.</td>
<td>Select a rewrite rule type from the drop-down list, for example, dscp, ieee-802.1, or inet-precedence.</td>
</tr>
<tr>
<td>Add</td>
<td>Opens a page that allows you to rewrite outgoing CoS values of a packet based on the forwarding class and loss priority.</td>
<td>To assign a code point, forwarding class, and loss priority to the rewrite rule, click Add.</td>
</tr>
<tr>
<td><strong>Add Code Point Mapping</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Code point</td>
<td>Specifies the CoS value in bits and the alias of a classifier.</td>
<td>To specify a CoS value and alias, select one from the drop-down list.</td>
</tr>
<tr>
<td>Forwarding class</td>
<td>Assigns the forwarding class to the rewrite rule.</td>
<td>To assign a forwarding class, select one from the drop-down list:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ expedited-forwarding—Provides low loss, low delay, low jitter, assured bandwidth, and end-to-end service. Packets can be forwarded out of sequence or dropped.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ best-effort—Provides no special CoS handling of packets. Typically, RED drop profile is aggressive and no loss priority is defined.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ assured-forwarding—Provides high assurance for packets within the specified service profile. Excess packets are dropped.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ network-control—Packets can be delayed but not dropped.</td>
</tr>
<tr>
<td>Loss priority</td>
<td>Assigns a loss priority to the specified rewrite rule.</td>
<td>To assign a loss priority, select one:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ high—Packet has a high loss priority.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ low—Packet has a low loss priority.</td>
</tr>
</tbody>
</table>

### Defining Schedulers

An individual device interface has multiple queues assigned to store packets temporarily before transmission. To determine the order in which to service the queues, the device uses a round-robin scheduling method based on priority and the queue’s weighted round-robin (WRR) credits. JUNOS schedulers allow you to define the priority, bandwidth, delay buffer size, rate control status, and RED drop profiles to be applied to a particular queue for packet transmission. For more information on schedulers, see the “Schedulers” on page 797.

To configure schedulers using the J-Web configuration editor:

1. Select Configure > Class of Service > Schedulers.
The Configure Schedulers summary page appears.

2. Fill in the options as shown in Table 195 on page 825.
3. Click one of the following buttons:
   - To apply the configuration and return to the main configuration page, click **OK**.
   - To cancel your entries and return to the main page, click **Cancel**.

### Table 195: Schedulers Configuration Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure Schedulers Summary</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduler name</td>
<td>Displays the names of defined schedulers.</td>
<td>None</td>
</tr>
<tr>
<td>Scheduler priority</td>
<td>Displays the transmission priority of the scheduler, which determines the order in which an output interface transmits traffic from the queues.</td>
<td>None</td>
</tr>
<tr>
<td><strong>Details of Scheduler</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Displays the scheduler name.</td>
<td>None</td>
</tr>
<tr>
<td>Value</td>
<td>Displays the CoS value.</td>
<td>None</td>
</tr>
<tr>
<td>Add</td>
<td>Opens a page that allows you to add a scheduler.</td>
<td>To add a scheduler, click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens a page that allows you to edit a selected scheduler.</td>
<td>To edit a scheduler, select an existing scheduler in the summary page and click <strong>Edit</strong>.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes selected schedulers.</td>
<td>To remove an existing scheduler, select the scheduler and click <strong>Delete</strong>.</td>
</tr>
<tr>
<td><strong>Add Scheduler/Edit Scheduler</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduler name</td>
<td>Specifies the name for a scheduler.</td>
<td>To name a scheduler, type the name—for example, be-scheduler.</td>
</tr>
<tr>
<td>Scheduler priority</td>
<td>Sets the transmission priority of the scheduler, which determines the order in which an output interface transmits traffic from the queues.</td>
<td>To specify a priority, select one:</td>
</tr>
<tr>
<td></td>
<td>You can set scheduling priority at different levels in an order of increasing priority from low to high.</td>
<td>■ high—Packets in this queue have high priority.</td>
</tr>
<tr>
<td></td>
<td>A high-priority queue with a high transmission rate might lock out lower-priority traffic.</td>
<td>■ low—Packets in this queue are transmitted last.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ medium—low—Packets in this queue have medium-low priority.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ medium—high—Packets in this queue have medium-high priority.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ strict—high—Packets in this queue are transmitted first.</td>
</tr>
</tbody>
</table>
### Table 195: Schedulers Configuration Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer size</td>
<td>Defines the size of the delay buffer.</td>
<td>To define a delay buffer size for a scheduler, select the appropriate option:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- To enforce exact buffer size, select <strong>Exact</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- To specify a buffer size as a temporal value (microseconds), select <strong>Temporal</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- To specify buffer size as a percentage of the total buffer, select <strong>Percent</strong> and type an integer from 1 through 100.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- To specify buffer size as the remaining available buffer, select <strong>Remainder</strong>.</td>
</tr>
<tr>
<td></td>
<td>By default, queues 0 through 7 have the following percentage of the total available buffer space:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Queue 0—95 percent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Queue 1—0 percent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Queue 2—0 percent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Queue 3—0 percent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Queue 4—0 percent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Queue 5—0 percent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Queue 6—0 percent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Queue 7—5 percent</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** A large buffer size value correlates with a greater possibility of packet delays. This might not be practical for sensitive traffic such as voice or video.

<table>
<thead>
<tr>
<th>Shaping rate</th>
<th>Defines the minimum bandwidth allocated to a queue.</th>
<th>To define a shaping rate, select the appropriate option:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- To specify shaping rate as an absolute number of bits per second, select <strong>rate</strong> and type an integer from 3200 to 160,000,000,000 bits per second.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- To specify shaping rate as a percentage, select <strong>percent</strong> and type an integer from 0 through 100.</td>
</tr>
<tr>
<td></td>
<td>The default shaping rate is 100 percent, which is the same as no shaping at all.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transmit rate</th>
<th>Defines the transmission rate of a scheduler.</th>
<th>To define a transmit rate, select the appropriate option:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- To specify a transmit rate, select <strong>rate</strong> and type an integer from 3200 to 160,000,000,000 bits per second.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- To enforce an exact transmit rate, select <strong>rate</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- To specify the remaining transmission capacity, select <strong>remainder</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- To specify a percentage of transmission capacity, select <strong>percent</strong> and type an integer from 1 through 100.</td>
</tr>
</tbody>
</table>

|                                      |                                                                          |                                                                 |
|                                      |                                                                          |                                                                 |

By default, queues 0 through 7 have the following percentage of transmission capacity:

- Queue 0—95 percent
- Queue 1—0 percent
- Queue 2—0 percent
- Queue 3—0 percent
- Queue 4—0 percent
- Queue 6—0 percent
- Queue 7—5 percent
Defining Scheduler Maps

After defining schedulers you associate them with forwarding classes by means of scheduler maps. For more information on scheduler maps, see “CoS Process on Outgoing Packets” on page 803.

To configure scheduler maps using the J-Web configuration editor:

1. Select **Configure > Class of Service > Scheduler Maps**. The Configure Scheduler Maps summary page appears.
2. Fill in the options as shown in Table 196 on page 827.
3. Click one of the following buttons:
   - To apply the configuration and return to the main configuration page, click **OK**.
   - To cancel your entries and return to the main page, click **Cancel**.

### Table 196: Scheduler Maps Configuration Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure Scheduler Maps</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduler map name</td>
<td>Displays the names of defined scheduler maps. Scheduler maps link schedulers to forwarding classes.</td>
<td>None</td>
</tr>
<tr>
<td>Schedulers</td>
<td>For each map, displays the schedulers assigned to it.</td>
<td>None</td>
</tr>
<tr>
<td>Forwarding Class</td>
<td>For each map, displays the forwarding classes assigned to it.</td>
<td>None</td>
</tr>
<tr>
<td><strong>Details of Scheduler</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Displays the scheduler assigned to the selected scheduler map</td>
<td>None</td>
</tr>
<tr>
<td>Value</td>
<td>Displays the CoS values.</td>
<td>None</td>
</tr>
<tr>
<td>Add</td>
<td>Opens a page that allows you to add a scheduler map.</td>
<td>To add a scheduler map, click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens a page that allows you to edit a selected scheduler map.</td>
<td>To edit an existing scheduler map, select the scheduler map in the summary page and click <strong>Edit</strong>.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes selected scheduler maps.</td>
<td>To remove an existing scheduler map, select the scheduler map and click <strong>Delete</strong>.</td>
</tr>
<tr>
<td><strong>Add Scheduler Map/Edit Scheduler Map</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduler map name</td>
<td>Specifies the name for a scheduler map.</td>
<td>To name a map, type the name—for example, be-scheduler-map.</td>
</tr>
</tbody>
</table>
Table 196: Scheduler Maps Configuration Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduler mapping</td>
<td>Allows you to associate a preconfigured scheduler with a forwarding class.</td>
<td>To associate a scheduler with a forwarding class, locate the forwarding class and select the scheduler in the box next to it.</td>
</tr>
<tr>
<td></td>
<td>Once applied to an interface, the scheduler maps affect the hardware queues, packet schedulers, and RED drop profiles.</td>
<td></td>
</tr>
</tbody>
</table>

Defining Drop Profiles

A drop profile is a feature of the random early detection (RED) process that allows packets to be dropped before queues are full. Drop profiles are composed of two main values—the queue fullness and the drop probability. For more information on drop profiles, see “RED Drop Profiles” on page 799.

To configure drop profiles using the J-Web configuration editor:

1. Select Configure > Class of Service > Drop Profile.

   The RED drop profiles summary page appears.

2. Fill in the options as shown in Table 197 on page 828.

3. Click one of the following buttons:
   - To apply the configuration and return to the main configuration page, click OK.
   - To cancel your entries and return to the main page, click Cancel.

Table 197: RED Drop Profile Configuration Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Drop Profiles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drop profile name</td>
<td>Displays the configured random early detection (RED) drop profile names.</td>
<td>None</td>
</tr>
<tr>
<td>Profile type</td>
<td>Displays whether a RED drop profile type is interpolated or segmented.</td>
<td>None</td>
</tr>
<tr>
<td>Data points</td>
<td>Displays information about the data point types.</td>
<td>None</td>
</tr>
<tr>
<td>Add</td>
<td>Opens a page that allows you to add a RED drop profile.</td>
<td>To create a new RED drop profile, click Add.</td>
</tr>
<tr>
<td>Edit</td>
<td>Opens a page that allows you to edit a RED drop profile.</td>
<td>To edit an existing profile, select the profile in the summary page and click Edit.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes selected RED drop profiles.</td>
<td>To remove an existing profile, select the profile and click Delete.</td>
</tr>
</tbody>
</table>

Add RED Drop Profile/Edit RED Drop Profile
### Table 197: RED Drop Profile Configuration Options (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop profile name</td>
<td>Specifies a name for a drop profile.</td>
<td>To name a drop profile, type the name—for example, <code>be-normal</code>.</td>
</tr>
<tr>
<td></td>
<td>A drop profile consists of pairs of values between 0 and 100, one for queue buffer fill level and one for drop probability, that determine the relationship between a buffer’s fullness and the likelihood it will drop packets. The values you assign to each pair must increase relative to the previous pair of values. With a few value pairs, the system automatically constructs a drop profile.</td>
<td></td>
</tr>
<tr>
<td>RED drop profile type</td>
<td>Specifies whether a RED drop profile type is segmented or interpolated.</td>
<td>Select <code>Segmented</code> or <code>Interpolated</code>.</td>
</tr>
<tr>
<td></td>
<td>■ Segmented—The value pairs are represented by line fragments, which connect each data point on the graph to produce a segmented profile.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Interpolated—The value pairs are interpolated to produce a smooth profile.</td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td>Opens a page that allows you to add the specified queue buffer fill level and drop probability as a data point for the graph.</td>
<td>To add fill level and drop probability, click <code>Add</code>.</td>
</tr>
<tr>
<td>Data point</td>
<td>Specifies the points for generating the RED drop profile graph. Each data point is defined by a pair of x and y coordinates and represents the relationship between them.</td>
<td>To specify x and y coordinates for data points, type a number between 0 and 100 in the following boxes:</td>
</tr>
<tr>
<td></td>
<td>The x axis represents the queue buffer fill level, which is a percentage value of how full the queue is. A value of 100 means the queue is full.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The y axis represents the drop probability, which is a percentage value of the chances of a packet being dropped. A value of 0 means that a packet is never dropped, and a value of 100 means that all packets are dropped.</td>
<td></td>
</tr>
</tbody>
</table>

### Defining Virtual Channel Groups

**NOTE:** SRX3400, SRX3600, SRX5600, and SRX5800 devices do not support virtual channels.

Use virtual channels to avoid oversubscription of links by limiting traffic from a higher aggregated bandwidth to a lower one—for example, to limit traffic from a main office to branch offices. You channelize this traffic by applying queuing, packet scheduling,
and accounting rules to logical interfaces. For more information on virtual channels, see “Virtual Channels” on page 800.

To configure virtual channel groups using the J-Web configuration editor:

1. Select **Configure > Class of Service > Virtual Channel Groups**.

   The configure class of service page appears.

2. Fill in the options as shown in Table 197 on page 828.

3. Click one of the following buttons:
   - To apply the configuration and return to the main configuration page, click **OK**.
   - To cancel your entries and return to the main page, click **Cancel**.

### Table 198: Virtual Channel Group Quick Configuration Page Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual Channel Groups Summary</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual Channel Group Name</td>
<td>Displays names of defined virtual channel groups.</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Allows you to edit a virtual channel group.</td>
<td></td>
</tr>
<tr>
<td>Virtual Channel Name</td>
<td>Displays names of defined virtual channels.</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Allows you to edit a virtual channel.</td>
<td></td>
</tr>
<tr>
<td>Default</td>
<td>Marks the default virtual channel of a group.</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>One of the virtual channels in a group must be configured as the default channel. Any traffic not explicitly directed to a particular channel is transmitted by this channel.</td>
<td></td>
</tr>
<tr>
<td>Scheduler Map</td>
<td>Displays the scheduler map assigned to a particular virtual channel.</td>
<td>None</td>
</tr>
<tr>
<td>Shaping Rate</td>
<td>Displays the shaping rate configured for a virtual channel.</td>
<td>None</td>
</tr>
<tr>
<td>Add</td>
<td>Opens a page that allows you to add a virtual channel group.</td>
<td>To add a virtual channel group, click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes a specific virtual channel group.</td>
<td>To remove a specific virtual channel group, select it from the summary page, and click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>

### Add a Virtual Channel Group/Edit a Virtual Channel Group

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Channel Group Name</td>
<td>Specifies a name for a virtual channel group.</td>
<td>To name a group, type the name—for example, wan-vc-group.</td>
</tr>
</tbody>
</table>
Table 198: Virtual Channel Group Quick Configuration Page Summary (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Your Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Creates a virtual channel group.</td>
<td>To create a virtual channel group, click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>Opens a page that allows you to add a virtual channel to the specified group.</td>
<td></td>
</tr>
</tbody>
</table>

**Add a Virtual Channel/Edit Virtual Channel**

<table>
<thead>
<tr>
<th>Virtual Channel Name</th>
<th>Specifies the name of a virtual channel to be assigned to a virtual channel group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>To name a virtual channel, either select a predefined name from the list or type a new name—for example, <strong>branch1-vc</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scheduler Map</th>
<th>Specifies a predefined scheduler map to assign to a virtual channel.</th>
</tr>
</thead>
<tbody>
<tr>
<td>To specify a scheduler map, select it from the Scheduler Map list.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Shaping Rate</th>
<th>Specifies the shaping rate for a virtual channel.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The shaper limits the maximum bandwidth transmitted by a virtual channel.</td>
<td></td>
</tr>
<tr>
<td>Configuring a shaping rate is optional. If no shaping rate is configured, a virtual channel without a shaper can use the full logical interface bandwidth.</td>
<td></td>
</tr>
<tr>
<td>To specify a shaping rate, select one of the following options:</td>
<td></td>
</tr>
<tr>
<td>To specify no shaping rate, select <strong>Unconfigured</strong>.</td>
<td></td>
</tr>
<tr>
<td>To configure a shaping rate as an absolute number of bits per second, select <strong>Absolute Rate</strong> and type a value between 3200 and 32,000,000,000.</td>
<td></td>
</tr>
<tr>
<td>To configure a shaping rate as a percentage, select <strong>Percent</strong> and type a value between 0 and 100.</td>
<td></td>
</tr>
</tbody>
</table>

### Assigning CoS Components to Interfaces

**NOTE:** SRX Series devices do not support WAN interfaces (including T1/E1 and channelized T1/E1).

After you have defined CoS components, you must assign them to logical or physical interfaces. The Assign to Interface option allows you to assign scheduler maps to physical or logical interfaces and to assign forwarding classes, classifiers, rewrite rules, or virtual channel groups to logical interfaces.

To assign interfaces using the J-Web configuration editor:

1. Select **Configure > Class of Service > Assign to Interface**.
   
   The Configure Interface Association summary page appears. The summary page displays the interfaces available for CoS component assignment and the status of existing CoS components.

2. Fill in the options as shown in Table 199 on page 832.
3. To apply the configuration and return to the main configuration page, click **OK**.
4. To cancel your entries and return to the main page, click **Cancel**.

### Table 199: Assigning CoS Components to Interfaces

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure Interface Association</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Displays the port and interface name.</td>
<td>None</td>
</tr>
<tr>
<td>Scheduler Map</td>
<td>Displays predefined scheduler maps for the physical interface.</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>A scheduler map enables the physical interface to have more than one set of output queues.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> For 4-port Fast Ethernet ePIMs, if you apply a CoS scheduler map on outgoing (egress) traffic, the device does not divide the bandwidth appropriately among the CoS queues. As a workaround, configure enforced CoS shaping on the ports.</td>
<td></td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td>Opens an edit page that allows you to associate the system default scheduler map or a preconfigured map to the selected interface.</td>
<td>To change a map for an interface, select it from the Scheduler Map list and click <strong>Edit</strong>.</td>
</tr>
<tr>
<td><strong>Details of Logical Interfaces</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Forwarding class</td>
<td>Displays the forwarding classes assigned to a particular interface.</td>
<td>None</td>
</tr>
<tr>
<td>Scheduler map</td>
<td>Displays the scheduler maps assigned to a particular interface.</td>
<td>None</td>
</tr>
<tr>
<td>Virtual channel group</td>
<td>Displays the virtual channel groups assigned to a particular interface.</td>
<td>None</td>
</tr>
<tr>
<td>Classifier</td>
<td>Displays the classifiers assigned to a particular interface—for example, information about DSCP, DSCPv6, EXP, and inet classifiers.</td>
<td>None</td>
</tr>
<tr>
<td>Rewrite rule</td>
<td>Displays the rewrite rules assigned to a particular interface—for example, information about DSCP, DSCPv6, EXP and inet rewrite rules.</td>
<td>None</td>
</tr>
<tr>
<td><strong>Add</strong></td>
<td>Opens a page that allows you to add a CoS service to a physical interface.</td>
<td>To add a CoS service to a physical interface, click <strong>Add</strong>.</td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td>Opens a page that allows you to edit a CoS services assigned to an interface.</td>
<td>To edit an existing service, select the service in the summary page and click <strong>Edit</strong>.</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Removes CoS services assigned to a specific interface.</td>
<td>To remove CoS services assigned to a specific interface, locate the interface name, click the check box next to it, and click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>
### Table 199: Assigning CoS Components to Interfaces (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add Logical Interface/Edit Logical Interface</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit</td>
<td>Specifies the name of a logical interface.</td>
<td>To specify an interface for CoS assignment, type its name in the Unit box.</td>
</tr>
<tr>
<td></td>
<td>Allows you to assign CoS components to all logical interfaces configured on a physical interface at the same time.</td>
<td>To assign CoS services to all logical interfaces configured on this physical interface, type the wildcard character (*).</td>
</tr>
<tr>
<td>Scheduler Map</td>
<td>Specifies a predefined scheduler map for this interface.</td>
<td>To assign a scheduler map to the interface, select it from the list.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> You can configure either a scheduler map or a virtual channel group on a logical interface, not both.</td>
<td></td>
</tr>
<tr>
<td>Forwarding Class</td>
<td>Assigns a predefined forwarding class to incoming packets on a logical interface.</td>
<td>To assign a forwarding class to the interface, select it from the list.</td>
</tr>
<tr>
<td>Virtual Channel Group</td>
<td>Applies a virtual channel group to a logical interface.</td>
<td>To specify a virtual channel group for the interface, select it from the list.</td>
</tr>
<tr>
<td></td>
<td>Applying a virtual channel group creates a set of eight queues for each virtual channel in the group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> You can configure either a scheduler map or a virtual channel group on a logical interface, not both.</td>
<td></td>
</tr>
<tr>
<td>Classifiers</td>
<td>Allows you to apply classification maps to a logical interface.</td>
<td>To assign a classification map to the interface, select an appropriate classifier for each CoS value type used on the interface.</td>
</tr>
<tr>
<td></td>
<td>Classifiers assign a forwarding class and loss priority to an incoming packet based on its CoS value.</td>
<td></td>
</tr>
<tr>
<td>Rewrite Rules</td>
<td>Allows you to apply rewrite rule configurations to a logical interface.</td>
<td>To apply a rewrite rule configuration to the interface, select a rule for each CoS value type used on the interface.</td>
</tr>
<tr>
<td></td>
<td>Rewrite rules rewrite the CoS values in an outgoing packet based on forwarding class and loss priority.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>You can choose to apply your own rewrite rule or a default one. The default rewrite assignments are based on the default bit definitions of DSCP, DSCP IPv6, MPLS EXP, and IP precedence.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring CoS Components with a Configuration Editor

To configure the device as a node in a network supporting CoS, read the section “Before You Begin” on page 816, determine your needs, and select the tasks you need to perform from the following list. For information about using the J-Web and CLI...
configuration editors, see the J-Web Interface User Guide and the Junos CLI User Guide.

- Configuring a Policer for a Firewall Filter on page 834
- Configuring and Applying a Firewall Filter for a Multifield Classifier on page 835
- Assigning Forwarding Classes to Output Queues on page 838
- Example: Configuring Up to Eight Forwarding Classes on page 841
- Configuring and Applying Rewrite Rules on page 845
- Configuring and Applying Behavior Aggregate Classifiers on page 848
- Configuring RED Drop Profiles for Congestion Control on page 854
- Configuring Schedulers on page 857
- Configuring and Applying Scheduler Maps on page 860
- Scheduler Maps: Sample Configuration on page 863
- Schedulers: Sample Configuration on page 863
- Configuring and Applying Virtual Channels on page 864
- Configuring and Applying an Adaptive Shaper on page 868

**Configuring a Policer for a Firewall Filter**

You configure a policer to detect packets that exceed the limits established for expedited forwarding. The packets that exceed these limits are given a higher loss priority than packets within the bandwidth and burst size limits.

The following example shows how to configure a policer called `ef-policer` that identifies for likely discard expedited forwarding packets with a burst size greater than 2000 bytes and a bandwidth greater than 10 percent.


To configure an expedited forwarding policer for a firewall filter for the Services Router:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 200 on page 835.
3. Go on to “Configuring and Applying a Firewall Filter for a Multifield Classifier” on page 835.
Table 200: Configuring a Policer for a Firewall Filter

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Firewall</strong> level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select <strong>Configure &gt; CLI Tools &gt; Point and Click CLI</strong>&lt;br&gt;2. Next to Firewall, click <strong>Configure or Edit</strong></td>
<td>From the [edit] hierarchy level, enter <strong>edit firewall</strong></td>
</tr>
<tr>
<td>Create the policer for expedited forwarding, and give the policer a name—for example, <strong>ef-policer</strong>.</td>
<td>1. Click <strong>Add new entry</strong> next to Policer.&lt;br&gt;2. In the Policer name box, type <strong>ef-policer</strong></td>
<td>Enter <strong>edit policer ef-policer</strong></td>
</tr>
<tr>
<td>Set the burst limit for the policer—for example, <strong>2k</strong>.</td>
<td>1. Click <strong>Configure</strong> next to If exceeding.&lt;br&gt;2. In the Burst size limit box, type a limit for the burst size allowed—for example, <strong>2k</strong>.&lt;br&gt;3. From the Bandwidth list, select <strong>bandwidth-percent</strong>.&lt;br&gt;4. In the Bandwidth percent box, type <strong>10</strong>.&lt;br&gt;5. Click <strong>OK</strong></td>
<td>Enter <strong>set if-exceeding burst-limit-size 2k</strong>&lt;br&gt;Enter <strong>set if-exceeding bandwidth-percent 10</strong></td>
</tr>
<tr>
<td>Enter the loss priority for packets exceeding the limits established by the policer—for example, <strong>high</strong>.</td>
<td>1. Click <strong>Configure</strong> next to Then.&lt;br&gt;2. From the Loss priority list, select <strong>high</strong>.&lt;br&gt;3. Click <strong>OK</strong></td>
<td>Enter <strong>set then loss-priority high</strong></td>
</tr>
</tbody>
</table>

**Configuring and Applying a Firewall Filter for a Multifield Classifier**

You configure a multifield (MF) classifier to detect packets of interest to CoS and assign the packet to the proper forwarding class independently of the DiffServ code point (DSCP). To configure a multifield classifier on a customer-facing or host-facing link, configure a firewall filter to classify traffic. Packets are classified as they arrive on an interface.

One common way to detect packets of CoS interest is by source or destination address. The destination address is used in this example, but many other matching criteria for packet detection are available to firewall filters.

This example shows how to configure the firewall filter **mf-classifier** and apply it to the Services Router’s Gigabit Ethernet interface **ge-0/0/0**. The firewall filter consists of the rules (terms) listed in Table 201 on page 836.
Table 201: Sample mf-classifier Firewall Filter Terms

<table>
<thead>
<tr>
<th>Rule (Term)</th>
<th>Purpose</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>assured forwarding</td>
<td>Detects packets destined for 192.168.44.55, assigns them to an assured forwarding class, and gives them a low likelihood of being dropped.</td>
<td>Match condition: destination address 192.168.44.55 Forwarding class: af-class Loss priority: low</td>
</tr>
<tr>
<td>expedited-forwarding</td>
<td>Detects packets destined for 192.168.66.77, assigns them to an expedited forwarding class, and subjects them to the EF policer configured in “Configuring a Policer for a Firewall Filter” on page 834.</td>
<td>Match condition: destination address 192.168.66.77 Forwarding class: ef-class Policer: ef-policer</td>
</tr>
<tr>
<td>network control</td>
<td>Detects packets with a network control precedence and forwards them to the network control class.</td>
<td>Match condition: precedence net-control Forwarding class: nc-class</td>
</tr>
<tr>
<td>best-effort-data</td>
<td>Detects all other packets and assigns them to the best effort class.</td>
<td>Forwarding class: be-class</td>
</tr>
</tbody>
</table>


To configure a firewall filter for a multifield classifier for the Services Router:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 202 on page 836.
3. Go on to “Assigning Forwarding Classes to Output Queues” on page 838.

Table 202: Configuring and Applying a Firewall Filter for a Multifield Classifier

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Firewall level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit firewall</td>
</tr>
<tr>
<td></td>
<td>2. Next to Firewall, click Configure or Edit.</td>
<td></td>
</tr>
<tr>
<td>Create the multifield classifier filter and name it—for example, mf-classifier</td>
<td>1. Click Add new entry next to Filter.</td>
<td>Enter</td>
</tr>
<tr>
<td></td>
<td>2. In the Filter name box, type mf-classifier.</td>
<td>edit filter mf-classifier</td>
</tr>
<tr>
<td></td>
<td>3. Select the check box next to Interface specific.</td>
<td>set interface-specific</td>
</tr>
</tbody>
</table>
Table 202: Configuring and Applying a Firewall Filter for a Multifield Classifier (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Create the term for the assured forwarding traffic class, and give it a name—for example, assured-forwarding. | 1. Click **Add new entry** next to Term.  
2. In the Rule name box, type assured-forwarding. | Enter edit term assured-forwarding |
| Create the match condition for the assured forwarding traffic class. Use the destination address for assured forwarding traffic—for example, 192.168.44.55. | 1. Click **Configure** next to From.  
2. Click **Add new entry** next to Destination address.  
3. In the Address box, type 192.168.44.55.  
4. Click OK twice. | Enter set from destination-address 192.168.44.55 |
| Create the forwarding class for assured forwarding DiffServ traffic—for example, af-class. | 1. Click **Configure** next to Then.  
2. In the Forwarding class box, type af-class.  
3. From the Loss priority list, select low.  
4. Click OK twice. | Enter set then forwarding-class af-class  
set then loss-priority low |
| Set the loss priority for the assured forwarding traffic class—for example, low. | | |
| Create the term for the expedited forwarding traffic class, and give it a name—for example, expedited-forwarding. | 1. Click **Add new entry** next to Term.  
2. In the Rule name box, type expedited-forwarding. | From the [edit firewall filter mf-classifier] hierarchy level, enter edit term expedited-forwarding |
| Create the match condition for the expedited forwarding traffic class. Use the destination address for expedited forwarding traffic—for example, 192.168.66.77. | 1. Click **Configure** next to From.  
2. Click **Add new entry** next to Destination address.  
3. In the Address box, type 192.168.66.77.  
4. Click OK twice. | Enter set from destination-address 192.168.66.77 |
| Create the forwarding class for expedited forwarding DiffServ traffic—for example, ef-class. | 1. Click **Configure** next to Then.  
2. In the Forwarding class box, type ef-class.  
3. From the Policer choice list, select Policer.  
4. In the Policer box, type ef-policer.  
5. Click OK twice. | Enter set then forwarding-class ef-class  
set then policer ef-policer |
| Apply the policer for the expedited forwarding traffic class. Use the EF policer previously configured for expedited forwarding DiffServ traffic—ef-policer. (See “Configuring a Policer for a Firewall Filter” on page 834.) | | |
| Create the term for the network control traffic class, and give it a name—for example, network-control. | 1. Click **Add new entry** next to Term.  
2. In the Rule name box, type network-control. | From the [edit firewall filter mf-classifier] hierarchy level, enter edit term network-control |
Table 202: Configuring and Applying a Firewall Filter for a Multifield Classifier (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create the match condition for the network control traffic class.</td>
<td></td>
<td>Enter set from precedence net-control</td>
</tr>
<tr>
<td>1. Click Configure next to From.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. From the Precedence choice list, select Precedence.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Click Add new entry next to Precedence.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. From the Value keyword list, select net-control.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Click OK twice.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create the forwarding class for the network control traffic class, and give it a name—for example, nc-class.</td>
<td></td>
<td>Enter set then forwarding-class nc-class</td>
</tr>
<tr>
<td>1. Click Configure next to Then.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. In the Forwarding class box, type nc-class.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Click OK twice.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create the term for the best-effort traffic class, and give it a name—for example, best-effort-data.</td>
<td></td>
<td>From the [edit firewall filter mf-classifier] hierarchy level, enter edit term best-effort-data</td>
</tr>
<tr>
<td>1. Click Add new entry next to Term.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. In the Rule name box, type best-effort-data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create the forwarding class for the best-effort traffic class, and give it a name—for example, be-class. (Because this is the last term in the filter, it has no match condition.)</td>
<td></td>
<td>Enter set then forwarding-class be-class</td>
</tr>
<tr>
<td>1. Click Configure next to Then.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. In the Forwarding class box, type be-class.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Click OK four times.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Navigate to the Interfaces level in the configuration hierarchy.</td>
<td>On the main Configuration page next to Interfaces, click Configure or Edit.</td>
<td>From the [edit] hierarchy level, enter edit interfaces</td>
</tr>
<tr>
<td>Apply the multifield classifier firewall filter mf-classifier as an input filter on each customer-facing or host-facing interface that needs the filter—for example, on ge-0/0/0, unit 0.</td>
<td></td>
<td>Enter set ge-0/0/0 unit 0 family inet filter input mf-classifier</td>
</tr>
<tr>
<td>1. Click the Interface ge-0/0/0 and Unit 0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Click Configure next to Inet.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Click Configure next to Filter.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. From the Input choice list, select Input.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. In the Input box, type mf-classifier.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Click OK.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Assigning Forwarding Classes to Output Queues

You must assign the forwarding classes established by the mf-classifier multifield classifier to output queues. This example assigns output queues as shown in Table 203 on page 839.
Table 203: Sample Output Queue Assignments for mf-classifier Forwarding Queues

<table>
<thead>
<tr>
<th>mf-classifier Forwarding Class</th>
<th>For Traffic Type</th>
<th>Output Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>be-class</td>
<td>Best-effort traffic</td>
<td>Queue 0</td>
</tr>
<tr>
<td>ef-class</td>
<td>Expedited forwarding traffic</td>
<td>Queue 1</td>
</tr>
<tr>
<td>af-class</td>
<td>Assured forwarding traffic</td>
<td>Queue 2</td>
</tr>
<tr>
<td>nc-class</td>
<td>Network control traffic</td>
<td>Queue 3</td>
</tr>
</tbody>
</table>

For multifield classifier details, see “Configuring and Applying a Firewall Filter for a Multifield Classifier” on page 835.

To assign forwarding classes to output queues:
1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 204 on page 839.
3. Go on to “Configuring and Applying Rewrite Rules” on page 845.

Table 204: Assigning Forwarding Classes to Output Queues

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Class of service level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select <strong>Configure &gt; CLI Tools &gt; Point and Click CLI</strong>. 2. Next to Class of service, click <strong>Configure</strong> or <strong>Edit</strong>.</td>
<td>From the [edit] hierarchy level, enter edit class-of-service</td>
</tr>
<tr>
<td>Assign best-effort traffic to queue 0.</td>
<td>1. Click <strong>Configure</strong> next to Forwarding classes. 2. Click <strong>Add new entry</strong> next to Queue. 3. In the Queue num box, type 0. 4. In the Class name box, type the previously configured name of the best-effort class—be-class. 5. Click <strong>OK</strong>.</td>
<td>Enter set forwarding-classes queue 0 be-class</td>
</tr>
<tr>
<td>Assign expedited forwarding traffic to queue 1.</td>
<td>1. Click <strong>Add new entry</strong> next to Queue. 2. In the Queue num box, type 1. 3. In the Class name box, type the previously configured name of the expedited forwarding class—ef-class. 4. Click <strong>OK</strong>.</td>
<td>Enter set forwarding-classes queue 1 ef-class</td>
</tr>
</tbody>
</table>
### Configuring Forwarding Classes

To configure CoS forwarding classes on an SRX Series device, include the following statements at the \[edit class-of-service\] hierarchy level of the configuration:

```plaintext
[edit class-of-service]
forwarding-classes {
  class class-name queue-num queue-number priority (high | low);
  queue queue-number class-name priority (high | low);
}
interfaces {
  interface-name {
    unit logical-unit-number {
      forwarding-class class-name;
    }
  }
}
restricted-queues {
  forwarding-class class-name queue-number;
}
```

You cannot commit a configuration that assigns the same forwarding class to two different queues.

### Assigning a Forwarding Class to an Interface

On an SRX Series device, you can configure fixed classification on a logical interface by specifying a forwarding class to be applied to all packets received by the logical interface, regardless of the packet contents.

To assign a forwarding class configuration to the input logical interface, include the `forwarding-class` statement at the \[edit class-of-service interfaces interface-name unit logical-unit-number\] hierarchy level:

---

**Table 204: Assigning Forwarding Classes to Output Queues (continued)**

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign assured forwarding traffic to queue 2.</td>
<td>1. Click <strong>Add new entry</strong> next to Queue. 2. In the Queue num box, type 2. 3. In the Class name box, type the previously configured name of the assured forwarding class—af-class. 4. Click <strong>OK</strong>.</td>
<td>Enter set forwarding-classes queue 2 af-class</td>
</tr>
<tr>
<td>Assign network control traffic to queue 3.</td>
<td>1. Click <strong>Add new entry</strong> next to Queue. 2. In the Queue num box, type 3. 3. In the Class name box, type the previously configured name of the network control forwarding class—nc-class. 4. Click <strong>OK</strong>.</td>
<td>Enter set forwarding-classes queue 3 nc-class</td>
</tr>
</tbody>
</table>
[edit class-of-service interfaces interface-name unit logical-unit-number]
forwarding-class class-name;

You can include interface wildcards for interface-name and logical-unit-number.

In the following example, all packets coming into the device from the ge-3/0/0.0 interface are assigned to the assured-forwarding forwarding class:

[edit class-of-service]
interfaces {
  ge-3/0/0 {
    unit 0 {
      forwarding-class assured-forwarding;
    }
  }
}

**Example: Configuring Up to Eight Forwarding Classes**

By default on all platforms, four output queues are mapped to four forwarding classes as shown in Table 186 on page 806. On J Series or SRX Series devices, you can configure up to eight forwarding classes and eight queues.

To configure up to eight forwarding classes, include the queue statement at the [edit class-of-service forwarding-classes] hierarchy level:

[edit class-of-service forwarding-classes]
queue queue-number class-name;

The output queue number can be from 0 through 7, and you must map the forwarding classes one-to-one with the output queues. The default scheduler transmission rate and buffer size percentages for queues 0 through 7 are 95, 0, 0, 5, 0, 0, 0, and 0 percent.

For example, to configure a one-to-one mapping between eight forwarding classes and eight queues: you would use the following configuration:

[edit class-of-service]
forwarding-classes {
  queue 0 be;
  queue 1 ef;
  queue 2 af;
  queue 3 nc;
  queue 4 ef1;
  queue 5 ef2;
  queue 6 af1;
  queue 7 nc1;
}

**Defining Eight Classifiers**

[edit class-of-service]
classifiers {
  dscp dscp-table {
    forwarding-class ef {
      loss-priority low code-points [101000, 101001];
      loss-priority high code-points [101010, 101011];
    }
  }
}
Adding Eight Schedulers to a Scheduler Map

Configure a custom scheduler map that applies globally to all interfaces, except those that are restricted to four queues:

```
[edit class-of-service]
scheduler-maps {
sched {
    forwarding-class be scheduler Q0;
    forwarding-class ef scheduler Q1;
    forwarding-class af scheduler Q2;
    forwarding-class nc scheduler Q3;
    forwarding-class ef1 scheduler Q4;
    forwarding-class ef2 scheduler Q5;
    forwarding-class af1 scheduler Q6;
    forwarding-class nc1 scheduler Q7;
}
}
schedulers {
    Q0 {
        transmit-rate percent 25;
        buffer-size percent 25;
        priority low;
        drop-profile-map loss-priority any protocol both drop-default;
    }
    Q1 {
        buffer-size temporal 2000;
    }
```
priority strict-high;
drop-profile-map loss-priority any protocol both drop-ef;
}
Q2 {
    transmit-rate percent 35;
    buffer-size percent 35;
    priority low;
    drop-profile-map loss-priority any protocol both drop-default;
}
Q3 {
    transmit-rate percent 5;
    buffer-size percent 5;
    drop-profile-map loss-priority any protocol both drop-default;
}
Q4 {
    transmit-rate percent 5;
    priority high;
    drop-profile-map loss-priority any protocol both drop-ef;
}
Q5 {
    transmit-rate percent 10;
    priority high;
    drop-profile-map loss-priority any protocol both drop-ef;
}
Q6 {
    transmit-rate remainder;
    priority low;
    drop-profile-map loss-priority any protocol both drop-default;
}
Q7 {
    transmit-rate percent 5;
    priority high;
    drop-profile-map loss-priority any protocol both drop-default;
}

Configuring CoS Components with a Configuration Editor
Configuring CoS Components with a Configuration Editor
Configuring and Applying Rewrite Rules

You can configure rewrite rules to replace DiffServ code points (DSCPs) on packets received from the customer or host with the values expected by other devices. You do not have to configure rewrite rules if the received packets already contain valid DSCPs. Rewrite rules apply the forwarding class information and packet loss priority used internally by the device to establish the DSCP on outbound packets. Once configured, you must apply the rewrite rules to the correct interfaces.

The following example shows how to create the rewrite rules `rewrite-dscps` and apply them to the device’s Gigabit Ethernet interface `ge-0/0/0`. The rewrite rules replace the DSCPs on packets in the four forwarding classes, as shown in Table 205 on page 845.

<table>
<thead>
<tr>
<th>mf-classifier Forwarding Class</th>
<th>For CoS Traffic Type</th>
<th>rewrite-dscps Rewrite Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>be-class</td>
<td>Best-effort traffic</td>
<td>Low-priority code point: 00000000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High-priority code point: 0000001</td>
</tr>
<tr>
<td>ef-class</td>
<td>Expedited forwarding traffic</td>
<td>Low-priority code point: 101110</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High-priority code point: 101111</td>
</tr>
<tr>
<td>af-class</td>
<td>Assured forwarding traffic</td>
<td>Low-priority code point: 001010</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High-priority code point: 001100</td>
</tr>
<tr>
<td>nc-class</td>
<td>Network control traffic</td>
<td>Low-priority code point: 110000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High-priority code point: 110001</td>
</tr>
</tbody>
</table>

To configure and apply rewrite rules for the device:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 206 on page 846.
3. Go on to “Configuring and Applying Behavior Aggregate Classifiers” on page 848.

```bash
  loss-priority low code-point 111;
} forward-class nc2 {
  loss-priority low code-point 110;
}
```
### Table 206: Configuring and Applying Rewrite Rules

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Navigate to the **Class of service** level in the configuration hierarchy. | 1. In the J-Web interface, select **Configure > CLI Tools > Point and Click CLI**.  
2. Next to Class of service, click **Configure or Edit**. | From the [edit] hierarchy level, enter  
**edit class-of-service** |
| Configure rewrite rules for DiffServ CoS. | 1. Click **Configure** next to Rewrite rules.  
2. Click **Add new entry** next to Dscp.  
3. In the Name box, type the name of the rewrite rules—for example, **rewrite-dscps**. | Enter  
**edit rewrite-rules dscp rewrite-dscps** |
| Configure best-effort forwarding class rewrite rules. | 1. Click **Add new entry** next to Forwarding class.  
2. In the Class name box, type the name of the previously configured best-effort forwarding class—**be-class**.  
3. Click **Add new entry** next to Loss priority.  
4. From the Loss val list, select **low**.  
5. In the Code point box, type the value of the low-priority code point for best-effort traffic—for example, **000000**.  
6. Click **OK**.  
7. Click **Add new entry** next to Loss priority.  
8. From the Loss val list, select **high**.  
9. In the Code point box, type the value of the high-priority code point for best-effort traffic—for example, **000001**.  
10. Click **OK** twice. | Enter  
**set forwarding-class be-class loss-priority low code-point 000000**  
**set forwarding-class be-class loss-priority high code-point 000001** |
### Table 206: Configuring and Applying Rewrite Rules (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Configure expedited forwarding class rewrite rules. | 1. Click **Add new entry** next to Forwarding class.  
2. In the Class name box, type the name of the previously configured expedited forwarding class—**ef-class**.  
3. Click **Add new entry** next to Loss priority.  
4. From the Loss val list, select **low**.  
5. In the Code point box, type the value of the low-priority code point for expedited forwarding traffic—for example, **101110**.  
6. Click **OK**.  
7. Click **Add new entry** next to Loss priority.  
8. From the Loss val list, select **high**.  
9. In the Code point box, type the value of the high-priority code point for expedited forwarding traffic—for example, **101111**.  
10. Click **OK** twice. | Enter  
set forwarding-class ef-class loss-priority low code-point 101110  
set forwarding-class ef-class loss-priority high code-point 101111 |
| Configure assured forwarding class rewrite rules. | 1. Click **Add new entry** next to Forwarding class.  
2. In the Class name box, type the name of the previously configured assured forwarding class—**af-class**.  
3. Click **Add new entry** next to Loss priority.  
4. From the Loss val list, select **low**.  
5. In the Code point box, type the value of the low-priority code point for assured forwarding traffic—for example, **001010**.  
6. Click **OK**.  
7. Click **Add new entry** next to Loss priority.  
8. From the Loss val list, select **high**.  
9. In the Code point box, type the value of the high-priority code point for assured forwarding traffic—for example, **001100**.  
10. Click **OK** twice. | Enter  
set forwarding-class af-class loss-priority low code-point 001010  
set forwarding-class af-class loss-priority high code-point 001100 |
### Table 206: Configuring and Applying Rewrite Rules (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure network control class rewrite rules.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Click <strong>Add new entry</strong> next to <strong>Forwarding class.</strong></td>
<td></td>
<td>Enter</td>
</tr>
<tr>
<td>2. In the <strong>Class name box</strong>, type the name of the previously configured network control forwarding class—<strong>nc-class</strong>.</td>
<td></td>
<td>set forwarding-class nc-class loss-priority low code-point 110000</td>
</tr>
<tr>
<td>3. Click <strong>Add new entry</strong> next to <strong>Loss priority.</strong></td>
<td></td>
<td>set forwarding-class nc-class loss-priority high code-point 110001</td>
</tr>
<tr>
<td>4. From the <strong>Loss val list</strong>, select <strong>low</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. In the <strong>Code point box</strong>, type the value of the low-priority code point for network control traffic—for example, <strong>110000</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Click <strong>OK</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Click <strong>Add new entry</strong> next to <strong>Loss priority.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. From the <strong>Loss val list</strong>, select <strong>high</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. In the <strong>Code point box</strong>, type the value of the high-priority code point for network control traffic—for example, <strong>110001</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Click <strong>OK</strong> four times.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Apply rewrite rules to an interface.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(See the interface naming conventions in <em>Junos OS Interfaces Configuration Guide for Security Devices.</em>)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Click <strong>Add new entry</strong> next to <strong>Interfaces</strong></td>
<td></td>
<td>From the [edit class of service] hierarchy level, enter</td>
</tr>
<tr>
<td>2. In the <strong>Interface name box</strong>, type the name of the interface—for example, <strong>ge-0/0/0</strong>.</td>
<td></td>
<td>set interfaces ge-0/0/0 unit 0 rewrite-rules dscp rewrite-dscps</td>
</tr>
<tr>
<td>3. Click <strong>Add new entry</strong> next to <strong>Unit</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. In the <strong>Unit number box</strong>, type the logical interface unit number—<strong>0</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Click <strong>Configure</strong> next to <strong>Rewrite rules.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. In the <strong>Rewrite rules name box</strong>, under <strong>Dscp</strong>, type the name of the previously configured rewrite rules—<strong>rewrite-dscps</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Click <strong>OK</strong>.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring and Applying Behavior Aggregate Classifiers

You configure behavior aggregate classifiers to classify packets that contain valid DSCPs to appropriate queues. Once configured, you must apply the behavior aggregate classifier to the correct interfaces.
The following example shows how to configure the DSCP behavior aggregate classifier `ba-classifier` as the default DSCP map, and apply it to the device’s Gigabit Ethernet interface `ge-0/0/0`. The behavior aggregate classifier assigns loss priorities, as shown in Table 207 on page 849, to incoming packets in the four forwarding classes.

### Table 207: Sample ba-classifier Loss Priority Assignments

<table>
<thead>
<tr>
<th>mf-classifier Forwarding Class</th>
<th>For CoS Traffic Type</th>
<th>ba-classifier Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>be-class</td>
<td>Best-effort traffic</td>
<td>High-priority code point: 000001</td>
</tr>
<tr>
<td>ef-class</td>
<td>Expedited forwarding traffic</td>
<td>High-priority code point: 101111</td>
</tr>
<tr>
<td>af-class</td>
<td>Assured forwarding traffic</td>
<td>High-priority code point: 001100</td>
</tr>
<tr>
<td>nc-class</td>
<td>Network control traffic</td>
<td>High-priority code point: 110001</td>
</tr>
</tbody>
</table>

To configure and apply behavior aggregate classifiers for the device:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 208 on page 849.
3. Go on to “Configuring RED Drop Profiles for Congestion Control” on page 854.

### Table 208: Configuring and Applying Behavior Aggregate Classifiers

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Class of service level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>1. From the [edit] hierarchy level, enter edit class-of-service.</td>
</tr>
<tr>
<td></td>
<td>2. Next to Class of service, click Configure or Edit.</td>
<td>2. Enter edit classifiers dscp ba-classifier.</td>
</tr>
<tr>
<td>Configure behavior aggregate classifiers for DiffServ CoS.</td>
<td>1. Click Configure next to Classifiers.</td>
<td>3. Enter set import default.</td>
</tr>
<tr>
<td></td>
<td>2. Click Add new entry next to Dscp.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. In the Name box, type the name of the behavior aggregate classifier—for example, ba-classifier.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. In the Import box, type the name of the default DSCP map, default.</td>
<td></td>
</tr>
</tbody>
</table>
Table 208: Configuring and Applying Behavior Aggregate Classifiers (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a best-effort forwarding class classifier.</td>
<td>1. Click <strong>Add new entry</strong> next to Forwarding class.</td>
<td>Enter set forwarding-class be-class loss-priority high code-points 000001</td>
</tr>
<tr>
<td></td>
<td>2. In the Class name box, type the name of the previously configured best-effort forwarding class—be-class.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add new entry</strong> next to Loss priority.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. From the Loss val list, select <strong>high</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Add new entry</strong> next to Code points.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. In the Value box, type the value of the high-priority code point for best-effort traffic—for example, 00001.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>OK</strong> three times.</td>
<td></td>
</tr>
</tbody>
</table>

Configure an expedited forwarding class classifier.

1. Click **Add new entry** next to Forwarding class.
2. In the Class name box, type the name of the previously configured expedited forwarding class—ef-class.
3. Click **Add new entry** next to Loss priority.
4. From the Loss val list, select **high**.
5. Click **Add new entry** next to Code points.
6. In the Value box, type the value of the high-priority code point for expedited forwarding traffic—for example, 101111.
7. Click **OK** three times.

Enter set forwarding-class ef-class loss-priority high code-points 101111
### Table 208: Configuring and Applying Behavior Aggregate Classifiers *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Configure an assured forwarding class classifier. | 1. Click **Add new entry** next to Forwarding class.  
2. In the Class name box, type the name of the previously configured assured forwarding class—**af-class**.  
3. Click **Add new entry** next to Loss priority.  
4. From the Loss val list, select **high**.  
5. Click **Add new entry** next to Code points.  
6. In the Value box, type the value of the high-priority code point for assured forwarding traffic—for example, **001100**.  
7. Click **OK** three times. | Enter  
set forwarding-class af-class loss-priority high code-points 001100 |
| Configure a network control class classifier. | 1. Click **Add new entry** next to Forwarding class.  
2. In the Class name box, type the name of the previously configured network control forwarding class—**nc-class**.  
3. Click **Add new entry** next to Loss priority.  
4. From the Loss val list, select **high**.  
5. Click **Add new entry** next to Code points.  
6. In the Value box, type the value of the high-priority code point for network control traffic—for example, **110001**.  
7. Click **OK** five times. | Enter  
set forwarding-class nc-class loss-priority high code-points 110001 |
Table 208: Configuring and Applying Behavior Aggregate Classifiers (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply the behavior aggregate classifier to an interface.</td>
<td>1. Click Add new entry next to Interfaces.</td>
<td>From the [edit class of service] hierarchy level, enter set interfaces ge-0/0/0 unit 0 classifiers dscp ba-classifier</td>
</tr>
<tr>
<td>(See the interface naming conventions in Junos OS Interfaces Configuration Guide for Security Devices)</td>
<td>2. In the Interface name box, type the name of the interface—for example, ge-0/0/0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Click Add new entry next to Unit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. In the Unit number box, type the logical interface unit number—0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Click Configure next to Classifiers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. In the Classifiers box, under Dscp, type the name of the previously configured behavior aggregate classifier—ba-classifier.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. Click OK.</td>
<td></td>
</tr>
</tbody>
</table>

Example: Defining Aliases for Bits

When you configure classes and define classifiers, you can refer to the markers by alias names. You can configure user-defined classifiers in terms of alias names. If the value of an alias changes, it alters the behavior of any classifier that references it.

To define a code-point alias on an SRX Series device, include the code-point-aliases statement at the [edit class-of-service] hierarchy level:

```
[edit class-of-service]
code-point-aliases {
  (dscp | exp | ieee-802.1 | inet-precedence) {
    alias-name bits;
  }
}
```

The CoS marker types are as follows:

- **dscp**—Handles incoming IPv4 packets.
- **exp**—Handles MPLS packets using Layer 2 headers.
- **ieee-802.1**—Handles Layer 2 CoS.
- **inet-precedence**—Handles incoming IPv4 packets. IP precedence mapping requires only the upper three bits of the DSCP field.

For example, you can set up the following configuration:

```
[edit class-of-service]
code-point-aliases {
  dscp {
    alias-name bits;
  }
}
The sample configuration produces this mapping:

```
user@host> show class-of-service code-point-aliases dscp
Alias       Bit pattern
ef/my2      101110
af11        001010
af12        001100
af13        001110
af21        010010
af22        010100
af23        010110
af31        011010
af32        011100
af33        011110
af41        100010
af42        100100
af43        100110
be          000001
cs1         001000
cs2         010000
cs3         011000
cs4         100000
cs5         101000
nc1/cs6/cs7 110000
nc2         111000
my1         110001
```

The following notes explain certain results in the mapping:

- **my1 110001**:
  - 110001 was not mapped to anything before, and my1 is a new alias.
  - Nothing in the default mapping table is changed by this statement.

- **my2 101110**:
  - 101110 is now mapped to my2 as well as ef.

- **be 000001**:
  - be is now mapped to 000001.
  - The old value of be, 000000, is not associated with any alias. Packets with this DSCP value are now mapped to the default forwarding class.

- **cs7 110000**:
  - cs7 is now mapped to 110000, as well as nc1 and cs6.
  - The old value of cs7, 111000, is still mapped to nc2.
Configuring RED Drop Profiles for Congestion Control

If the device must support assured forwarding, you can control congestion by configuring random early detection (RED) drop profiles. RED drop profiles use drop probabilities for different levels of buffer fullness to determine which scheduling queue on the device is likely to drop assured forwarding packets under congested conditions. The device can drop packets when the queue buffer becomes filled to the configured percentage.

Assured forwarding traffic with the PLP (packet loss priority) bit set is more likely to be discarded than traffic without the PLP bit set. This example shows how to configure a drop probability and a queue fill level for both PLP and non-PLP assured forwarding traffic. It is only one example of how to use RED drop profiles.

The example shows how to configure the RED drop profiles listed in Table 209 on page 854.

Table 209: Sample RED Drop Profiles

<table>
<thead>
<tr>
<th>Drop Profile</th>
<th>Drop Probability</th>
<th>Queue Fill Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>af-normal—For non-PLP (normal) assured forwarding traffic</td>
<td>Between 0 (never dropped) and 100 percent (always dropped)</td>
<td>Between 95 and 100 percent</td>
</tr>
<tr>
<td>af-with-plp—For PLP (aggressive packet dropping) assured forwarding traffic</td>
<td>Between 95 and 100 percent (always dropped)</td>
<td>Between 80 and 95 percent</td>
</tr>
</tbody>
</table>

To configure RED drop profiles for assured forwarding congestion control on the device:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 210 on page 855.
3. If you are finished configuring the device, commit the configuration.
4. Go on to one of the following tasks:
   - To assign resources, priorities, and profiles to output queues, see “Configuring Schedulers” on page 857.
   - To apply rules to logical interfaces, see “Configuring and Applying Virtual Channels” on page 864.
   - To use adaptive shapers to limit bandwidth for Frame Relay, see “Configuring Adaptive Shaping for Frame Relay” on page 875.
   - To check the configuration, see “Verifying a CoS Configuration” on page 941.
Table 210: Configuring RED Drop Profiles for Assured Forwarding Congestion Control

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Class of service level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI. 2. Next to Class of service, click Configure or Edit.</td>
<td>From the [edit] hierarchy level, enter edit class-of-service.</td>
</tr>
<tr>
<td>Configure the lower drop probability for normal, non-PLP traffic.</td>
<td>1. Click Add new entry next to Drop profiles. 2. In the Profile name box, type the name of the drop profile—for example, af-normal. 3. Click Configure next to Interpolate. 4. Click Add new entry next to Drop probability. 5. In the Value box, type a number for the first drop point—for example, 0. 6. Click OK. 7. Click Add new entry next to Drop probability again. 8. In the Value box, type a number for the next drop point—for example, 100. 9. Click OK.</td>
<td>Enter edit drop-profiles af-normal interpolate set drop-probability 0 set drop-probability 100.</td>
</tr>
<tr>
<td>Configure a queue fill level for the lower non-PLP drop probability.</td>
<td>1. Click Add new entry next to Fill level. 2. In the Value box, type a number for the first fill level—for example, 95. 3. Click OK. 4. Click Add new entry next to Fill level. 5. In the Value box, type a number for the next fill level—for example, 100. 6. Click OK three times.</td>
<td>Enter set fill-level 95 set fill-level 100.</td>
</tr>
<tr>
<td>Configure the higher drop probability for PLP traffic.</td>
<td>1. Click Add new entry next to Drop profiles. 2. In the Profile name box, type the name of the drop profile—for example, af-with-plp. 3. Click Configure next to Interpolate. 4. Click Add new entry next to Drop probability. 5. In the Value box, type a number for the first drop point—for example, 95. 6. Click OK. 7. Click Add new entry next to Drop probability. 8. In the Value box, type a number for the next drop point—for example, 100. 9. Click OK.</td>
<td>From the [edit class of service] hierarchy level, enter edit drop-profiles af-with-PLP interpolate set drop-probability 95 set drop-probability 100.</td>
</tr>
</tbody>
</table>
Table 210: Configuring RED Drop Profiles for Assured Forwarding Congestion Control (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Configure a queue fill level for the higher PLP drop probability. | 1. Click Add new entry next to Fill level. Enter set fill-level 80  
2. In the Value box, type a number for the first fill level—for example, 80.  
3. Click OK. set fill-level 95  
4. Click Add new entry next to Fill level.  
5. In the Value box, type a number for the next fill level—for example, 95.  
6. Click OK. | |

Example: Configuring RED Drop Profiles

Create a segmented configuration and an interpolated configuration that correspond to the graphs in Figure 94 on page 856. The values defined in the configuration are matched to represent the data points in the graph line. In this example, the drop probability is 25 percent when the queue is 50 percent full. The drop probability increases to 50 percent when the queue is 75 percent full.

Figure 94: Segmented and Interpolated Drop Profiles

Segmented
class-of-service {
    drop-profiles {
        segmented-style-profile {
            fill-level 25 drop-probability 25;
            fill-level 50 drop-probability 50;
            fill-level 75 drop-probability 75;
            fill-level 95 drop-probability 100;
        }
    }
}
To create the profile’s graph line, the software begins at the bottom-left corner, representing a 0 percent fill level and a 0 percent drop probability. This configuration draws a line directly to the right until it reaches the first defined fill level, 25 percent for this configuration. The software then continues the line vertically until the first drop probability is reached. This process is repeated for all of the defined levels and probabilities until the top-right corner of the graph is reached.

Create a smoother graph line by configuring the profile with the **interpolate** statement. This allows the software to automatically generate 64 data points on the graph beginning at (0, 0) and ending at (100, 100). Along the way, the graph line intersects specific data points, which you define as follows:

```plaintext
Interpolated class-of-service {
    drop-profiles {
        interpolated-style-profile {
            interpolate {
                fill-level [ 50 75 ];
                drop-probability [ 25 50 ];
            }
        }
    }
}
```

### Configuring Schedulers

You configure schedulers to assign resources, priorities, and drop profiles to output queues. By default, only queues 0 and 3 have resources assigned.

**NOTE:** SRX Series devices support hierarchical schedulers, including per-unit-schedulers. For more information, see “Configuring CoS Hierarchical Schedulers” on page 910.

This example creates the schedulers listed in Table 211 on page 857.

<table>
<thead>
<tr>
<th>Scheduler</th>
<th>For CoS Traffic Type</th>
<th>Assigned Priority</th>
<th>Allocated Portion of Queue Buffer</th>
<th>Assigned Bandwidth (Transmit Rate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>be-scheduler</td>
<td>Best-effort traffic</td>
<td>Low</td>
<td>40 percent</td>
<td>10 percent</td>
</tr>
<tr>
<td>ef-scheduler</td>
<td>Expedited forwarding traffic</td>
<td>High</td>
<td>10 percent</td>
<td>10 percent</td>
</tr>
<tr>
<td>af-scheduler</td>
<td>Assured forwarding traffic</td>
<td>High</td>
<td>45 percent</td>
<td>45 percent</td>
</tr>
<tr>
<td>nc-scheduler</td>
<td>Network control traffic</td>
<td>Low</td>
<td>5 percent</td>
<td>5 percent</td>
</tr>
</tbody>
</table>

To configure schedulers for the device:
1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 212 on page 858.

### Table 212: Configuring Schedulers

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Class of service level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI</td>
<td>From the [edit] hierarchy level, enter edit class-of-service</td>
</tr>
<tr>
<td></td>
<td>2. Next to Class of service, click Configure or Edit.</td>
<td></td>
</tr>
<tr>
<td>Configure a best-effort scheduler.</td>
<td>1. Click Add new entry next to Schedulers.</td>
<td>Enter</td>
</tr>
<tr>
<td></td>
<td>2. In the Scheduler name box, type the name of the best-effort scheduler—for example, be-scheduler.</td>
<td>edit schedulers be-scheduler</td>
</tr>
<tr>
<td>Configure a best-effort scheduler priority and buffer size.</td>
<td>1. In the Priority box, type low.</td>
<td>Enter</td>
</tr>
<tr>
<td></td>
<td>2. Click Configure next to Buffer size.</td>
<td>set priority low</td>
</tr>
<tr>
<td></td>
<td>3. From the Buffer size choice list, select the basis for the buffer allocation method—for example, Percent.</td>
<td>set buffer-size percent 40</td>
</tr>
<tr>
<td></td>
<td>4. In the Percent box, type the percentage of the buffer to be used by the best-effort scheduler—for example, 40.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Click OK</td>
<td></td>
</tr>
<tr>
<td>Configure a best-effort scheduler transmit rate.</td>
<td>1. Click Configure next to Transmit rate.</td>
<td>Enter</td>
</tr>
<tr>
<td></td>
<td>2. From the Transmit rate choice list, select the basis for the transmit rate method—for example, Percent.</td>
<td>set transmit-rate percent 10</td>
</tr>
<tr>
<td></td>
<td>3. In the Percent box, type the percentage of the bandwidth to be used by the best-effort scheduler—for example, 10.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Click OK</td>
<td></td>
</tr>
<tr>
<td>Configure an expedited forwarding scheduler.</td>
<td>1. Click Add new entry next to Schedulers.</td>
<td>From the [edit class of service] hierarchy level, enter edit schedulers ef-scheduler</td>
</tr>
<tr>
<td></td>
<td>2. In the Scheduler name box, type the name of the expedited forwarding scheduler—for example, ef-scheduler.</td>
<td></td>
</tr>
<tr>
<td>Configure an expedited forwarding scheduler priority and buffer size.</td>
<td>1. In the Priority box, type high.</td>
<td>Enter</td>
</tr>
<tr>
<td></td>
<td>2. Click Configure next to Buffer size.</td>
<td>set priority high</td>
</tr>
<tr>
<td></td>
<td>3. From the Buffer size choice list, select the basis for the buffer allocation method—for example, Percent.</td>
<td>set buffer-size percent 10</td>
</tr>
<tr>
<td></td>
<td>4. In the Percent box, type the percentage of the buffer to be used by the expedited forwarding scheduler—for example, 10.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Click OK</td>
<td></td>
</tr>
</tbody>
</table>
### Table 212: Configuring Schedulers (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure an expedited forwarding scheduler transmit rate.</strong></td>
<td>1. Click <strong>Configure</strong> next to Transmit rate.  &lt;br&gt;2. From the Transmit rate choice list, select the basis for the transmit rate method—for example, <strong>Percent</strong>.  &lt;br&gt;3. In the Percent box, type the percentage of the bandwidth to be used by the expedited forwarding scheduler—for example, <strong>10</strong>.  &lt;br&gt;4. Click <strong>OK</strong> twice.</td>
<td>Enter  &lt;br&gt;set transmit-rate percent 10</td>
</tr>
<tr>
<td><strong>Configure an assured forwarding scheduler.</strong></td>
<td>1. Click <strong>Add new entry</strong> next to Schedulers.  &lt;br&gt;2. In the Scheduler name box, type the name of the assured forwarding scheduler—for example, <strong>af-scheduler</strong>.</td>
<td><strong>From the [edit class of service] hierarchy level, enter</strong>  &lt;br&gt;<strong>edit schedulers af-scheduler</strong></td>
</tr>
<tr>
<td><strong>Configure an assured forwarding scheduler priority and buffer size.</strong></td>
<td>1. In the Priority box, type <strong>high</strong>.  &lt;br&gt;2. Click <strong>Configure</strong> next to Buffer size.  &lt;br&gt;3. From the Buffer size choice list, select the basis for the buffer allocation method—for example, <strong>Percent</strong>.  &lt;br&gt;4. In the Percent box, type the percentage of the buffer to be used by the assured forwarding scheduler—for example, <strong>45</strong>.  &lt;br&gt;5. Click <strong>OK</strong>.</td>
<td>Enter  &lt;br&gt;set priority high  &lt;br&gt;set buffer-size percent 45</td>
</tr>
<tr>
<td><strong>Configure an assured forwarding scheduler transmit rate.</strong></td>
<td>1. Click <strong>Configure</strong> next to Transmit rate.  &lt;br&gt;2. From the Transmit rate choice list, select the basis for the transmit rate method—for example, <strong>Percent</strong>.  &lt;br&gt;3. In the Percent box, type the percentage of the bandwidth to be used by the assured forwarding scheduler—for example, <strong>45</strong>.  &lt;br&gt;4. Click <strong>OK</strong>.</td>
<td>Enter  &lt;br&gt;set transmit-rate percent 45</td>
</tr>
<tr>
<td><strong>(Optional) Configure a drop profile map for assured forwarding low and high priority. (DiffServ can have a RED drop profile associated with assured forwarding.)</strong></td>
<td>1. Click <strong>Add new entry</strong> next to Drop profile map.  &lt;br&gt;2. From the Loss priority box, select <strong>Low</strong>.  &lt;br&gt;3. From the Protocol box, select <strong>Any</strong>.  &lt;br&gt;4. In the Drop profile box, type the name of the drop profile—for example, <strong>af-normal</strong>.  &lt;br&gt;5. Click <strong>OK</strong>.  &lt;br&gt;6. Click <strong>Add new entry</strong> next to Drop profile map.  &lt;br&gt;7. From the Loss priority box, select <strong>High</strong>.  &lt;br&gt;8. From the Protocol box, select <strong>Any</strong>.  &lt;br&gt;9. In the Drop profile box, type the name of the drop profile—for example, <strong>af-with-PLP</strong>.  &lt;br&gt;10. Click <strong>OK</strong> twice.</td>
<td>Enter  &lt;br&gt;set drop-profile-map loss-priority low protocol any drop-profile af-normal  &lt;br&gt;set drop-profile-map loss-priority high protocol any drop-profile af-with-PLP</td>
</tr>
</tbody>
</table>
Table 212: Configuring Schedulers (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a network control scheduler.</td>
<td>1. Click Add new entry next to Schedulers.</td>
<td>From the [edit class of service] hierarchy level, enter edit schedulers nc-scheduler.</td>
</tr>
<tr>
<td></td>
<td>2. In the Scheduler name box, type the name of the network control scheduler—for example, nc-scheduler.</td>
<td></td>
</tr>
<tr>
<td>Configure a network control scheduler priority and buffer size.</td>
<td>1. In the Priority box, type low.</td>
<td>Enter set priority low</td>
</tr>
<tr>
<td></td>
<td>2. Click Configure next to Buffer size.</td>
<td>set buffer-size percent 5</td>
</tr>
<tr>
<td></td>
<td>3. From the Buffer size choice list, select the basis for the buffer allocation method—for example, Percent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. In the Percent box, type the percentage of the buffer to be used by the network control scheduler—for example, 5.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Click OK.</td>
<td></td>
</tr>
<tr>
<td>Configure a network control scheduler transmit rate.</td>
<td>1. Click Configure next to Transmit rate.</td>
<td>Enter set transmit-rate percent 5</td>
</tr>
<tr>
<td></td>
<td>2. From the Transmit rate choice list, select the basis for the transmit rate method—for example, Percent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. In the Percent box, type the percentage of the bandwidth to be used by the network control scheduler—for example, 5.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Click OK.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring and Applying Scheduler Maps

You configure a scheduler map to assign a forwarding class to a scheduler, then apply the scheduler map to any interface that must enforce DiffServ CoS.

The following example shows how to create the scheduler map diffserv-cos-map and apply it to the device’s Ethernet interface ge-0/0/0. The map associates the mf-classifier forwarding classes configured in “Configuring and Applying a Firewall Filter for a Multifield Classifier” on page 835 to the schedulers configured in “Configuring Schedulers” on page 857, as shown in Table 213 on page 860.

Table 213: Sample diffserv-cos-map Scheduler Mapping

<table>
<thead>
<tr>
<th>mf-classifier Forwarding Class</th>
<th>For CoS Traffic Type</th>
<th>diffserv-cos-map Scheduler</th>
</tr>
</thead>
<tbody>
<tr>
<td>be-class</td>
<td>Best-effort traffic</td>
<td>be-scheduler</td>
</tr>
<tr>
<td>ef-class</td>
<td>Expedited forwarding traffic</td>
<td>ef-scheduler</td>
</tr>
<tr>
<td>af-class</td>
<td>Assured forwarding traffic</td>
<td>af-scheduler</td>
</tr>
<tr>
<td>nc-class</td>
<td>Network control traffic</td>
<td>nc-scheduler</td>
</tr>
</tbody>
</table>
To configure and apply scheduler maps:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 214 on page 861.
3. If you are finished configuring the device, commit the configuration.
4. Go on to one of the following tasks:
   - To apply rules to logical interfaces, see “Configuring and Applying Virtual Channels” on page 864.
   - To use adaptive shapers to limit bandwidth for Frame Relay, see “Configuring Adaptive Shaping for Frame Relay” on page 875.
   - To check the configuration, see “Verifying a CoS Configuration” on page 941.

### Table 214: Configuring Scheduler Maps

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Class of service level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI. 2. Next to Class of service, click Configure or Edit.</td>
<td>From the [edit] hierarchy level, enter edit class-of-service.</td>
</tr>
<tr>
<td>Configure a scheduler map for DiffServ CoS.</td>
<td>1. Click Add new entry next to Scheduler maps. 2. In the Map name box, type the name of the scheduler map—for example, diffserv-cos-map.</td>
<td>Enter edit scheduler-maps diffserv-cos-map.</td>
</tr>
<tr>
<td>Configure a best-effort forwarding class and scheduler.</td>
<td>1. Click Add new entry next to Forwarding class. 2. In the Class name box, type the name of the previously configured best-effort forwarding class—be-class. 3. In the Scheduler box, type the name of the previously configured best-effort scheduler—be-scheduler. 4. Click OK.</td>
<td>Enter set forwarding-class be-class scheduler be-scheduler.</td>
</tr>
</tbody>
</table>
**Table 214: Configuring Scheduler Maps (continued)**

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure an expedited forwarding class</td>
<td>1. Click <strong>Add new entry</strong> next to Forwarding class.</td>
<td>Enter</td>
</tr>
<tr>
<td>and scheduler.</td>
<td>2. In the Class name box, type the name of the previously configured expedited forwarding</td>
<td>set forwarding-class ef-class scheduler</td>
</tr>
<tr>
<td></td>
<td>class—<em>ef-class</em>.</td>
<td>ef-scheduler</td>
</tr>
<tr>
<td></td>
<td>3. In the Scheduler box, type the name of the previously configured expedited forwarding</td>
<td></td>
</tr>
<tr>
<td></td>
<td>scheduler—<em>ef-scheduler</em>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td>Configure an assured forwarding class</td>
<td>1. Click <strong>Add new entry</strong> next to Forwarding class.</td>
<td>Enter</td>
</tr>
<tr>
<td>and scheduler.</td>
<td>2. In the Class name box, type the name of the previously configured assured forwarding class—<em>af-class</em>.</td>
<td>set forwarding-class af-class scheduler</td>
</tr>
<tr>
<td></td>
<td>3. In the Scheduler box, type the name of the previously configured assured forwarding</td>
<td>af-scheduler</td>
</tr>
<tr>
<td></td>
<td>scheduler—<em>af-scheduler</em>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td>Configure a network control class and</td>
<td>1. Click <strong>Add new entry</strong> next to Forwarding class.</td>
<td>Enter</td>
</tr>
<tr>
<td>scheduler.</td>
<td>2. In the Class name box, type the name of the previously configured network control class—<em>nc-class</em>.</td>
<td>set forwarding-class nc-class scheduler</td>
</tr>
<tr>
<td></td>
<td>3. In the Scheduler box, type the name of the previously configured network control scheduler—<em>nc-scheduler</em>.</td>
<td>nc-scheduler</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>OK</strong> twice.</td>
<td></td>
</tr>
<tr>
<td>Apply the scheduler map to an interface.</td>
<td>1. Click <strong>Add new entry</strong> next to Interfaces.</td>
<td>From the [edit class of service] hierarchy level, enter</td>
</tr>
<tr>
<td>(See the interface naming conventions in</td>
<td>2. In the Interface name box, type the name of the interface—for example, <em>ge-0/0/0</em>.</td>
<td>set interfaces <em>ge-0/0/0</em> scheduler-map</td>
</tr>
<tr>
<td>JUNOS OS Interfaces Configuration Guide</td>
<td>3. Click <strong>Add new entry</strong> next to Unit.</td>
<td></td>
</tr>
<tr>
<td>for Security Devices.)</td>
<td>4. In the Unit number box, type the logical interface unit number—<em>0</em>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. In the Scheduler map box, type the name of the previously configured scheduler map—<em>diffserv-cos-map</em>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Click <strong>OK</strong>.</td>
<td></td>
</tr>
</tbody>
</table>
Scheduler Maps: Sample Configuration

Once you define a scheduler, you can include it in a scheduler map, which maps a specified forwarding class to a scheduler configuration. To do this, include the scheduler-maps statement at the [edit class-of-service] hierarchy level:

```
[edit class-of-service]
scheduler-maps {
  map-name {
    forwarding-class class-name scheduler scheduler-name;
  }
}
```

After you have defined the scheduler map, you can associate it with an output interface. To do this, include the scheduler-map statement at the [edit class-of-service interfaces interface-name] hierarchy level:

```
[edit class-of-service interfaces interface-name]
scheduler-map map-name;
```

Interface wildcards are supported.

Schedulers: Sample Configuration

You use schedulers to define the properties of output queues. These properties include the amount of interface bandwidth assigned to the queue, the size of the memory buffer allocated for storing packets, the priority of the queue, and the random early detection (RED) drop profiles associated with the queue.

You associate the schedulers with forwarding classes by means of scheduler maps. You can then associate each scheduler map with an interface, thereby configuring the hardware queues, packet schedulers, and RED processes that operate according to this mapping.

To configure class-of-service (CoS) schedulers, use the following sample configuration at the [edit class-of-service] hierarchy level:

```
[edit class-of-service]
interfaces {
  interface-name {
    scheduler-map map-name;
    scheduler-map-chassis map-name;
    schedulers number;
    shaping-rate rate;
    unit {
      output-traffic-control-profile profile-name;
      scheduler-map map-name;
      shaping-rate rate;
    }
  }
}
fabric {
  scheduler-map {
```
priority (high | low) scheduler scheduler-name;
}
}
scheduler-maps {
  map-name {
    forwarding-class class-name scheduler scheduler-name;
  }
}
schedulers {
  scheduler-name {
    buffer-size (percent percentage | remainder | temporal microseconds);
    drop-profile-map loss-priority (any | low | medium-low | medium-high | high) protocol
      (any | non-tcp | tcp) drop-profile profile-name;
    priority priority-level;
    transmit-rate (rate | percent percentage remainder) <exact | rate-limit>;
  }
}
traffic-control-profiles profile-name {
  delay-buffer-rate (percent percentage | rate);
  guaranteed-rate (percent percentage | rate);
  scheduler-map map-name;
  shaping-rate (percent percentage | rate);
}

NOTE: For J Series devices and SRX210, SRX240, and SRX650 devices, when configuring the “protocol parameter” in the drop-profile-map statement, tcp and non-tcp values are not supported, only the value “any” is supported.

Configuring and Applying Virtual Channels

You configure a virtual channel to set up queuing, packet scheduling, and accounting rules to be applied to one or more logical interfaces. You then must apply the virtual channel to a particular logical interface. Virtual channels can be applied in different ways. For more information on virtual channels, see “Configuring Virtual Channels” on page 869. In the example here, an output firewall filter is used for directing traffic to a particular virtual channel.

The following example shows how to create the virtual channels branch1-vc, branch2-vc, and branch3-vc and apply them in the firewall filter choose-vc to the Services Router’s T3 interface t3-1/0/0.

To configure and apply virtual channels for the Services Router:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 215 on page 865.
3. If you are finished configuring the router, commit the configuration.
4. Go on to one of the following tasks:
   - To assign resources, priorities, and profiles to output queues, see “Configuring Schedulers” on page 857.
To use adaptive shapers to limit bandwidth for Frame Relay, see “Configuring Adaptive Shaping for Frame Relay” on page 875.

To check the configuration, see “Verifying a CoS Configuration” on page 941.

Table 215: Configuring and Applying Virtual Channels

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Navigate to the **Class of service** level in the configuration hierarchy. | 1. In the J-Web interface, select Configure > CLI Tools > Point and Click CLI.  
2. Next to Class of service, click Configure or Edit. | From the [edit] hierarchy level, enter edit class-of-service |
| Define the virtual channels **branch1–vc**, **branch2–vc**, **branch3–vc**, and the default virtual channel. You must specify a default virtual channel. | 1. Click **Add new entry** next to Virtual channels.  
2. In the Channel name box, type the name of the virtual channel—for example, **branch1–vc**.  
3. Click **OK**.  
2. Repeat this statement for **branch2–vc**, **branch3–vc**, and **default-vc**. |
| Define the virtual channel group **wan-vc-group** to include the four virtual channels, and assign each virtual channel the scheduler map **bestscheduler**. | 1. Click **Add new entry** next to Virtual channel groups.  
2. In the Group name box, type the name of the virtual channel group—**wan-vc-group**.  
3. Click **Add new entry** next to Channel.  
4. In the Channel name box, type the name of the previously configured virtual channels—**branch1–vc**.  
5. In the Scheduler map box, type the name of the previously configured scheduler map—**bestscheduler**.  
6. Click **OK**.  
7. Add the virtual channels **branch2–vc**, **branch3–vc**, and **default-vc**. Select the **Default** box when adding the virtual channel **default-vc**. | 1. Enter set virtual-channel-groups wan-vc-group branch1–vc  
2. Repeat this statement for **branch2–vc**, **branch3–vc**, and **default-vc**.  
3. Enter set virtual-channel-groups wan-vc-group default-vc default |
Table 215: Configuring and Applying Virtual Channels (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Specifying a shaping rate of 2 Mbps for each virtual channel within the virtual channel group. | 1. Click branch1–vc in the list of virtual channels.  
2. Select the Shaping rate box.  
3. Click Configure.  
4. Select Absolute rate from the Rate choice box.  
5. In the Absolute rate box, type the shaping rate—2m.  
6. Add the shaping rate for the branch2–vc and branch3–vc virtual channels.  
7. Click OK three times. | 1. Enter set virtual-channel-groups wan-vc-group branch1–vc shaping-rate 2m  
2. Repeat this statement for branch2–vc and branch3–vc. |

Apply the virtual channel group to the logical interface t3–1/0/0. (See the interface naming conventions in Junos OS Interfaces Configuration Guide for Security Devices.) | 1. Click Add new entry next to Interfaces.  
2. In the Interface name box, type the name of the interface—t3–1/0/0.  
3. Click Add new entry next to Unit.  
4. In the Unit number box, type the logical interface unit number—0.  
5. In the Virtual channel group box, type the name of the previously configured virtual channel group—wan-vc-group.  
6. Click OK. | From the [edit class of service] hierarchy level, enter  
set interfaces t3–1/0/0 unit 0 virtual-channel-group wan-vc-group |
### Table 215: Configuring and Applying Virtual Channels (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Create the firewall filter `choose-vc` to select the traffic that is transmitted on a particular virtual channel. | 1. On the main Configuration page next to Firewall, click **Configure** or **Edit**.  
2. Click **Add new entry** next to Filter.  
3. In the Filter name box, type the name of the firewall filter—`choose-vc`.  
4. Click **Add new entry** next to Term.  
5. In the Rule name box, type the name of the firewall term—`branch1`.  
6. Click **Configure** next to From.  
7. Click **Add new entry** next to Destination address.  
8. In the Address box, type the IP address of the destination host—`192.168.10.0/24`.  
9. Click **OK** twice.  
10. On the firewall term page, click **Configure** next to Then.  
11. Select **Accept** from the Designation box.  
12. In the Virtual channel box, type the name of the previously configured virtual channel—`branch1-vc`.  
13. Click **OK**.  
14. Repeat these steps for the virtual channels `branch2-vc` and `branch3-vc`. | 1. From the [edit] hierarchy level, enter `edit firewall`  
2. Enter  
   `set family inet filter choose-vc term branch1 from destination 192.168.10.0/24`  
3. Enter  
   `set family inet filter choose-vc term branch1 then accept`  
4. Enter  
   `set family inet filter choose-vc term branch1 then virtual-channel branch1-vc`  
5. Repeat these steps for virtual channels `branch2-vc` and `branch3-vc`. |
| Apply the firewall filter `choose-vc` to output traffic on the t3-1/0/0.0 interface. | 1. On the main Configuration page next to Interfaces, click **Configure** or **Edit**.  
2. Click `t3-1/0/0` in the list of configured interfaces.  
3. Click `0` in the list of configured logical units for the interface.  
4. Click **Edit** next to Inet.  
5. Click **Configure** next to Filter.  
6. In the Output box, type the name of the previously configured firewall filter—`choose-vc`.  
7. Click **OK**. | 1. From the [edit] hierarchy level, enter `edit interfaces`  
2. Enter  
   `set t3-1/0/0 unit 0 family inet filter output choose-vc` |
Configuring and Applying an Adaptive Shaper

You can use adaptive shaping to limit the bandwidth of traffic flowing on a Frame Relay logical interface. If you configure and apply adaptive shaping, the device checks the backward explicit congestion notification (BECN) bit within the last inbound (ingress) packet received on the interface. For more information on adaptive shaping, see “Configuring Adaptive Shaping for Frame Relay” on page 875.

**NOTE:** Adaptive shaping is not available on SRX3400, SRX3600, SRX5600, and SRX5800 devices.

The following example shows how to create an adaptive shaper `fr-shaper` and apply it to the device's T1 interface `t1-0/0/2`. The adapter shaper limits the transmit bandwidth on the interface to 64 Kbps.

To configure and apply an adaptive shaper for the device:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 216 on page 868.
3. If you are finished configuring the device, commit the configuration.
4. Go on to one of the following tasks:
   - To assign resources, priorities, and profiles to output queues, see “Configuring Schedulers” on page 857.
   - To apply rules to logical interfaces, see “Configuring and Applying Virtual Channels” on page 864.
   - To check the configuration, see “Verifying a CoS Configuration” on page 941.

### Table 216: Configuring and Applying an Adaptive Shaper

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Class of service</strong> level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit class-of-service</td>
</tr>
<tr>
<td></td>
<td>2. Next to Class of service, click Configure or Edit.</td>
<td></td>
</tr>
</tbody>
</table>
**Table 216: Configuring and Applying an Adaptive Shaper (continued)**

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the adaptive shaper name and maximum transmit rate.</td>
<td>1. Next to Adaptive Shapers, click Add new entry.</td>
<td>Enter set adaptive-shapers fr-shaper trigger becn shaping-rate 64k</td>
</tr>
<tr>
<td></td>
<td>2. In the Adaptive shaper name box, type fr-shaper.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Next to Trigger, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Next to Becn, select the check box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Next to Shaping rate, select the check box and click Configure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. From the Rate choice list, select Absolute rate.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. In the Absolute rate box, type 64k.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. Click OK three times.</td>
<td></td>
</tr>
<tr>
<td>Apply the adaptive shaper to the logical interface t1-0/0/2.0</td>
<td>1. Next to Interfaces, click Add new entry.</td>
<td>Enter set interfaces t1-0/0/2.0 unit 0 adaptive-shaper fr-shaper</td>
</tr>
<tr>
<td>(See the interface naming conventions in Junos OS Interfaces Configuration Guide for Security Devices.)</td>
<td>2. In the Interface name box, type the name of the interface—t1-0/0/2.0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Next to Unit, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. In the Unit number box, type the logical interface unit number—0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. In the Adaptive shaper box, type the name of the adaptive shaper—fr-shaper.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Click OK.</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring Virtual Channels**

For J Series devices and SRX210, SRX240, and SRX650 devices, you can configure virtual channels, which allow you to limit traffic sent from a corporate headquarters to branch offices. Virtual channels might be required when the headquarters site has an expected aggregate bandwidth higher than that of the individual branch offices. The router at the headquarters site must limit the traffic sent to each of the branch office routers to avoid oversubscribing their links. For instance, if branch 1 has a 1.5-megabits per second (Mbps) link and the headquarters router attempts to send 6 Mbps to branch 1, all of the traffic in excess of 1.5 Mbps is dropped in the ISP network.

For information about which devices support the features documented in this chapter, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.
This chapter discusses the following topics:
- Configuring CoS Virtual Channels on page 870
- Creating a List of Virtual Channel Names on page 871
- Defining a Virtual Channel Group on page 871
- Applying a Virtual Channel Group to a Logical Interface on page 872
- Selecting Traffic to Be Transmitted from a Particular Virtual Channel on page 873
- Example: Configuring Virtual Channels on page 873

**Configuring CoS Virtual Channels**

To limit the traffic the headquarters router sends to each branch, you can configure virtual channels on a logical interface. Each virtual channel has a set of eight queues with a scheduler and an optional shaper. You can use an output firewall filter to direct traffic to a particular virtual channel. For example, a filter can direct all traffic with a destination address for branch office 1 to virtual channel 1, and all traffic with a destination address for branch office 2 to virtual channel 2.

When you configure virtual channels on an interface, the virtual channel group uses the same scheduler and shaper you configure at the [edit interfaces interface-name unit logical-unit-number] hierarchy level. In this way, virtual channels are an extension of regular scheduling and shaping and not an independent entity.

Although a virtual channel group is assigned to a logical interface, a virtual channel is not the same as a logical interface. The only features supported on a virtual channel are queuing, packet scheduling, and accounting. Rewrite rules and routing protocols apply to the entire logical interface.

To configure virtual channels, you can include the following statements at the [edit class-of-service], [edit firewall], and [edit interfaces] hierarchy levels of the configuration:

```plaintext
[edit class-of-service]
virtual-channels {
    virtual-channel-name;
}
virtual-channel-groups {
    virtual-channel-group-name {
        virtual-channel-name {
            scheduler-map map-name;
            shaping-rate (percent percentage | rate);
            default;
        }
    }
}

interfaces {
    interface-name {
        unit logical-unit-number {
            virtual-channel-group virtual-channel-group-name;
        }
    }
}
```


```c
[edit firewall]
family family-name {
    filter filter-name {
        term term-name {
            then {
                virtual-channel virtual-channel-name;
            }
        }
    }
}

[edit interfaces]
interface-name {
    per-unit-scheduler;
}
```

**Creating a List of Virtual Channel Names**

To create a list of virtual channels that you can assign to a virtual channel group, include the `virtual-channels` statement at the `[edit class-of-service]` hierarchy level:

```c
[edit class-of-service]
virtual-channels {
    virtual-channel-name;
}
```

**Defining a Virtual Channel Group**

To define a virtual channel group that you can assign to a logical interface, include the `virtual-channel-groups` statement at the `[edit class-of-service]` hierarchy level:

```c
[edit class-of-service]
virtual-channel-groups {
    virtual-channel-group-name {
        virtual-channel-name {
            scheduler-map map-name;
            shaping-rate (percent percentage | rate);
            default ;
        }
    }
}
```

`virtual-channel-group-name` can be any name that you want. `virtual-channel-name` must be one of the names that you define at the `[edit class-of-service virtual-channels]` hierarchy level. You can include multiple virtual channel names in a group.

`map-name` must be one of the scheduler maps that you configure at the `[edit class-of-service scheduler-maps]` hierarchy level. For more information, see “Configuring Schedulers” on page 857.

The scheduler map is required. `map-name` must be one of the scheduler maps that you configure at the `[edit class-of-service scheduler-maps]` hierarchy level. For more information, see “Configuring Schedulers” on page 857.

The shaping rate is optional. If you configure the shaping rate as a percentage, when the virtual channel is applied to a logical interface, the shaping rate is set to the specified percentage of the interface bandwidth. If you configure a shaper on a virtual
channel, the shaper limits the maximum bandwidth transmitted by that virtual channel. Virtual channels without a shaper can use the full logical interface bandwidth. If there are multiple unshaped virtual channels, they share the available logical interface bandwidth equally.

When you apply the virtual channel group to a logical interface, a set of eight queues is created for each of the virtual channels in the group. The scheduler-map statement applies a scheduler to these queues. If you include the shaping-rate statement, a shaper is applied to the entire virtual channel.

You must configure one of the virtual channels in the group to be the default channel. Therefore, the default statement is required in the configuration of one virtual channel per channel group. Any traffic not explicitly directed to a particular channel is transmitted by this default virtual channel.

**Applying a Virtual Channel Group to a Logical Interface**

To apply a virtual channel group to a logical interface, include the virtual-channel-group statement at the [edit class-of-service interfaces interface-name unit logical-unit-number] hierarchy level:

```
[edit class-of-service interfaces interface-name unit logical-unit-number]
virtual-channel-group virtual-channel-group-name;
```

For the corresponding physical interface, you must also include the per-unit-scheduler statement at the [edit interfaces interface-name] hierarchy level:

```
[edit interfaces interface-name]
per-unit-scheduler;
```

The per-unit-scheduler statement enables one set of output queues for each logical interface configured under the physical interface.

When you apply a virtual channel group to a logical interface, the software creates a set of eight queues for each of the virtual channels in the group.

If you apply a virtual channel group to multiple logical interfaces, the software creates a set of eight queues on each logical interface. The virtual channel names listed in the group are used on all the logical interfaces. We recommend specifying the scheduler and shaping rates in the virtual channel configuration in terms of percentages, rather than absolute rates. This allows you to apply the same virtual channel group to logical interfaces that have different bandwidths.

When you apply a virtual channel group to a logical interface, you cannot include the scheduler-map and shaping-rate statements at the [edit class-of-service interfaces interface-name unit logical-unit-number] hierarchy level. In other words, you can configure a scheduler map and a shaping rate on a logical interface, or you can configure virtual channels on the logical interface, but not both.

If you configure multiple logical interfaces on a single physical interface, each logical interface is guaranteed an equal fraction of the physical interface bandwidth:

```
logical-interface-bandwidth = physical-interface-bandwidth / number-of-logical-interfaces
```
If one or more logical interfaces do not completely use their allocation, the other logical interfaces share the excess bandwidth equally.

If you configure multiple virtual channels on a logical interface, they are each guaranteed an equal fraction of the logical interface bandwidth:

\[
\text{virtual-channel-bandwidth} = \frac{\text{logical-interface-bandwidth}}{\text{number-of-virtual-channels}}
\]

If you configure a shaper on a virtual channel, the shaper limits the maximum bandwidth transmitted by that virtual channel. Virtual channels without a shaper can use the full logical interface bandwidth. If there are multiple unshaped virtual channels, they share the available logical interface bandwidth equally.

**Selecting Traffic to Be Transmitted from a Particular Virtual Channel**

To select the traffic to be transmitted by a particular virtual channel, include the `virtual-channel` statement at the `[edit firewall family family-name filter filter-name term term-name then]` hierarchy level:

```
[edit firewall family family-name filter filter-name term term-name then]
virtual-channel virtual-channel-name;
```

The `virtual-channel` statement is a firewall action modifier. For more information about firewall action modifiers, see the *Junos Policy Framework Configuration Guide*.

**Example: Configuring Virtual Channels**

This configuration creates four virtual channels on the interface t3-1/0/0.0. Three of them (branch1-vc, branch2-vc, and branch3-vc) are shaped to 1.5 Mbps. The fourth virtual channel is the default (default-vc), and it is not shaped, so it can use the full interface bandwidth. The output filter on the interface sends all traffic with a destination address matching 192.168.10.0/24 to branch1-vc, and similar configurations are set for branch2-vc and branch3-vc. Traffic not matching any of the addresses goes to the default, unshaped virtual channel.

```
class-of-service {
  interfaces {
    t3-1/0/0 {
      unit 0 {
        virtual-channel-group wan-vc-group;
      }
    }
  }
}

virtual-channels {
  branch1-vc;
  branch2-vc;
  branch3-vc;
  default-vc;
}

virtual-channel-groups {
  wan-vc-group {
    branch1-vc {
      scheduler-map interface-global;
    }
  }
}
```

Chapter 33: Configuring Class of Service
shaping-rate 1.5m;
}
branch2-vc {
    scheduler-map interface-global;
    shaping-rate 1.5m;
}
branch3-vc {
    scheduler-map interface-global;
    shaping-rate 1.5m;
}
default-vc {
    scheduler-map interface-global;
    default;
}
}
}
}
}
firewall {
    family inet {
        filter choose-vc {
            term branch1 {
                from {
                    destination 192.168.10.0/24;
                }
                then {
                    accept;
                    virtual-channel branch1-vc;
                }
            }
            term branch2 {
                from {
                    destination 192.168.11.0/24;
                }
                then {
                    accept;
                    virtual-channel branch2-vc;
                }
            }
            term branch3 {
                from {
                    destination 192.168.12.0/24;
                }
                then {
                    accept;
                    virtual-channel branch3-vc;
                }
            }
            term default {
                then {
                    accept;
                }
            }
        }
    }
}
Configuring Adaptive Shaping for Frame Relay

For J Series devices and SRX210, SRX240, and SRX650 devices, you can configure adaptive shapers, which allow you to shape Frame Relay logical interfaces to a maximum rate, based on congestion. Adaptive shaping is triggered by the backward explicit congestion notification (BECN) bit in Frame Relay packet headers. Thus, adaptive shaping allows you to use the information provided in Frame Relay packet headers to detect possible congestion and to adjust your bandwidth limitation accordingly.

Adaptive shaping is triggered when the last ingress packet on the logical interface has its BECN bit set to 1. When adaptive shaping is triggered, the output queues on the logical interface are shaped according to the adaptive shaper configuration.

Adaptive shaping is an alternative to regular logical interface shaping. If the last ingress packet has its BECN bit set to 0, the logical interface queues are shaped according to the shaping-rate statement at the [edit class-of-service interfaces interface-name unit logical-unit-number] hierarchy level, which should be configured at a higher rate than the rate you configure for the adaptive shaper. If you do not include the shaping-rate statement in the configuration, the default logical interface bandwidth is the average of unused bandwidth for the number of logical interfaces that require default bandwidth treatment. For more information about shaping rates and bandwidth sharing, see “Configuring Excess Bandwidth Sharing” on page 937.

To configure an adaptive shaper, you can include the following statements at the [edit class-of-service] hierarchy level of the configuration:

```plaintext
[edit class-of-service]
adaptive-shapers {
    adaptive-shaper-name {
        trigger type shaping-rate (percent percentage | rate);
    }
}

interfaces {
    interface-name {
        unit logical-unit-number {
            adaptive-shaper adaptive-shaper-name;
        }
    }
}
```

Configuring Adaptive Shaping for Frame Relay
NOTE: For more information on configuring and applying an adaptive shaper using the configuration editor, see “Configuring and Applying an Adaptive Shaper” on page 868.

Configuring an Adaptive Shaper

To configure an adaptive shaper, include the adaptive-shapers statement at the [edit class-of-service] hierarchy level:

```
[edit class-of-service]
adaptive-shapers {  
adaptive-shaper-name {  
    trigger type shaping-rate (percent percentage | rate);  
  }
}
```

The trigger type can be becn only. If the last ingress packet on the logical interface has its BECN bit set to 1, the output queues on the logical interface are shaped according to the associated shaping rate.

The associated shaping rate can be a percentage of the available interface bandwidth from 0 through 100 percent. Alternatively, you can configure the shaping rate to be an absolute peak rate, in bits per second (bps) from 3200 through 32,000,000,000 bps. You can specify the value either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).

Applying an Adaptive Shaper to a Logical Interface

To apply an adaptive shaper to a logical interface, include the adaptive-shaper statement at the [edit class-of-service interfaces interface-name unit logical-unit-number] hierarchy level:

```
[edit class-of-service interfaces interface-name unit logical-unit-number]
adaptive-shaper adaptive-shaper-name;
```

Classifying Frame Relay Traffic

For J Series and SRX210, SRX240, and SRX650 device interfaces with Frame Relay encapsulation, you can set the loss priority of Frame Relay traffic, based on the discard eligibility (DE) bit. For each incoming frame with the DE bit containing the CoS value 0 or 1, you can configure a Frame Relay loss priority value of low, medium-low, medium-high, or high.

You can apply a classifier to the same interface on which you configure a Frame Relay loss priority value. The Frame Relay loss priority map is applied first, followed by the classifier. The classifier can change the loss priority to a higher value only (for example, from low to high). If the classifier specifies a loss priority with a lower value than the current loss priority of a particular packet, the classifier does not change the loss priority of that packet.
This section is organized as follows:

- Assigning the Default Frame Relay Loss Priority Map to an Interface on page 877
- Defining a Custom Frame Relay Loss Priority Map on page 877
- Verifying Your Configuration on page 878

**Assigning the Default Frame Relay Loss Priority Map to an Interface**

The default Frame Relay loss priority map contains the following settings:

```
loss-priority low code-point 0;
loss-priority high code-point 1;
```

This default map sets the loss priority to 
**low** for each incoming frame with the DE bit containing the 0 CoS value. The map sets the loss priority to **high** for each incoming frame with the DE bit containing the 1 CoS value.

To assign the default map to an interface, include the `frame-relay-de default` statement at the `[edit class-of-service interfaces interface-name unit logical-unit-number loss-priority-maps]` hierarchy level:

```
[edit class-of-service interfaces interface-name unit logical-unit-number loss-priority-maps]
frame-relay-de default;
```

**Defining a Custom Frame Relay Loss Priority Map**

To define a custom Frame Relay loss priority map, include the following statements at the `[edit class-of-service]` hierarchy level:

```
[edit class-of-service]
loss-priority-maps {
  frame-relay-de map-name {
    loss-priority (low | medium-low | medium-high | high) code-point (0 | 1);
  }
}
```

A custom loss priority map sets the loss priority to **low**, **medium-low**, **medium-high**, or **high** for each incoming frame with the DE bit containing the specified 0 or 1 CoS value.

**Applying the Map to a Logical Interface**

The map does not take effect until you apply it to a logical interface. To apply a map to a logical interface, include the `frame-relay-de map-name` statement at the `[edit class-of-service interfaces interface-name unit logical-unit-number loss-priority-maps]` hierarchy level:

```
[edit class-of-service interfaces interface-name unit logical-unit-number loss-priority-maps]
frame-relay-de map-name;
```
Verifying Your Configuration

To verify your configuration, you can issue the following operational mode commands:

- show class-of-service forwarding-table loss-priority-map
- show class-of-service forwarding-table loss-priority-map mapping
- show chassis forwarding
- show pfe fwdd

NOTE: On J Series devices, show commands might still display a loss-priority-map as applied to an interface even if the commit configuring it fails.

Rewriting Frame Relay Headers

For J Series device interfaces with Frame Relay encapsulation, you can rewrite the discard eligibility (DE) bit based on the loss priority of Frame Relay traffic. For each outgoing frame with the loss priority set to low, medium-low, medium-high, or high, you can set the DE bit CoS value to 0 or 1.

You can combine a Frame Relay rewrite rule with other rewrite rules on the same interface. For example, you can rewrite both the DE bit and MPLS EXP bit.

This section is organized as follows:

- Assigning the Default Frame Relay Rewrite Rule to an Interface on page 878
- Defining a Custom Frame Relay Rewrite Rule on page 879

Assigning the Default Frame Relay Rewrite Rule to an Interface

The default Frame Relay rewrite rule contains the following settings:

loss-priority low code-point 0;
loss-priority medium-low code-point 0;
loss-priority medium-high code-point 1;
loss-priority high code-point 1;

This default rule sets the DE CoS value to 0 for each outgoing frame with the loss priority set to low or medium-low. This default rule sets the DE CoS value to 1 for each outgoing frame with the loss priority set to medium-high or high.

To assign the default rule to an interface, include the frame-relay-de default statement at the [edit class-of-service interfaces interface interface-name unit logical-unit-number rewrite-rules] hierarchy level:

[edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules]
frame-relay-de default;
Defining a Custom Frame Relay Rewrite Rule

To define a custom Frame Relay rewrite rule, include the following statements at the [edit class-of-service] hierarchy level:

```
[edit class-of-service]
rewrite-rules {
    frame-relay-de rewrite-name {
        import (rewrite-name | default);
        forwarding-class class-name {
            loss-priority level code-point (0 | 1);
        }
    }
}
```

A custom rewrite rule sets the DE bit to the 0 or 1 CoS value based on the assigned loss priority of low, medium-low, medium-high, or high for each outgoing frame.

Applying the Rule to a Logical Interface

The rule does not take effect until you apply it to a logical interface. To apply a rule to a logical interface, include the `frame-relay-de map-name` statement at the [edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules] hierarchy level:

```
[edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules]
frame-relay-de map-name;
```

Configuring Strict-High Priority

NOTE: This section is applicable to only J Series device and SRX210, SRX240, and SRX650 devices.

You can configure one queue per interface to have strict high priority, which causes delay-sensitive traffic, such as voice traffic, to be removed and forwarded with minimum delay. Packets that are queued in a strict-priority queue are removed before packets in other queues, including high-priority queues.

The strict high-priority queuing feature allows you to configure traffic policing that prevents lower-priority queues from being starved. The strict-priority queue does not cause starvation of other queues because the configured policer allows the queue to exceed the configured bandwidth only when other queues are not congested. If the interface is congested, the software polices strict-priority queues to the configured bandwidth.

To prevent queue starvation of other queues, you must configure an output (egress) policer that defines a limit for the amount of traffic that the queue can service. The
software services all traffic in the strict-priority queue that is under the defined limit. When strict-priority traffic exceeds the limit, the policer marks the traffic in excess of the limit as out-of-profile. If the output port is congested, the software drops out-of-profile traffic.

You can also configure a second policer with an upper limit. When strict-priority traffic exceeds the upper limit, the software drops the traffic in excess of the upper limit, regardless of whether the output port is congested. This upper-limit policer is not a requirement for preventing starvation of the lower-priority queues. The policer for the lower limit, which marks the packets as out-of-profile, is sufficient to prevent starvation of other queues.

The following steps describe how strict priority queuing and policing works:

1. Identify delay-sensitive traffic by configuring a behavior aggregate (BA) or multifield (MF) classifier.
2. Minimize delay by assigning all delay-sensitive packets to the strict priority queue.
3. Prevent starvation on other queues by configuring a policer that checks the data stream entering the strict priority queue. The policer defines a lower bound, marks the packets that exceed the lower bound as out-of-profile, and drops the out-of-profile packets if the physical interface is congested. If there is no congestion, the software forwards all packets, including the out-of-profile packets.
4. Optionally, configure another policer that defines an upper bound and drops the packets that exceed the upper bound, regardless of congestion on the physical interface.

To configure strict priority queuing and prevent starvation of other queues, include the priority strict-high statement at the [edit class-of-service schedulers scheduler-name] hierarchy level and the if exceeding and then out-of-profile statements at the [edit firewall policer policer-name] hierarchy level:

[edit class-of-service schedulers scheduler-name]
priority strict-high;

[edit firewall policer policer-name]
if exceeding {
    bandwidth-limit bps;
    bandwidth-percent number;
    burst-size-limit bytes;
} then out-of-profile;

To verify your configuration, you can issue the following operational mode commands:

- show class-of-service scheduler-map map-name
- show interfaces interface-name extensive
- show interfaces queue interface-name


**Example: Configuring Strict High Priority Using the CLI**

Use a BA classifier to classify traffic based on the IP precedence of the packet. The classifier defines IP precedence value `101` as voice traffic and `000` as data traffic.

Configure two policers on the output interface that identify excess voice traffic belonging to the `voice-class` forwarding class. If the traffic exceeds 1 Mbps, a policer marks the traffic in excess of 1 Mbps as out-of-profile. If the traffic exceeds 2 Mbps, the second policer discards the traffic in excess of 2 Mbps.

```plaintext
Configure a BA Classifier
class-of-service {
    classifiers {
        inet-precedence corp-traffic {
            forwarding-class voice-class {
                loss-priority low code-points 101;
            }
            forwarding-class data-class {
                loss-priority high code-points 000;
            }
        }
    }
}

Configure the Forwarding Classes
forwarding-classes {
    queue 0 voice-class;
    queue 1 data-class;
}

Configure the Scheduler Map
scheduler-maps {
    corp-map {
        forwarding-class voice-class scheduler voice-sched;
        forwarding-class data-class scheduler data-sched;
    }
}

Configure the Schedulers
schedulers {
    voice-sched {
        priority strict-high;
    }
    data-sched {
        priority low;
    }
}

Apply the BA Classifier to an Input Interface
interfaces {
    fe-0/0/0 {
        unit 0 {
            classifiers {
                inet-precedence corp-traffic;
            }
        }
    }
}
```
Apply the Scheduler Map to an Output Interface

```
e1-1/0/1 {
    scheduler-map corp-map;
}
```

Configure Two Policers

```
firewall {
    policer voice-excess {
        if-exceeding {
            bandwidth-limit 1m;
            burst-size-limit 200k;
        }
        then out-of-profile;
    }
    policer voice-drop {
        if-exceeding {
            bandwidth-limit 2m;
            burst-size-limit 200k;
        }
        then discard;
    }
    filter voice-term {
        term 01 {
            from {
                forwarding-class voice-class;
            }
            then {
                policer voice-drop;
                next term;
            }
        }
        term 02 {
            from {
                forwarding-class voice-class;
            }
            then policer voice-excess;
        }
        term 03 {
            then accept;
        }
    }
}
```

Apply the Filter to the Output Interface

```
interfaces {
    e1-1/0/1 {
        unit 0 {
            family inet {
                filter {
                    output voice-term;
                }
                address 11.1.1.1/24;
            }
        }
    }
}
```
Example: Configuring Priority Scheduling

JUNOS Software supports multiple levels of transmission priority, which in order of increasing priority are low, medium-low, medium-high, and high, and strict-high. This allows the software to service higher-priority queues before lower-priority queues.

Priority scheduling determines the order in which an output interface transmits traffic from the queues, thus ensuring that queues containing important traffic are provided better access to the outgoing interface. This is accomplished through a procedure in which the software examines the priority of the queue. In addition, the software determines if the individual queue is within its defined bandwidth profile. This binary decision, which is reevaluated on a regular time cycle, compares the amount of data transmitted by the queue against the amount of bandwidth allocated to it by the scheduler. When the transmitted amount is less than the allocated amount, the queue is considered to be in profile. A queue is out-of-profile when its transmitted amount is larger than its allocated amount.

The queues for a given output physical interface (or output logical interface if per-unit scheduling is enabled on that interface) are divided into sets based on their priority. Any such set contains queues of the same priority.

The software traverses the sets in descending order of priority. If at least one of the queues in the set has a packet to transmit, the software selects that set. A queue from the set is selected based on the weighted round-robin (WRR) algorithm, which operates within the set.

You can configure priority scheduling, as shown in the following example:

1. Configure a scheduler, be-sched, with medium-low priority.

   ```
   [edit class-of-service]
   schedulers {
     be-sched {
       priority medium-low;
     }
   }
   ```

2. Configure a scheduler map, be-map, that associates be-sched with the best-effort forwarding class.

   ```
   [edit class-of-service]
   scheduler-maps {
     be-map {
       forwarding-class best-effort scheduler be-sched;
     }
   }
   ```

3. Assign be-map to a Gigabit Ethernet interface, ge-0/0/0.
Configuring CoS for Tunnels

CoS queuing, scheduling, and shaping allow you to control and improve the flow of traffic through tunnel interfaces like GRE and IP-IP interfaces. The GRE and IP-IP interfaces on a J Series device are internal, configurable interfaces named `gr-0/0/0` and `ip-0/0/0`.

To configure CoS for a GRE or IP-IP tunnel, you must first enable tunnel queuing on the router. If tunnel queuing is not enabled, the router continues to send traffic through the tunnel but ignores any configured CoS schedulers and shapers.

**NOTE:** You cannot enable tunnel queuing on J Series interfaces other than tunnel interfaces, although the router allows you to commit such a configuration.

You then define the GRE or IP-IP tunnel interface and its per-unit scheduler and set a line rate for the tunnel with the CoS shaper.

To configure CoS for tunnels, include the following statements at the [edit class-of-service] and [edit interfaces] hierarchy level:

```
[edit class-of-service]
interfaces {
    tunnel-interface-name {
        unit logical-unit-number {
            scheduler-map scheduler-map-name;
            shaping-rate, rate;
            rewrite-rules {
                dscp (rewrite-name | default);
                dscp-ipv6 (rewrite-name | default);
                exp (rewrite-name | default) protocol protocol-types;
                exp-push-push-push default;
                exp-swap-push-push default;
                ieee-802.1 (rewrite-name | default);
                inet-precedence (rewrite-name | default);
            }
        }
    }
    schedulers
    gre_be {
        transmit-rate transmit-rate-percent;
        shaping-rate rate;
        buffer-size buffer-size-percent;
        priority low;
        drop-profile-map loss-priority any protocol any drop-profile DP1;
    }
}
```
For an example of configuring GRE tunnels, see “Example: Configuring CoS for GRE/IPIP tunnels” on page 888.

**Configuring CoS Queuing for Tunnels with a Configuration Editor**

To configure COS queuing for GRE or IP-IP tunnels:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.

2. Perform the configuration tasks described in Table 217 on page 886 to configure CoS queuing for tunnel interfaces.
   a. Enable tunnel queuing on the router.
   b. Define the GRE or IP-IP tunnel interface.
c. Define the per-unit scheduler for the GRE or IP-IP tunnel interface.

d. Define the tunnel’s line rate by using the shaper definition.

3. Configure forwarding classes and schedulers.

   For information on configuring forwarding classes, see “Assigning Forwarding Classes to Output Queues” on page 838. For information on configuring schedulers, see “Configuring Schedulers” on page 857.

4. Configure a scheduler map and apply the scheduler map to the tunnel interface.

   For information on configuring a scheduler map, see “Configuring and Applying Scheduler Maps” on page 860.

5. Configure classifiers and apply them to the tunnel interface.

   For information on configuring classifiers, see “Configuring and Applying Behavior Aggregate Classifiers” on page 848.

6. Create rewrite rules and apply them to the tunnel interface.

   For information on configuring rewrite rules, see “Configuring and Applying Rewrite Rules” on page 845.

7. If you are finished configuring the router, commit the configuration.

8. Go on to one of the following tasks:

   ■ To configure other CoS components, see “Configuring CoS Components with a Configuration Editor” on page 833.

   ■ To check the configuration, see “Verifying a CoS Configuration” on page 941.

---

**Table 217: Configuring CoS for GRE Tunnels**

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Chassis level in the configuration hierarchy, and enable tunnel queuing on the router.</td>
<td>1. In the J-Web interface, select <strong>Configure &gt; CLI Tools &gt; Point and Click CLI</strong></td>
<td>From the [edit] hierarchy level, enter</td>
</tr>
<tr>
<td></td>
<td>2. Next to Chassis, click <strong>Configure</strong> or <strong>Edit</strong>.</td>
<td><strong>edit chassis fpc 0 pic 0 tunnel-queuing</strong></td>
</tr>
<tr>
<td></td>
<td>3. Next to Fpc, click <strong>Add new entry</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Next to Slot, type 0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Next to Pic, click <strong>Add New Entry</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Next to Slot, type 0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. Select the check box next to Tunnel queuing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>OK</strong> until you return to the main Configuration page.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 217: Configuring CoS for GRE Tunnels (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the <strong>Interfaces</strong> level in the configuration hierarchy, and define the GRE tunnel interface <strong>gr-0/0/0</strong>.</td>
<td>1. On the main Configuration page, next to Interfaces click <strong>Configure</strong> or <strong>Edit</strong>.</td>
<td>From the [edit] hierarchy level, enter edit interfaces <strong>gr-0/0/0</strong> unit 0.</td>
</tr>
<tr>
<td></td>
<td>2. In the Interfaces name box, type <strong>gr-0/0/0</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Next to Unit, click <strong>Add new entry</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. In the Interfaces unit number box, type <strong>0</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>OK</strong>.</td>
<td></td>
</tr>
<tr>
<td>Define the per-unit scheduler for the GRE tunnel interface.</td>
<td>1. From the Scheduler type list, select <strong>Per unit scheduler</strong>.</td>
<td>From the [edit] hierarchy level, enter set interfaces <strong>gr-0/0/0</strong> per-unit-scheduler.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>OK</strong> until you return to the main Configuration page.</td>
<td></td>
</tr>
<tr>
<td>Navigate to the <strong>Class of service level</strong> in the configuration hierarchy, and define the GRE tunnel’s line rate (for example, 100 Mbps) by using the shaper definition.</td>
<td>1. On the main configuration page next to Class of service, click <strong>Configure</strong> or <strong>Edit</strong>.</td>
<td>From the [edit] hierarchy level, enter set class-of-service interfaces <strong>gr-0/0/0</strong> unit 0 shaping-rate 100m</td>
</tr>
<tr>
<td></td>
<td>2. Next to Interfaces, click <strong>Add new entry</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. In the Interface name box, type the name of the interface <strong>gr-0/0/0</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. Next to unit, click <strong>Add New Entry</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. In the Interface unit number box, type the logical interface unit number <strong>0</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Select the Shaping rate check box, and click <strong>Configure</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. Next to Shaping Rate choice, select <strong>Rate</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. In the Rate box, type <strong>100m</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9. Click <strong>OK</strong> until you return to the main Class of Service configuration page.</td>
<td></td>
</tr>
</tbody>
</table>

**Preserving the ToS Value of a Tunneled Packet**

To ensure that the tunneled packet continues to have the same CoS treatment even in the physical interface, you must preserve the type-of-service (ToS) value from the inner IP header to the outer IP header.

For transit traffic, JUNOS Software preserves the CoS value of the tunnel packet for both GRE and IP-IP tunnel interfaces. The inner IPv4 or IPv6 ToS bits are copied to the outer IPv4 ToS header for both types of tunnel interfaces.

For Routing Engine traffic, however, the router handles GRE tunnel interface traffic differently from IP-IP tunnel interface traffic. Unlike for IP-IP tunnels, the IPv4 ToS bits are not copied to the outer IPv4 header by default. You have a configuration option to copy the ToS value from the packet’s inner IPv4 header to the outer IPv4 header.
To copy the inner ToS bits to the outer IP header (which is required for some tunneled routing protocols) on packets sent by the Routing Engine, include the `copy-tos-to-outer-ip-header` statement at the logical unit hierarchy level of a GRE interface.

**NOTE:** For IPv6 traffic, the inner ToS value is not copied to the outer IPv4 header for both GRE and IP-IP tunnel interfaces even if the `copy-tos-to-outer-ip-header` statement is specified.

This example copies the inner ToS bits to the outer IP header on a GRE tunnel:

```
[edit interfaces]
gr-0/0/0 {
  unit 0 {
    copy-tos-to-outer-ip-header;
    family inet;
  }
}
```

**Example: Configuring CoS for GRE/IPIP tunnels**

In the network shown in Figure 95 on page 888, Router A has a GRE tunnel established with Router B through interface ge-1/0/0. Router A also has an IP-IP tunnel established with Router C through interface ge-1/0/2. Router A is configured so that tunnel-queuing is enabled. Routers B and Router C do not have tunnel-queuing configured.

![Figure 95: Configuring CoS Queuing for GRE Tunnels](image)

Router A (has tunnel queuing)  chassis {
  fpc 0 {
    pic 0 {
      tunnel-queuing;
    }
  }
}
interfaces
  gr-0/0/0 {
    per-unit-scheduler;
    unit 0 {
      tunnel {
        source 192.12.12.1;
        destination 192.12.12.2;
        ttl 4;
      }
      family inet {
        address 192.22.22.1/30;
      }
      copy-tos-to-outer-ip-header;
    }
  }
  ip-0/0/0 {
    per-unit-scheduler;
    unit 0 {
      tunnel {
        source 192.13.13.1;
        destination 192.13.13.2;
        ttl 4;
      }
      family inet {
        address 192.33.33.1/30;
      }
    }
  }
  ge-1/0/0 {
    unit 0 {
      family inet {
        address 192.12.12.1/24;
      }
    }
  }
  ge-1/0/1 {
    unit 0 {
      family inet {
        address 192.13.13.1/24;
      }
    }
  }
class-of-service{
  classifiers {
    dscp gre-dscp {
      forwarding-class fc_be {
        loss-priority high code-points 000000;
      }
      forwarding-class fc_ef {
        loss-priority high code-points 101110;
      }
      forwarding-class fc_af{
        loss-priority low code-points 001010;
      }
      forwarding-class fc_nc {
        loss-priority low code-points 111111;
    }
configuring-cos-for-tunnels

inet-precedence ipip-inet-prec {
  forwarding-class fc_be {
    loss-priority high code-points 000;
  }
  forwarding-class fc_ef {
    loss-priority high code-points 001;
  }
  forwarding-class fc_af {
    loss-priority low code-points 010;
  }
  forwarding-class fc_nc {
    loss-priority low code-points 011;
  }
}

drop-profiles {
  DP1 {
    fill-level 80 drop-probability 60;
  }
  DP2 {
    fill-level 75 drop-probability 80;
  }
}

forwarding-classes {
  queue 0 fc_be;
  queue 1 fc_ef;
  queue 2 fc_af;
  queue 3 fc_nc;
}

interfaces {
  gr-0/0/0 {
    unit 0 {
      scheduler-map gre_sched_map;
      shaping-rate 4m;
      classifiers {
        dscp gre-dscp;
      }
      rewrite-rules {
        inet-precedence tnl_rw;
      }
    }
  }
  ip-0/0/0 {
    unit 0 {
      scheduler-map ipip_sched_map;
      shaping-rate 7m;
      classifiers {
        inet-precedence ipip-inet-prec;
      }
      rewrite-rules {
        inet-precedence tnl_rw;
      }
    }
  }
}
rewrite-rules {
  inet-precedence tnl_rw {
    forwarding-class fc_be {
      loss-priority high code-point 100;
    }
    forwarding-class fc_ef {
      loss-priority low code-point 101;
    }
    forwarding-class fc_af {
      loss-priority high code-point 110;
    }
    forwarding-class fc_nc {
      loss-priority high code-point 111;
    }
  }
}
scheduler-maps {
  gre_sched_map {
    forwarding-class fc_be scheduler gre_be;
    forwarding-class fc_ef scheduler gre_ef;
    forwarding-class fc_af scheduler gre_af;
    forwarding-class fc_nc scheduler gre_nc;
  }
  ipip_sched_map {
    forwarding-class fc_be scheduler ipip_be;
    forwarding-class fc_ef scheduler ipip_ef;
    forwarding-class fc_af scheduler ipip_af;
    forwarding-class fc_nc scheduler ipip_nc;
  }
}
schedulers {
  gre_be {
    transmit-rate percent 30;
    shaping-rate 2m;
    buffer-size percent 30;
    priority low;
    drop-profile-map loss-priority high protocol any drop-profile DP1;
  }
  gre_ef {
    transmit-rate percent 30;
    shaping-rate 1m;
    buffer-size percent 30;
    priority low;
    drop-profile-map loss-priority high protocol any drop-profile DP1;
  }
  gre_af {
    transmit-rate percent 25;
    buffer-size percent 25;
    priority high;
    drop-profile-map loss-priority high protocol any drop-profile DP1;
  }
  gre_nc {
    transmit-rate percent 15;
    buffer-size percent 15;
    priority high;
  }
}
Router B (has no tunnel queuing)

interface
g-0/0/0 {
  per-unit-scheduler;
  unit 0 {
    tunnel {
      source 192.12.12.2;
      destination 192.12.12.1;
      ttl 4;
    }
    family inet {
      address 192.22.22.2/30;
    }
    copy-tos-to-outer-ip-header;
  }
}
ge-1/0/3 {
  unit 0 {
    family inet {
      address 192.12.12.2/24;
    }
  }
}
Restrictions on CoS Shapers

On a J Series device, when defining a CoS shaping rate on a tunnel interface, be aware of the following restrictions:

- The shaping rate on the tunnel interface must be less than that of the physical egress interface.
- The shaping rate measures only the packet size that includes the Layer 3 packet with GRE or IP-IP encapsulation. The Layer 2 encapsulation added by the physical interface is not factored into the shaping rate measurement.
- The CoS behavior works as expected only when the physical interface carries the shaped GRE or IP-IP tunnel traffic alone. If the physical interface carries other traffic, thereby lowering the available bandwidth for tunnel interface traffic, the CoS features do not work as expected.
- You cannot configure a logical interface shaper and a virtual circuit shaper simultaneously on the device. If virtual circuit shaping is desired, do not define a logical interface shaper. Instead, define a shaping rate for all the virtual circuits.

Configuring Strict High Priority for Queuing with a Configuration Editor

You can configure one queue per interface to have strict-high priority, which causes delay-sensitive traffic, such as voice traffic, to be removed from the queue and forwarded with minimum delay. Packets that are queued in a strict-priority queue are removed from the queue before packets in other queues, including high-priority queues. For more information on strict-high priority, see “Configuring Strict-High Priority” on page 879.

To configure strict-priority queuing and prevent starvation of other queues:
1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.

2. Perform the configuration tasks described in Table 218 on page 894.

3. If you are finished configuring the router, commit the configuration.

Table 218: Configuring Strict-High Priority Queuing and Starvation Prevention

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring a BA Classifier</td>
<td>In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI</td>
<td>From the [edit] hierarchy level, enter edit Class of service classifiers inet-precedence corp-traffic forwarding-class voice-class loss-priority low</td>
</tr>
<tr>
<td></td>
<td>Next to Class of service, click Configure or Edit.</td>
<td>Enter set code-points 101</td>
</tr>
<tr>
<td></td>
<td>Next to Classifiers, click Configure or Edit.</td>
<td>From the [edit] hierarchy level, enter edit class-of-service classifiers inet-precedence corp-traffic forwarding-class data-class loss-priority high</td>
</tr>
<tr>
<td></td>
<td>Next to Inet precedence, click Add new entry.</td>
<td>Enter set code-points 000</td>
</tr>
<tr>
<td></td>
<td>Enter corp-traffic in the Name box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Next to Forwarding class, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter voice-class in the Class name box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Next to Loss priority, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter low in the Loss val box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Next to Code points, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter 101 in the Value box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Click OK three times.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the Inet precedence forwarding class page, enter voice-class in the Class name box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Next to Loss priority, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter high in the Loss val box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Next to Code points, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter 000 in the Value box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Click OK five times.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring the Forwarding Classes

1. Use a BA classifier to classify traffic based on the IP precedence of the packet. The classifier defines IP precedence value 101 as voice traffic and 000 as data traffic.
Table 218: Configuring Strict-High Priority Queuing and Starvation Prevention  (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign priority queuing to voice and data traffic.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit class-of-service forwarding-classes queue 0 voice-class</td>
</tr>
<tr>
<td></td>
<td>2. Next to Class of service, click Configure or Edit.</td>
<td>enter</td>
</tr>
<tr>
<td></td>
<td>3. Next to Forwarding classes, click Configure or Edit.</td>
<td>edit class-of-service forwarding-classes queue 1 data-class</td>
</tr>
<tr>
<td></td>
<td>4. Next to Queue, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Enter 0 in the Queue num box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Enter voice-class in the Class name box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. Click OK to return to the Forwarding Classes page.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. Next to Queue, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9. Enter 1 in the Queue num box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10. Enter data-class in the Class name box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>11. Click OK three times.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring the Scheduler Map and Schedulers

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the scheduler map and voice scheduler.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit class-of-service scheduler-maps corp-map forwarding-class voice-class</td>
</tr>
<tr>
<td></td>
<td>2. Next to Class of service, click Configure or Edit.</td>
<td>Enter</td>
</tr>
<tr>
<td></td>
<td>3. Next to Scheduler maps, click Add new entry.</td>
<td>set scheduler voice-sched</td>
</tr>
<tr>
<td></td>
<td>4. In the Map name box, type corp-map.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. Next to Forwarding class, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. In the Class name box, type voice-class.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. In the Scheduler name box, type voice-sched.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. Click OK three times.</td>
<td></td>
</tr>
</tbody>
</table>
Table 218: Configuring Strict-High Priority Queuing and Starvation Prevention  *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the voice and data traffic schedulers, and set the priority.</td>
<td></td>
<td>From the [edit] hierarchy level, enter edit class-of-service schedulers voice-sched Enter set priority strict-high Enter from [edit] hierarchy level, enter edit class-of-service schedulers data-sched Enter set priority low</td>
</tr>
<tr>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Next to Class of service, click Configure or Edit.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Next to Schedulers, click Add new entry.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. In the Scheduler name box, type voice-sched.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. In the Priority box, type strict-high.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Click OK.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Next to Schedulers, click Add new entry.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. In the Scheduler name box, type data-sched.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. In the Priority box, type low.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Click OK twice.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Applying the BA Classifier to an Input Interface and Scheduler Map to an Output Interface**
Table 218: Configuring Strict-High Priority Queuing and Starvation Prevention (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply the BA classifier to an input interface—for example, ge-0/0/0.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI</td>
<td>From the [edit] hierarchy level, enter edit interfaces ge-0/0/0 unit 0</td>
</tr>
<tr>
<td>Apply the scheduler map to and output interface—for example, e1-1/0/0.</td>
<td>2. Next to Interfaces, click Configure or Edit</td>
<td>From the [edit] hierarchy level, enter edit class of service classifiers inet-precedence</td>
</tr>
<tr>
<td></td>
<td>3. Next to Interface, click Add new entry</td>
<td>corp-traffic</td>
</tr>
<tr>
<td></td>
<td>4. In the Interface name box, type ge-0/0/0.</td>
<td>From the [edit] hierarchy level, enter edit interfaces e1-1/0/0 unit 0</td>
</tr>
<tr>
<td></td>
<td>5. Click OK three times</td>
<td>From the [edit] hierarchy level, enter edit class-of-service scheduler-maps corp-map</td>
</tr>
<tr>
<td></td>
<td>6. In the Edit Configuration page, next to Class of service, click Configure or Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7. Next to Classifiers, click Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8. Next to Inet precedence, click Add new entry</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9. In the Name box, type corp-traffic</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10. Click OK three times</td>
<td></td>
</tr>
<tr>
<td></td>
<td>11. In the Edit Configuration page, next to Interfaces, click Configure or Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12. Next to Interface name, type e1-1/0/1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>13. Click OK twice</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14. In the Edit Configuration page, next to Class of service, click Configure or Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15. Next to Scheduler maps, click Add new entry</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16. In the Map name box, type corp-map</td>
<td></td>
</tr>
<tr>
<td></td>
<td>17. Click OK twice</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring Two Policers**

Apply the BA classifier to an input interface—for example, ge-0/0/0. Then, apply the scheduler map to an output interface—for example, e1-1/0/0. (See the interface naming conventions in Junos OS Interfaces Configuration Guide for Security Devices.)

Applying the BA classifier to an input interface—for example, ge-0/0/0. Applying the scheduler map to an output interface—for example, e1-1/0/0. (See the interface naming conventions in Junos OS Interfaces Configuration Guide for Security Devices.)

Apply the BA classifier to an input interface—for example, ge-0/0/0. Then, apply the scheduler map to an output interface—for example, e1-1/0/0. (See the interface naming conventions in Junos OS Interfaces Configuration Guide for Security Devices.)
Table 218: Configuring Strict-High Priority Queuing and Starvation Prevention  
(continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure two policers: one as voice-drop and second as voice-excess.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit firewall policer voice-drop if-exceeding</td>
</tr>
<tr>
<td></td>
<td>2. Next to Firewall, click Configure or Edit.</td>
<td>Enter</td>
</tr>
<tr>
<td></td>
<td>3. Next to Policer, click Add new entry.</td>
<td>set burst-size-limit 200000</td>
</tr>
<tr>
<td></td>
<td>4. In the Policer name box, type voice-drop.</td>
<td>bandwidth-limit 2000000</td>
</tr>
<tr>
<td></td>
<td>5. Next to If Exceeding, select the check box and click Configure.</td>
<td>Enter</td>
</tr>
<tr>
<td></td>
<td>6. In the Burst size limit box, type 200000.</td>
<td>set then discard</td>
</tr>
<tr>
<td></td>
<td>7. In the Bandwidth list, select Bandwidth limit.</td>
<td>From the [edit] hierarchy level, enter edit firewall policer voice-excess if-exceeding</td>
</tr>
<tr>
<td></td>
<td>8. In the Bandwidth limit box, type 2000000.</td>
<td>Enter</td>
</tr>
<tr>
<td></td>
<td>9. Click OK.</td>
<td>set burst-size-limit 200000</td>
</tr>
<tr>
<td></td>
<td>10. On the Policer page, next to Then, click Configure.</td>
<td>bandwidth-limit 1000000</td>
</tr>
<tr>
<td></td>
<td>11. Next to Discard, select the check box.</td>
<td>Enter</td>
</tr>
<tr>
<td></td>
<td>12. Click OK twice.</td>
<td>set then out-of-profile</td>
</tr>
<tr>
<td></td>
<td>13. In the Firewall Configuration page next to Policer, click Add new entry.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14. In the Policer name box, type voice-excess.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15. Next to If Exceeding, select the check box and click Configure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16. In the Burst size limit box, type 200000.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>17. In the Bandwidth list, select Bandwidth limit.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>18. In the Bandwidth limit box, type 1000000.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>19. Click OK.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>20. On the Policer page, next to Then, click Configure.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>21. Next to Out of profile, select the check box.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>22. Click OK twice.</td>
<td></td>
</tr>
</tbody>
</table>
Table 218: Configuring Strict-High Priority Queuing and Starvation Prevention (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Create a firewall filter voice-term that includes the new policers.  
First, add the policer voice-drop to the term. | 1. In the Firewall Configuration page next to Filter, click Add new entry.  
2. In the Filter name box, type voice-term.  
3. Next to Term click Add new entry.  
4. In the Rule name box, type term 01.  
5. Next to Term, click Add new entry.  
6. Next to From, click Configure.  
7. Next to Forwarding class choice, select forwarding-class.  
8. Next to Forwarding class, click Add new entry.  
9. In the String box, type voice-class.  
10. Click OK twice.  
11. In the Term Filter page, next to Then, click Configure.  
12. Next to Policer choice, select policer.  
13. In the Policer box, type voice-drop.  
14. Next to Designation, select Next.  
15. In the Next box, select term.  
16. Click OK twice. | From the [edit] hierarchy level, enter edit firewall filter voice-term term 01 from forwarding-class voice-class then policer voice-drop next term |
| Then add the policer voice-excess to the term. | 1. In the Firewall Filter page, next to Term, click Add new entry.  
2. In the Rule name box, type term 02.  
3. Next to From, click Configure.  
4. Next to Forwarding class choice, select forwarding-class.  
5. Next to Forwarding class, click Add new entry.  
6. In the String box, type voice-class.  
7. Click OK twice.  
8. In the Term Filter page, next to Then, click Configure.  
9. Next to Policer choice, select policer.  
10. In the Policer box, type voice-excess.  
11. Next to Designation, select Accept.  
12. Click OK four times. | Enter edit firewall filter voice-term term 02 from forwarding-class voice-class then policer voice-excess accept |

**Applying the Filter to the Output Interface**
Table 218: Configuring Strict-High Priority Queuing and Starvation Prevention (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply filter voice-term to e1-1/0/0 using the CLI.</td>
<td>From the [edit] hierarchy level, enter edit interfaces e1-1/0/1 unit 0 family inet filter output voice-term</td>
<td>Enter set family inet address 11.1.1.1/24</td>
</tr>
</tbody>
</table>

**Configuring Large Delay Buffers with a Configuration Editor**

Large bursts of traffic from faster interfaces can cause congestion and dropped packets on slower interfaces that have small delay buffers. For example, a J Series device operating at the edge of the network can drop a portion of the burst traffic it receives on a channelized T1/E1 interface from a Fast Ethernet or Gigabit Ethernet interface on a router at the network core. On J Series devices, large delay buffers can be configured for both channelized T1/E1 and non-channelized T1/E1 interfaces.

To ensure that traffic is queued and transmitted properly on slower interfaces, you can configure a buffer size larger than the default maximum.

This section contains the following topics:

- Maximum Delay Buffer Sizes Available to Channelized T1/E1 Interfaces on page 900
- Delay Buffer Size Allocation Methods on page 901
- Specifying Delay Buffer Sizes for Queues on page 902
- Configuring a Large Delay Buffer on a non-Channelized T1 Interface on page 903
- Configuring a Large Delay Buffer on a Channelized T1 Interface on page 904

**Maximum Delay Buffer Sizes Available to Channelized T1/E1 Interfaces**

When you enable the large delay buffer feature on interfaces, a larger buffer is available for allocation to scheduler queues. The maximum delay buffer size that is available for an interface depends on the maximum available delay buffer time and the speed of the interface as shown in Table 219 on page 901.

- The default values are as follows:
  - Clear-channel interface—The default delay buffer time is 500,000 microseconds (0.5 seconds).
  - NxDS0 interface—The default delay buffer time is 1,200,000 microseconds (1.2 seconds).
### Table 219: Maximum Available Delay Buffer Time by Channelized Interface and Rate

<table>
<thead>
<tr>
<th>Effective Line Rate</th>
<th>Maximum Available Delay Buffer Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 4xDS0</td>
<td>4,000,000 microseconds (4 seconds)</td>
</tr>
<tr>
<td>&lt; 8xDS0</td>
<td>2,000,000 microseconds (2 seconds)</td>
</tr>
<tr>
<td>&lt; 16xDS0</td>
<td>1,000,000 microseconds (1 second)</td>
</tr>
<tr>
<td>&lt; = 32xDS0</td>
<td>500,000 microseconds (0.5 second)</td>
</tr>
<tr>
<td>&lt; = 30mbps</td>
<td>400,000 microseconds (0.4 seconds)</td>
</tr>
<tr>
<td>&lt; = 20mbps</td>
<td>300,000 microseconds (0.3 seconds)</td>
</tr>
<tr>
<td>&lt; = 10mbps</td>
<td>200,000 microseconds (0.2 seconds)</td>
</tr>
<tr>
<td>&lt; = 40mbps</td>
<td>150,000 microseconds (0.15 second)</td>
</tr>
</tbody>
</table>

You can calculate the maximum delay buffer size available for an interface, with the following formula:

\[ \text{interface speed} \times \text{maximum delay buffer time} = \text{maximum available delay buffer size} \]

For example, the following maximum delay buffer sizes are available to 1xDS0 and 2xDS0 interfaces:

- **1xDS0**—64 kilobits per second \(\times\) 4 seconds = 256 kilobits (32 kilobytes)
- **2xDS0**—128 kilobits per second \(\times\) 4 seconds = 512 kilobits (64 kilobytes)

If you configure a delay buffer size larger than the new maximum, the system allows you to commit the configuration but displays a system log warning message and uses the default buffer size setting instead of the configured maximum setting.

### Delay Buffer Size Allocation Methods

You can specify delay buffer sizes for each queue using schedulers. The queue buffer can be specified as a period of time (microseconds) or as a percentage of the total buffer or as the remaining buffer. Table 220 on page 901 shows different methods that you can specify for buffer allocation in queues.

### Table 220: Delay Buffer Size Allocation Methods

<table>
<thead>
<tr>
<th>Buffer Size Allocation Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage</td>
<td>A percentage of the total buffer.</td>
</tr>
</tbody>
</table>
Table 220: Delay Buffer Size Allocation Methods (continued)

<table>
<thead>
<tr>
<th>Buffer Size Allocation Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporal</td>
<td>A period of time, value in microseconds. When you configure a temporal buffer, you must also configure a transmit rate. The system calculates the queue buffer size by multiplying the available bandwidth of the interface times the configured temporal value and transmit rate. When you specify a temporal method, the drop profile is assigned a static buffer and the system starts dropping packets once the queue buffer size is full. By default, the other buffer types are assigned dynamic buffers that use surplus transmission bandwidth to absorb bursts of traffic.</td>
</tr>
<tr>
<td>Remainder</td>
<td>The remaining buffer available. The remainder is the percentage buffer that is not assigned to other queues. For example, if you assign 40 percent of the delay buffer to queue 0, allow queue 3 to keep the default allotment of 5 percent, and assign the remainder to queue 7, then queue 7 uses approximately 55 percent of the delay buffer.</td>
</tr>
</tbody>
</table>

Specifying Delay Buffer Sizes for Queues

You specify delay buffer sizes for queues using schedulers. The system calculates the buffer size of a queue based on the buffer allocation method you specify for it in the scheduler. See Table 220 on page 901 for different buffer allocation methods and Table 221 on page 902 for buffer size calculations.

Table 221: Delay Buffer Allocation Method and Queue Buffer

<table>
<thead>
<tr>
<th>Buffer Size Allocation Method</th>
<th>Queue Buffer Calculation</th>
<th>Example</th>
</tr>
</thead>
</table>
| Percentage                    | available interface bandwidth x configured buffer size percentage x maximum delay buffer time = queue buffer | Suppose you configure a queue on a 1xD50 interface to use 30 percent of the available delay buffer size. The system uses the maximum available delay buffer time (4 seconds) and allocates the queue 9600 bytes of delay buffer:  

\[ 64 \text{ Kbps} \times 0.3 \times 4 \text{ seconds} = 76800 \text{ bits} = 9600 \text{ bytes} \] |
Table 221: Delay Buffer Allocation Method and Queue Buffer (continued)

<table>
<thead>
<tr>
<th>Buffer Size Allocation Method</th>
<th>Queue Buffer Calculation</th>
<th>Example</th>
</tr>
</thead>
</table>
| Temporal                      | available interface bandwidth x configured transmit rate percentage x configured temporal buffer size = queue buffer | Suppose you configure a queue on a 1xDS0 interface to use 300,000 microseconds (3 seconds) of delay buffer, and you configure the transmission rate to be 20 percent. The queue receives 4800 bytes of delay buffer:  

\[
64 \text{ Kbps} \times 0.2 \times 3 \text{ seconds} = 38400 \text{ bits} = 4800 \text{ bytes}
\]

When you configure a temporal value that is greater than the maximum available delay buffer time, the system allocates this queue the remaining buffer after other queues are allocated buffer. Suppose you configure a temporal value of 6,000,000 microseconds on a 1xDS0 interface. Because this value is greater than the maximum allowed value of 4,000,000 microseconds, the queue is allocated the remaining delay buffer.

When you specify the buffer size as a percentage, the system ignores the transmit rate and calculates the buffer size based only on the buffer size percentage.

Configuring a Large Delay Buffer on a non-Channelized T1 Interface

To configure large-delay buffers on non C-TI/E1 interfaces, you must first enable the large buffer feature and then extend the q-pic-large-delay-buffer size on all interfaces. The maximum delay buffer time varies by the interface speed as shown in Table 222 on page 903.

Table 222: Recommended Delay Buffer Sizes

<table>
<thead>
<tr>
<th>Interface Speed (kbps)</th>
<th>Effective Bandwidth in kilobytes per second (kbps)</th>
<th>Recommended Buffer Size in microseconds (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 256kbps</td>
<td>&lt; 256kbps</td>
<td>4000ms</td>
</tr>
<tr>
<td>256kbps</td>
<td>&lt; 512kbps</td>
<td>2000ms</td>
</tr>
<tr>
<td>512kbps</td>
<td>&lt; 024kbps</td>
<td>1000ms</td>
</tr>
<tr>
<td>1024kbps</td>
<td>&lt; 2048kbps</td>
<td>500ms</td>
</tr>
<tr>
<td>&gt; 2048kbps</td>
<td></td>
<td>100ms</td>
</tr>
</tbody>
</table>

For more information on using J-web or the CLI configuration editor to configure large delay buffers, see “Configuring a Large Delay Buffer on a Channelized T1 Interface” on page 904.
Configuring a Large Delay Buffer on a Channelized T1 Interface

On J Series devices, you can configure large delay buffers on channelized T1/E1 interfaces. To configure large-delay buffer sizes, you must first enable the large buffer feature on the channelized T1/E1 PIM and then configure a buffer size for each queue in the CoS scheduler.

Each channelized T1/E1 interface can be configured as a single clear channel, or for channelized (NxDS0) operation, where N denotes channels 1 to 32 for an E1 interface and channels 1 to 24 for a T1 interface.

In this configuration, you enable the large delay buffer option on a channelized T1 PIM with an interface speed of 1.5 Mbps and a maximum delay buffer time of 500,000 microseconds. Based on the interface speed and the maximum delay buffer time, you can calculate the available delay buffer size for the interface. For more information, see “Maximum Delay Buffer Sizes Available to Channelized T1/E1 Interfaces” on page 900.

Next, you specify a queue buffer of 30 percent in a scheduler be-scheduler and associate the scheduler to a defined forwarding class be-class using a scheduler map large-buf-sched-map. Finally, you apply the scheduler map to the channelized T1 interface t1-3/0/0. As a result, a buffer of 9600 bytes is assigned to the queue associated with forwarding class be-class (see Table 221 on page 902). You can specify a delay buffer size for other queues following the instructions in this example.

To configure large delay buffers for channelized T1/E1 interfaces:

1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 223 on page 904.
3. If you are finished configuring the router, commit the configuration.
4. Go on to one of the following tasks:
   - To configure other CoS components, see “Configuring CoS Components with a Configuration Editor” on page 833.
   - From the CLI, enter the show class of service command, to check your configuration.

Table 223: Configuring a Large Delay Buffer

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to the Chassis level in the configuration hierarchy.</td>
<td>1. In the J-Web interface, select Configure &gt; CLI Tools &gt; Point and Click CLI.</td>
<td>From the [edit] hierarchy level, enter edit chassis</td>
</tr>
<tr>
<td></td>
<td>2. Next to Chassis, click Configure or Edit.</td>
<td></td>
</tr>
</tbody>
</table>
Table 223: Configuring a Large Delay Buffer  (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>J-Web Configuration Editor</th>
<th>CLI Configuration Editor</th>
</tr>
</thead>
</table>
| Enable the large buffer size feature on the channelized T1/E1 PIM in slot 3. | 1. Next to Fpc, click Add new entry.  
2. In the Slot box, type the slot number 3.  
3. Next to Pic, click Add new entry.  
4. In the Slot box, type 0.  
5. Next to Q pic large buffer, select the check box.  
6. Click OK. | Enter
set fpc 3 pic 0 q-pic-large-buffer |
| Navigate to the Class-of-service level in the configuration hierarchy. | On the main Configuration page next to Class of service, click Configure or Edit. | From the [edit] hierarchy level, enter
eedit class-of-service |
| Create be-scheduler and specify a buffer size of 30 percent for it. | 1. Next to Schedulers, click Add new entry.  
2. In the Scheduler name box, type the name of the scheduler—be-scheduler.  
3. Next to Buffer size, click Configure.  
4. From the Buffer size choice list, select percent.  
5. In the Percent box, type 30.  
6. Click OK. | Enter
set schedulers be-scheduler buffer-size percent 30 |
| Configure the scheduler map large-buf-sched-map to associate schedulers with defined forwarding classes. For information about configuring forwarding classes, see “Assigning Forwarding Classes to Output Queues” on page 838. | 1. On the Class of service page, next to Scheduler maps, click Add new entry.  
2. In the Map name box, type the name of the scheduler map—large-buf-sched-map.  
3. Next to Forwarding class, click Add new entry.  
4. In the Class name box, type the name of the forwarding class to be associated with the scheduler—be-class.  
5. In the Scheduler box, type the name of the scheduler to be associated with the forwarding class—be-scheduler.  
6. Click OK. | From the [edit class-of-service] hierarchy level, enter
set scheduler-maps large-buf-sched-map forwarding-class be-class scheduler be-scheduler |
| Apply the scheduler map to the channelized T1 interface. **NOTE:** For information about configuring channelized T1/E1 interfaces, see Junos OS Interfaces Configuration Guide for Security Devices. | 1. On the Class of service page, next to Interfaces, click Add new entry.  
2. In the Interface name box, type the name of the interface to which the scheduler map is to be applied—t1-3/0/0.  
3. Next to Unit, click Add new entry.  
4. In the Unit number box, type 0.  
5. In the Scheduler map box, type the name of the scheduler map—large-buf-sched-map.  
6. Click OK. | From the [edit class-of-service] hierarchy level, type
set interfaces t1-3/0/0 unit 0 scheduler-map large-buf-sched-map |
Applying an Ingress Interface Policer

Policers allow you to limit traffic of a certain class to a specified bandwidth and burst size. You can use policers to limit the amount of traffic passing into or out of an interface. SRX5600 and SRX5800 devices support two I/O cards (IOCs) (40x1 Gigabit Ethernet IOC and 4x10 Gigabit Ethernet IOC) and allow only inbound (ingress) interface policers.

**NOTE:** For applying a simple filter or policing actions to logical interfaces residing in an SRX5000 line Flex IOC (FIOC) on SRX5600 and SRX5800 devices, see “Configuring Simple Filters and Policers” on page 907.

Consider the following when applying a policer to an ingress interface:

- You can configure a tricolor marker in the firewall; however, you cannot use the marker in the input policer (the CLI will block it). For more information on applying tricolor markers, see “Example: Applying a Two-Rate Tricolor Marking Policer to a Firewall Filter” on page 909.

- Only the following options are valid: `logical-interface-policer`, `if-exceeding`, and `then`. For more information on applying a stateless firewall filter to an interface, see Junos OS Routing Protocols and Policies Configuration Guide for Security Devices.

- For the `if-exceeding` option, only `bandwidth-limit` and `burst-size-limit` are valid options. The `bandwidth-percent` option is not supported.

- For the `then` option, only `discard` is the valid option.

To filter packets transiting the device, apply the firewall filter to any nonrouting device.

```bash
ge-0/1/0 {
    unit 0 {
        family inet {
            policer {
                input ingress-p;
            }
            address 200.4.1.1/24 {
                arp 200.4.1.100 mac 00:00:de:ad:be:ee;
            }
        }
    }
}

ge-0/3/0 {
    unit 0 {
        family inet {
            address 200.4.3.1/24 {
                arp 200.4.3.100 mac 00:00:de:ad:be:ef;
            }
        }
    }
}
To view the configuration of the firewall policer ingress-p, use the `show configuration firewall policer` command. For example:

```
user@host# show configuration firewall policer ingress-p logical-interface-policer;
if-exceeding {
  bandwidth-limit 8m;
  burst-size-limit 1m
}
then-discard;
```

### Configuring Simple Filters and Policers

To handle oversubscribed traffic in the SRX3400, SRX3600, SRX5600, and SRX5800 devices, you can configure simple filters and policing.

**NOTE:** For SRX5600 and SRX5800 devices, the simple filter or policing actions can be applied only to logical interfaces residing in an SRX5000 line Flex IOC (FIOC), because only an SRX5000 line FIOC supports the simple filter and policing features on the SRX5600 and SRX5800 devices.

The simple filter functionality comprises of the following:

- Classifying packets according to configured policies
- Taking appropriate actions based on the results of classification

In JUNOS Software, ingress traffic policers can limit the rate of incoming traffic. There are two main reasons to use traffic policing:

- To enforce traffic rates to conform to the service-level agreement (SLA)
- To protect next hops, for example, protecting the central point and the SPU from being overwhelmed by excess traffic (example, DOS attacks)

Using the results of packet classification and traffic metering, a policer can take one of the following actions for a packet: forward a conforming (green) packet or drop a nonconforming (yellow) packet. Policers always discard a non conforming red packet.

The traffic metering supports the algorithm of the two-rate tricolor marker (TCM) (RFC 2698). For more information on packet classification and traffic metering, see “Configuring CoS Components with a Configuration Editor” on page 833.

### Configuring a Simple Filter

Simple filters, in contrast to other firewall filters, support only a subset of the full firewall filter syntax. Unlike normal filters, simple filters are for IPv4 traffic only and have the following restrictions:

- The next term action is not supported.
- Qualifiers, such as the except and protocol-except statements, are not supported.
Noncontiguous masks are not supported.

Multiple source addresses and destination addresses in a single term are not supported. If you configure multiple addresses, only the last one is used.

Ranges are not supported.

Output filters are not supported. You can apply a simple filter to inbound (ingress) traffic only.

To configure a simple filter, include the following statement at the [edit firewall] hierarchy level of the configuration:

```junos
Simple Filter
firewall {
    family inet {
        simple-filter sf-1 {
            term 1 {
                source-address 172.16.0.0/16;
                destination-address 20.16.0.0/16;
                source-port 1024;
            }
            then { # Action with term-1
                forwarding-class fc-be1;
                loss-priority high;
            }
            term 2 {
                source-address 173.16.0.0/16;
                destination-address 21.16.0.0/16;
            }
            then { # Action with term-2
                forwarding-class fc-ef1;
                loss-priority low;
            }
        }
    }
    interfaces { # Apply the simple filter.
        ge-1/2/3 {
            unit 0 {
                family inet {
                    simple-filter {
                        input sf-1;
                    }
                }
            }
        }
    }
}
```

### Applying a Simple Filter

A simple filter can be applied to logical interfaces. Use the following CLI commands to apply a simple filter:

```bash
edit interfaces interface-name unit logical-unit-number family family-name simple-filter {
    input filter-name;
}
```
NOTE: You can apply simple filters to the family inet only, and only in the input direction. Because of hardware limitations on the SRX3400, SRX3600, SRX5600, and SRX5800 devices, a maximum of 400 logical input interfaces (in one broadcom packet processor) can be applied with simple filters. For more information on limitations, see “SRX3400 and SRX3600 Device Hardware Capabilities and Limitations” on page 913.

Configuring Policers

In JUNOS Software, policers can be configured as part of the firewall filter hierarchy. For more information on configuring firewall policies, see the JUNOS Software Security Configuration Guide.

You can configure a policer and then apply it as one of the actions of a term in a simple filter. The policer can limit the rate of traffic that enters the logical interface to which the simple filter is applied. Figure 96 on page 909 illustrates the application of a policer.

Figure 96: Application of a Policer Through a Simple Filter

Use the following CLI commands to configure a policer:

```
policer policer-name {
    filter-specific;
    if-exceeding {
        bandwidth-limit bps;
        burst-size-limit bytes;
    }
    then {
        policer-action;
    }
}
```

Example: Applying a Two-Rate Tricolor Marking Policer to a Firewall Filter

To configure a trTCM policer to a firewall filter, use the following JUNOS CLI commands:

```
firewall {
    three-color-policer three-color-policer name{
    two-rate {
```
NOTE: The two-rate TCM policer supports only the color blind mode; color aware mode is not supported.

Configuring CoS Hierarchical Schedulers

In metro Ethernet environments, a VLAN typically corresponds to a customer premises equipment (CPE) device and the VLANs are identified by an inner VLAN tag on Ethernet frames (called the customer VLAN, or C-VLAN, tag). A set of VLANs can be grouped at the DSL access multiplexer (DSLAM) and identified by using the same outer VLAN tag (called the service VLAN, or S-VLAN, tag). The service VLANs are typically gathered at the Broadband Remote Access Server (BRAS) level, which can be (among other devices) an SRX Series device. On SRX5600 and SRX5800 devices, hierarchical schedulers let you provide shaping and scheduling at the service VLAN level as well as other levels, such as the physical interface. In other words, you can group a set of logical interfaces and then apply scheduling and shaping parameters to the logical interface set as well as to other levels.

This basic architecture is shown in Figure 97 on page 911. You can apply class-of-service (CoS) parameters at the premises on the CPE, on the customer or service VLANs, at the BRAS level, or at all levels.
On SRX5600 and SRX5800 devices, you can apply CoS shaping and scheduling at one of four different levels, including the VLAN set level.

The supported scheduler hierarchy is as follows:

- The physical interface (level 1)
- The service VLAN (level 2 is unique to SRX Series devices)
- The logical interface or customer VLAN (level 3)
- The queue (level 4)

You can specify a traffic control profile (output-traffic-control-profile) that can specify a shaping rate, a guaranteed rate, and a scheduler map with transmit rate and buffer delay. The scheduler map contains the mapping of queues (forwarding classes) to their respective schedulers (schedulers define the properties for the queue). Queue properties can specify a transmit rate and buffer management parameters such as buffer size and drop profile. For more information, see “Defining Schedulers” on page 824.

To configure CoS hierarchical schedulers, include the following statements at the [edit class-of-service interfaces] and [edit interfaces] hierarchy levels:

```
[edit class-of-service interfaces]
interface-set interface-set-name {
    excess-bandwidth-share (proportional value | equal);  
    internal-node;
```
Hierarchical Scheduler Terminology

Hierarchical schedulers introduce some new terms into a discussion of CoS capabilities. They also use some familiar terms in different contexts. This section presents a complete overview of the terms used with hierarchical schedulers.

The following terms are important for hierarchical schedulers:

- **Customer VLAN (C-VLAN)**—A C-VLAN, defined by IEEE 802.1ad. A stacked VLAN contains an outer tag corresponding to the S-VLAN, and an inner tag corresponding to the C-VLAN. A C-VLAN often corresponds to CPE. Scheduling and shaping is often used on a C-VLAN to establish minimum and maximum bandwidth limits for a customer. See also **S-VLAN**.

- **Interface set**—A logical group of interfaces that describe the characteristics of set of service VLANs, logical interfaces, or customer VLANs. Interface sets establish the set and name the traffic control profiles. See also **Service VLAN**.

- **Scheduler**—A scheduler defines the scheduling and queuing characteristics of a queue. Transmit rate, scheduler priority, and buffer size can be specified. In addition, a drop profile may be referenced to describe WRED congestion control aspects of the queue. See also **Scheduler map**.

- **Scheduler map**—A scheduler map is referenced by traffic control profiles to define queues. The scheduler map establishes the queues that comprise a scheduler node and associates a forwarding class with a scheduler. See also **Scheduler**.

- **Stacked VLAN**—An encapsulation on an S-VLAN with an outer tag corresponding to the S-VLAN, and an inner tag corresponding to the C-VLAN. See also **Service VLAN** and **Customer VLAN**.

- **Service VLAN (S-VLAN)**—An S-VLAN, defined by IEEE 802.1ad, often corresponds to a network aggregation device such as a DSLAM. Scheduling and shaping is often established for an S-VLAN to provide CoS for downstream devices with little buffering and simple schedulers. See also **Customer VLAN**.

- **Traffic control profile**—Defines the characteristics of a scheduler node. Traffic control profiles are used at several levels of the CLI, including the physical interface, interface set, and logical interface levels. Scheduling and queuing characteristics can be defined for the scheduler node using the **shaping-rate**, **guaranteed-rate**, and **delay-buffer-rate** statements. Queues over these scheduler
nodes are defined by referencing a scheduler map. See also Scheduler and Scheduler map.

- VLAN—Virtual LAN, defined on an Ethernet logical interface.

These terms are especially important when applied to a scheduler hierarchy. Scheduler hierarchies are composed of nodes and queues. Queues terminate the CLI hierarchy. Nodes can be either root nodes, leaf nodes, or internal (non-leaf) nodes. Internal nodes are nodes that have other nodes as “children” in the hierarchy. For example, if an interface-set statement is configured with a logical interface (such as unit 0) and queue, then the interface-set is an internal node at level 2 of the hierarchy. However, if there are no traffic control profiles configured on logical interfaces, then the interface set is at level 3 of the hierarchy.

Table 224 on page 913 shows how the configuration of an interface set or logical interface affects the terminology of hierarchical scheduler nodes.

**Table 224: Hierarchical Scheduler Nodes**

<table>
<thead>
<tr>
<th>Root Node (Level 1)</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Queue (Level 4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical interface</td>
<td>Interface set</td>
<td>Logical interfaces</td>
<td>One or more queues</td>
</tr>
<tr>
<td>Physical interface</td>
<td>Interface set</td>
<td>Logical interfaces</td>
<td>One or more queues</td>
</tr>
<tr>
<td>Physical interface</td>
<td>Logical interfaces</td>
<td>One or more queues</td>
<td></td>
</tr>
</tbody>
</table>

**SRX3400 and SRX3600 Device Hardware Capabilities and Limitations**

The following list describes the hardware capabilities and limitations for the SRX3400 and SRX3600 devices:
For SRX3400 and SRX3600 devices, each Input/Output Card (IOC) Flexible PIC Concentrator (FPC) or IOC slot has only one Physical Interface Card (PIC), which contains either two 10-Gigabit or sixteen 1-Gigabit Ethernet ports. Table 225 on page 914 shows the maximum number of cards and ports allowed in an SRX3400 and SRX3600 device.

### Table 225: Available NPCs and IO Ports for SRX3400 and SRX3600 Devices

<table>
<thead>
<tr>
<th>System</th>
<th>IOCs</th>
<th>IO Ports</th>
<th>NPCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRX3600</td>
<td>7</td>
<td>108 (16 x 6 + 12)</td>
<td>5</td>
</tr>
<tr>
<td>SRX3400</td>
<td>5</td>
<td>76 (16 x 4 + 12)</td>
<td>2</td>
</tr>
</tbody>
</table>

**NOTE:** The number of ports the Network Processing Unit (NPU) needs to handle may be different than the fixed 10:1 port to NPU ratio for 1G IOC, or the 1:1 ratio for the 10G IOC that is needed on the SRX5600 and SRX5800 devices, leading to oversubscription on the SRX3400 and SRX3600 devices.

SRX3400 and SRX3600 devices allow you to install up to three Network Processing Cards (NPC). In a single-NPC configuration, the NPC has to process all of the packets to and from each IOC. However, when there is more than one NPC available, an IOC will only exchange packets with a pre-assigned NPC. You can use the `set chassis ioc-npc-connectivity` CLI statement to configure the IOC-to-NPC mapping. By default, the mapping is assigned so that the load is shared equally among all NPCs. When the mapping is changed, for example, an IOC or NPC is removed, or you have mapped a specific NPC to an IOC, then the device has to be restarted. For more information, see the *JUNOS Software Administration Guide for Security Devices*.

For SRX3400 and SRX3600 devices, the IOC supports the following hierarchical scheduler characteristics:

- Level 1: Shaping at the physical interface (ifd)
- Level 2: Shaping and scheduling at the logical interface level (ifl)
- Level 3: Scheduling at the queue level

**NOTE:** Interface set (iflset) is not supported for the SRX3400 and SRX3600 devices.

Shaping at the port level—In SRX5600 and SRX5800 devices, an NPC supports 32 port-level shaping profiles at level 1, such that each front port can have its own shaping profile.

In SRX3400 and SRX3600 devices, an NPC supports only 16 port-level shaping profiles in the hardware, including two profiles that are predefined for 10-Gbps and 1-Gbps shaping rates. The user can configure up to 14 different levels of
shaping rates. If more levels are configured, then the closest match found in the 16 profiles will be used instead.

For example, assume that a system is already configured with the following rates for ifds:

10Mbps, 20Mbps, 40Mbps, 60Mbps, 80Mbps, 100Mbps, 200Mbps, 300Mbps, 400Mbps, 500Mbps, 600Mbps, 700Mbps, 800Mbps, 900Mbps, 1Gbps (predefined), 10Gbps (predefined)

Each of these 16 rates is programmed into one of the 16 profiles in the hardware, then consider the following two scenarios.

1. If the user changes one port’s shaping rate from 1Gbps to 100Mbps, which is already programmed in one of the 16 profiles, the profile with 100Mbps shaping rate will be used by the port.

2. If the user changes another port’s shaping rate from 1Gbps to 50Mbps, which is not in the shaping profiles, the closest matching profile with 60Mbps shaping rate will be used instead.

When scenario 2) happens, not all of the user-configured rates can be supported by the hardware. If more than 14 different rates are specified, only 14 will be programmed in the hardware. Which 14 rates are programmed in the hardware depends on many factors. For this reason, we recommend that you plan carefully and use no more than 14 levels of port-level shaping rates.

Weighed Random Early Discard (WRED) at the port level—Each NPU has 512 MB of frame memory. Also, 10-Gigabit Ethernet ports get more buffers than the 1-Gigabit Ethernet ports. Buffer availability depends on how much bandwidth (number of NPCs, ports, 1-Gigabit or 10-Gigabit, and so forth) the device has to support. The more the bandwidth that the device has to support, the less buffer is available. When two NPCs are available, the amount of frame buffer available is doubled.

**Configuring an Interface Set**

To configure an interface set, include the following statement at the [edit class-of-service interfaces] hierarchy level of the configuration:

```
[edit class-of-service interfaces]
interface-set interface-set-name { (interface-cos-parameters);
}
```

To apply the interface set to interfaces, include the following statements at the [edit interfaces] hierarchy level of the configuration:

```
interface-set interface-set-name {
  ethernet-interface-name { (interface-cos-parameters);
  }
}
```
Interface sets can be defined as a list of logical interfaces (unit 100, unit 200, and so on). Service providers can use these statements to group interfaces to apply scheduling parameters such as guaranteed rate and shaping rate to the traffic in the groups.

All traffic heading downstream must be gathered into an interface set with the interface-set statement at the [edit class-of-service interfaces] hierarchy level.

Interface sets are currently only used by CoS, but they are applied at the [edit interfaces] hierarchy level so that they might be available to other services.

```
[edit interfaces]
interface-set interface-set-name {
  ethernet-interface-name {
    unit unit-number {
      ...
    }
  }
}
```

The logical interface naming option lists Ethernet interfaces:

```
[edit interfaces]
interface-set unitl-set-ge-0 {
  ge-0/0/0 {
    unit 0;
    unit 1;
    ...
  }
}
```

**NOTE:** Ranges are not supported; you must list each logical interface separately.

---

**Applying an Interface Set**

Although the interface set is applied at the [edit interfaces] hierarchy level, the CoS parameters for the interface set are defined at the [edit class-of-service interfaces] hierarchy level, usually with the output-traffic-control-profile profile-name statement.

This example applies a traffic control profile called tcp-set1 to an interface set called set-ge-0:

```
[edit interfaces]
interface-set set-ge-0 {
  output-traffic-control-profile tcp-set1;
}
```

**Interface Set Caveats**

You cannot specify an interface set mixing the logical interface, S-VLAN, or VLAN outer tag list forms of the interface-set statement.
A logical interface can only belong to one interface set. If you try to add the same logical interface to different interface sets, the commit will fail.

This example will generate a commit error:

```plaintext
[edit interfaces]
interface-set set-one {
  ge-2/0/0 {
    unit 0;
    unit 2;
  }
}
interface-set set-two {
  ge-2/0/0 {
    unit 1;
    unit 3;
    unit 0; # COMMIT ERROR! Unit 0 already belongs to -set-one.
  }
}
```

Members of an interface set cannot span multiple physical interfaces. Only one physical interface is allowed to appear in an interface set.

This configuration is not supported:

```plaintext
[edit interfaces]
interface-set set-group {
  ge-0/0/1 {
    unit 0;
    unit 1;
  }
  ge-0/0/2 { # This type of configuration is NOT supported in the same interface set!
    unit 0;
    unit 1;
  }
}
```

### Introduction to Hierarchical Schedulers

When used, the interface set level of the hierarchy falls between the physical interface level (level 1) and the logical interface (level 3). Queues are always level 4 of the hierarchy.

Hierarchical schedulers add CoS parameters to the new interface set level of the configuration. They use traffic control profiles to set values for parameters such as shaping rate (the peak information rate [PIR]), guaranteed rate (the committed information rate [CIR] on these interfaces), scheduler maps (assigning queues and resources to traffic), and so on.

The following CoS configuration places the following parameters in traffic control profiles at various levels:

- Traffic control profile at the port level (`tcp-port-level1`):
  - A shaping rate (PIR) of 100 Mbps
  - A delay buffer rate of 100 Mbps
Traffic control profile at the interface set level (tcp-interface-level2):
- A shaping rate (PIR) of 60 Mbps
- A guaranteed rate (CIR) of 40 Mbps

Traffic control profile at the logical interface level (tcp-unit-level3):
- A shaping rate (PIR) of 50 Mbps
- A guaranteed rate (CIR) of 30 Mbps
- A scheduler map called smap1 to hold various queue properties (level 4)
- A delay buffer rate of 40 Mbps

In this case, the traffic control profiles look like this:

```
[edit class-of-service traffic-control-profiles]
tcp-port-level1 { # This is the physical port level
    shaping-rate 100m;
    delay-buffer-rate 100m;
}
tcp-interface-level2 { # This is the interface set level
    shaping-rate 60m;
    guaranteed-rate 40m;
}
tcp-unit-level3 { # This is the logical interface level
    shaping-rate 50m;
    guaranteed-rate 30m;
    scheduler-map smap1;
    delay-buffer-rate 40m;
}
```

Once configured, the traffic control profiles must be applied to the proper places in the CoS interfaces hierarchy.

```
[edit class-of-service interfaces]
interface-set level-2 {
    output-traffic-control-profile tcp-interface-level-2;
}
ge-0/1/0 {
    output-traffic-control-profile tcp-port-level-1;
    unit 0 {
        output-traffic-control-profile tcp-unit-level-3;
    }
}
```

In all cases, the properties for level 4 of the hierarchical schedulers are determined by the scheduler map.

**Scheduler Hierarchy Example**

This section provides a more complete example of building a 4-level hierarchy of schedulers. The configuration parameters are shown in Figure 98 on page 919. The queues are shown at the top of the figure with the other three levels of the hierarchy below.
The figure’s PIR values will be configured as the shaping rates, and the CIRs will be configured as the guaranteed rate on the Ethernet interface ge-1/0/0. The PIR can be oversubscribed (that is, the sum of the children PIRs can exceed the parent’s, as in svlan 1, where 200 + 200 + 100 exceeds the parent rate of 400). However, the sum of the children node level’s CIRs must never exceed the parent node’s CIR, as shown in all the service VLANs (otherwise, the guaranteed rate could never be provided in all cases).

This configuration example will present all details of the CoS configuration for the interface in the figure (ge-1/0/0), including:

- Interface Sets for the Hierarchical Example on page 919
- Interfaces for the Hierarchical Example on page 920
- Traffic Control Profiles for the Hierarchical Example on page 920
- Schedulers for the Hierarchical Example on page 921
- Drop Profiles for the Hierarchical Example on page 922
- Scheduler Maps for the Hierarchical Example on page 922
- Applying Traffic Control Profiles for the Hierarchical Example on page 922

**Interface Sets for the Hierarchical Example**

```plaintext
[edit interfaces]
interface-set svlan-0 {
  interface ge-1/0/0 {
    unit 0;
    unit 1;
  }
}
interface-set svlan-1 {
  interface ge-1/0/0 {
    unit 2;
    unit 3;
    unit 4;
  }
}
```
Interfaces for the Hierarchical Example

The keyword to configure hierarchical schedulers is at the physical interface level, as are VLAN tagging and the VLAN IDs. In this example, the interface sets are defined by logical interfaces (units) and not outer VLAN tags. All VLAN tags in this example are customer VLAN tags.

```plaintext
[edit interface ge-1/0/0]
hierarchical-scheduler;
vlan-tagging;
unit 0 {
  vlan-id 100;
}
unit 1 {
  vlan-id 101;
}
unit 2 {
  vlan-id 102;
}
unit 3 {
  vlan-id 103;
}
unit 4 {
  vlan-id 104;
}
```

Traffic Control Profiles for the Hierarchical Example

The traffic control profiles hold parameters for levels above the queue level of the scheduler hierarchy. This section defines traffic control profiles for both the service VLAN level (logical interfaces) and the customer VLAN (VLAN tag) level.

```plaintext
[edit class-of-service traffic-control-profiles]
tcp-500m-shaping-rate {
  shaping-rate 500m;
}
tcp-svlan0 {
  shaping-rate 200m;
  guaranteed-rate 100m;
  delay-buffer-rate 300m; # This parameter is not shown in the figure
}
tcp-svlan1 {
  shaping-rate 400m;
  guaranteed-rate 300m;
  delay-buffer-rate 100m; # This parameter is not shown in the figure
}
tcp-cvlan0 {
  shaping-rate 100m;
  guaranteed-rate 60m;
  scheduler-map tcp-map-cvlan0; # This example applies scheduler maps to customer VLANs
}
tcp-cvlan1 {
  shaping-rate 100m;
  guaranteed-rate 40m;
```
Schedulers for the Hierarchical Example

The schedulers hold the information about the queues, the last level of the hierarchy. Note the consistent naming schemes applied to repetitive elements in all parts of this example.

```
[edit class-of-service schedulers]
sched-cvlan0-qx {
    priority low;
    transmit-rate 20m;
    buffer-size temporal 100ms;
    drop-profile-map loss-priority low dp-low;
    drop-profile-map loss-priority high dp-high;
}
sched-cvlan1-q0 {
    priority high;
    transmit-rate 20m;
    buffer-size percent 40;
    drop-profile-map loss-priority low dp-low;
    drop-profile-map loss-priority high dp-high;
}
sched-cvlanx-qx {
    transmit-rate percent 30;
    buffer-size percent 30;
    drop-profile-map loss-priority low dp-low;
    drop-profile-map loss-priority high dp-high;
}
sched-cvlan1-qx {
    transmit-rate 10m;
    buffer-size temporal 100ms;
    drop-profile-map loss-priority low dp-low;
    drop-profile-map loss-priority high dp-high;
}
```
Drop Profiles for the Hierarchical Example

This section configures the drop profiles for the example. For more information about drop profiles, see “Configuring RED Drop Profiles for Congestion Control” on page 854.

```junos
[edit class-of-service drop-profiles]
dp-low {
    interpolate fill-level 80 drop-probability 80;
    interpolate fill-level 100 drop-probability 100;
}
dp-high {
    interpolate fill-level 60 drop-probability 80;
    interpolate fill-level 80 drop-probability 100;
}
```

Scheduler Maps for the Hierarchical Example

This section configures the scheduler maps for the example. Each one references a scheduler configured in “Schedulers for the Hierarchical Example” on page 921.

```junos
[edit class-of-service scheduler-maps]
tcp-map-cvlan0 {
    forwarding-class voice scheduler sched-cvlan0-qx;
    forwarding-class video scheduler sched-cvlan0-qx;
    forwarding-class data scheduler sched-cvlan0-qx;
}
tcp-map-cvlan1 {
    forwarding-class voice scheduler sched-cvlan1-q0;
    forwarding-class video scheduler sched-cvlan1-qx;
    forwarding-class data scheduler sched-cvlan1-qx;
}
tcp-map-cvlanx {
    forwarding-class voice scheduler sched-cvlanx-qx;
    forwarding-class video scheduler sched-cvlanx-qx;
    forwarding-class data scheduler sched-cvlanx-qx;
}
```

Applying Traffic Control Profiles for the Hierarchical Example

This section applies the traffic control profiles to the proper levels of the hierarchy.

**NOTE:** Although a shaping rate can be applied directly to the physical interface, hierarchical schedulers must use a traffic control profile to hold this parameter, as shown in “Controlling Remaining Traffic” on page 923.

```junos
[edit class-of-service interfaces]
ge-1/0/0 {
    output-traffic-control-profile tcp-500m-shaping-rate;
    unit 0 {
        output-traffic-control-profile tcp-cvlan0;
    }
    unit 1 {
```
output-traffic-control-profile tcp-cvlan1;
}
unit 2 {
  output-traffic-control-profile tcp-cvlan2;
}
unit 3 {
  output-traffic-control-profile tcp-cvlan3;
}
unit 4 {
  output-traffic-control-profile tcp-cvlan4;
}
}
interface-set svlan0 {
  output-traffic-control-profile tcp-svlan0;
}
interface-set svlan1 {
  output-traffic-control-profile tcp-svlan1;
}

Controlling Remaining Traffic

You can configure many logical interfaces under an interface. However, only a subset of them might have a traffic control profile attached. For example, you can configure three logical interfaces (units) over the same service VLAN, but you can apply a traffic control profile specifying best-effort and voice queues to only one of the logical interface units. Traffic from the two remaining logical interfaces is considered remaining traffic. To configure transmit rate guarantees for the remaining traffic, you configure the `output-traffic-control-profile-remaining` statement specifying a guaranteed rate for the remaining traffic. Without this statement, the remaining traffic gets a default, minimal bandwidth. In the same way, the `shaping-rate` and `delay-buffer-rate` statements can be specified in the traffic control profile referenced with the `output-traffic-control-profile-remaining` statement in order to shape and provide buffering for remaining traffic.

Consider the interface shown in Figure 99 on page 924. Customer VLANs 3 and 4 have no explicit traffic control profile. However, the service provider might want to establish a shaping and guaranteed transmit rate for aggregate traffic heading for those customer VLANs. The solution is to configure and apply a traffic control profile for all remaining traffic on the interface.
This example considers the case where customer VLANs 3 and 4 have no explicit traffic control profile, yet need to establish a shaping and guaranteed transmit rate for traffic heading for those customer VLANs. The solution is to add a traffic control profile to the svlan1 interface set. This example builds on the example used in “Scheduler Hierarchy Example” on page 918 and so this does not repeat all configuration details, only those at the service VLAN level.

```
[edit class-of-service interfaces]
interface-set svlan0 {
    output-traffic-control-profile tcp-svlan0;
}
interface-set svlan1 {
    output-traffic-control-profile tcp-svlan1;
    output-traffic-control-profile-remaining tcp-svlan1-remaining; # For all remaining traffic
}

[edit class-of-service traffic-control-profiles]
tcp-svlan1 {
    shaping-rate 400m;
    guaranteed-rate 300m;
}
tcp-svlan1-remaining {
    shaping-rate 300m;
    guaranteed-rate 200m;
    scheduler-map smap-remainder; # this smap is not shown in detail
}
```

Next, consider the example shown in Figure 100 on page 925.
In this example, `ge-1/0/0` has five logical interfaces (cvlan 0, 1, 2, 3 and 4), and `svlan0`, which are covered by the interface set:

- Scheduling for the interface set `svlan0` is specified by referencing an `output-traffic-control-profile` statement, which specifies the `guaranteed-rate`, `shaping-rate`, and `delay-buffer-rate` statement values for the interface set. In this example, the output traffic control profile called `tcp-svlan0` guarantees 100 Mbps and shapes the interface set `svlan0` to 200 Mbps.

- Scheduling and queuing for remaining traffic of `svlan0` is specified by referencing an `output-traffic-control-profile-remaining` statement, which references a `scheduler-map` statement that establishes queues for the remaining traffic. The specified traffic control profile can also configure guaranteed, shaping, and delay-buffer rates for the remaining traffic. In this example, `output-traffic-control-profile-remaining tcp-svlan0-rem` references `scheduler-map smap-svlan0-rem`, which calls for a best-effort queue for remaining traffic (that is, traffic on unit 3 and unit 4, which is not classified by the `svlan0` interface set). The example also specifies a `guaranteed-rate` of 200 Mbps and a `shaping-rate` of 300 Mbps for all remaining traffic.

- Scheduling and queuing for logical interface `ge-1/0/0 unit 1` is configured “traditionally” and uses an `output-traffic-control-profile` specified for that unit. In this example, `output-traffic-control-profile tcp-ifl1` specifies scheduling and queuing for `ge-1/0/0 unit 1`.

This example does not include the `edit interfaces` configuration.

```plaintext
[edit interfaces]
interface-set {
   svlan0 {
      output-traffic-control-profile tcp-svlan0; # Guarantee & shaper for svlan0
   }
}
ge-1/0/0 {
   output-traffic-control-profile-remaining tcp-svlan0-rem
      # Unit 3 and 4 are not explicitly configured, but captured by "remaining"
      unit 1 {
         output-traffic-control-profile tcp-ifl1; # Unit 1 be & ef queues
      }
   }
```
Here is how the traffic control profiles for this example are configured:

```plaintext
[edit class-of-service traffic-control-profiles]
tcp-svlan0 {
    shaping-rate 200m;
    guaranteed-rate 100m;
}
tcp-svlan0-rem {
    shaping-rate 300m;
    guaranteed-rate 200m;
    scheduler-map smap-svlan0-rem; # This specifies queues for remaining traffic
}
tcp-ifl1 {
    scheduler-map smap-ifl1;
}
```

Finally, here are the scheduler maps and queues for the example:

```plaintext
[edit class-of-service scheduler-maps]
smap-svlan0-rem {
    forwarding-class best-effort scheduler sched-foo;
}
smap-ifl1 {
    forwarding-class best-effort scheduler sched-bar;
    forwarding-class assured-forwarding scheduler sched-baz;
}
```

The configuration for the referenced schedulers is not given for this example.

**Internal Scheduler Nodes**

A node in the hierarchy is considered internal if either of the following conditions apply:
- Any one of its children nodes has a traffic control profile configured and applied.
- You configure the `internal-node` statement.

Why would it be important to make a certain node internal? Generally, there are more resources available at the logical interface (unit) level than at the interface set level. Also, it might be desirable to configure all resources at a single level, rather than spread over several levels. The `internal-node` statement provides this flexibility. This can be a helpful configuration device when interface-set queuing without logical interfaces is used exclusively on the interface.

The `internal-node` statement can be used to raise the interface set without children to the same level as the other configured interface sets with children, allowing them to compete for the same set of resources.

In summary, using the `internal-node` statement allows statements to all be scheduled at the same level with or without children.
The following example makes the interfaces sets if-set-1 and if-set-2 internal:

```
[edit class-of-service interfaces ]
interface-set {
  if-set-1 {
    internal-node;
    output-traffic-control-profile tcp-200m-no-smap;
  }
  if-set-2 {
    internal-node;
    output-traffic-control-profile tcp-100m-no-smap;
  }
}
```

If an interface set has logical interfaces configured with a traffic control profile, then the use of the internal-node statement has no effect.

Internal nodes can specify a traffic-control-profile-remaining statement.

**PIR-only and CIR Mode**

The actual behavior of many CoS parameters, especially the shaping rate and guaranteed rate, depend on whether the physical interface is operating in PIR-only (peak information rate) or CIR (committed information rate) mode.

In PIR-only mode, one or more nodes perform shaping. The physical interface is in the PIR-only mode if no child (or grandchild) node under the port has a guaranteed rate configured.

The mode of the port is important because in PIR-only mode, the scheduling across the child nodes is in proportion to their shaping rates (PIRs) and not the guaranteed rates (CIRs). This can be important if the observed behavior is not what is anticipated.

In CIR mode, one or more nodes applies a guaranteed rate and might perform shaping. A physical interface is in CIR mode if at least one child (or grandchild) node under the physical interface can have a shaping rate configured. In addition, any child or grandchild node under the physical interface can have a shaping rate configured.

Only the guaranteed rate matters. In CIR mode, nodes that do not have a guaranteed rate configured are assumed to have a very small guaranteed rate (queuing weight).

**Priority Propagation**

SRX5600 and SRX5800 devices with input/output cards (IOCs) perform priority propagation. Priority propagation is useful for mixed traffic environments when, for example, you want to make sure that the voice traffic of one customer does not suffer due to the data traffic of another customer. Nodes and queues are always serviced in the order of their priority. The priority of a queue is decided by configuration (the default priority is low) in the scheduler. However, not all elements of hierarchical schedulers have direct priorities configured. Internal nodes, for example, must determine their priority in other ways.
The priority of any internal node is decided by:

- The highest priority of an active child (interface sets only take the highest priority of their active children)
- Whether the node is above its configured guaranteed rate (CIR) or not (this is relevant only if the physical interface is in CIR mode)

Each queue will have a configured priority and a hardware priority. The usual mapping between the configured priority and the hardware priority as shown in Table 226 on page 928.

**Table 226: Queue Priority**

<table>
<thead>
<tr>
<th>Configured Priority</th>
<th>Hardware Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strict-high</td>
<td>0</td>
</tr>
<tr>
<td>High</td>
<td>0</td>
</tr>
<tr>
<td>Medium-high</td>
<td>1</td>
</tr>
<tr>
<td>Medium-low</td>
<td>1</td>
</tr>
<tr>
<td>Low</td>
<td>2</td>
</tr>
</tbody>
</table>

In CIR mode, the priority for each internal node depends on whether the highest active child node is above or below the guaranteed rate. The mapping between the highest active child's priority and the hardware priority below and above the guaranteed rate is shown in Table 227 on page 928.

**Table 227: Internal Node Queue Priority for CIR Mode**

<table>
<thead>
<tr>
<th>Configured Priority of Highest Active Child Node</th>
<th>Hardware Priority Below Guaranteed Rate</th>
<th>Hardware Priority Above Guaranteed Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strict-high</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>High</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Medium-high</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Medium-low</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Low</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

In PIR-only mode, nodes cannot send if they are above the configured shaping rate. The mapping between the configured priority and the hardware priority is for PIR-only mode is shown in Table 228 on page 929.
Table 228: Internal Node Queue Priority for PIR-Only Mode

<table>
<thead>
<tr>
<th>Configured Priority</th>
<th>Hardware Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strict-high</td>
<td>0</td>
</tr>
<tr>
<td>High</td>
<td>0</td>
</tr>
<tr>
<td>Medium-high</td>
<td>1</td>
</tr>
<tr>
<td>Medium-low</td>
<td>1</td>
</tr>
<tr>
<td>Low</td>
<td>2</td>
</tr>
</tbody>
</table>

A physical interface with hierarchical schedulers configured is shown in Figure 101 on page 929. The configured priorities are shown for each queue at the top of the figure. The hardware priorities for each node are shown in parentheses. Each node also shows any configured shaping rate (PIR) or guaranteed rate (CIR) and whether or not the queues are above or below the CIR. The nodes are shown in one of three states: above the CIR (clear), below the CIR (dark), or in a condition where the CIR does not matter (gray).

In the figure, the strict high queue for customer VLAN 0 (cvlan 0) receives service first, even though the customer VLAN is above the configured CIR (see Table 227 on page 928 for the reason: strict-high always has hardware priority 0 regardless of CIR state). Once that queue has been drained, and the priority of the node has become 3 instead of 0 (due to the lack of strict-high traffic), the system moves on to the medium queues next (cvlan 1 and cvlan 3), draining them in a round robin fashion (empty queues lose their hardware priority). The low queue on cvlan 4 (priority 2) will be sent next, because that mode is below the CIR. Then the high queues on cvlan 0 and cvlan2 (both now with priority 3) are drained in a round-robin fashion, and finally the low queue on cvlan 0 is drained (because svlan 0 has a priority of 3).
**IOC Hardware Properties**

On SRX5600 and SRX5800 devices, two IOCs (40x1GE IOC and 4x10GE IOC) are supported on which you can configure schedulers and queues. You can configure 15 VLAN sets per Gigabit Ethernet (40x1GE IOC) port and 255 VLAN sets per 10 Gigabit Ethernet (4x10GE IOC) port. The IOC performs priority propagation from one hierarchy level to another, and drop statistics are available on the IOC per color per queue instead of just per queue.

SRX5600 and SRX5800 devices with IOCs have Packet Forwarding Engines that can support up to 512 MB of frame memory, and packets are stored in 512-byte frames. Table 229 on page 930 compares the major properties of the the Packet Forwarding Engine within the IOC.

### Table 229: Forwarding Engine Properties within 40x1GE IOC and 4x10GE IOC

<table>
<thead>
<tr>
<th>Feature</th>
<th>PFE Within 40x1GE IOC and 4x10GE IOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of usable queues</td>
<td>16,000</td>
</tr>
<tr>
<td>Number of shaped logical interfaces</td>
<td>2,000 with 8 queues each, or 4,000 with 4 queues each.</td>
</tr>
<tr>
<td>Number of hardware priorities</td>
<td>4</td>
</tr>
<tr>
<td>Priority propagation</td>
<td>Yes</td>
</tr>
<tr>
<td>Dynamic mapping</td>
<td>Yes: schedulers/port are not fixed.</td>
</tr>
<tr>
<td>Drop statistics</td>
<td>Per queue per color (PLP high, low)</td>
</tr>
</tbody>
</table>

Additionally, the IOC features also support hierarchical weighted random early detection (WRED).

The IOC supports the following hierarchical scheduler characteristics:
- Shaping at the physical interface level
- Shaping and scheduling at the service VLAN interface set level
- Shaping and scheduling at the customer VLAN logical interface level
- Scheduling at the queue level

The IOC supports the following features for scalability:
- 16,000 queues per PFE
- 4 Packet Forwarding Engines per IOC
  - 4000 schedulers at logical interface level (level 3) with 4 queues each
  - 2000 schedulers at logical interface level (level 3) with 8 queues each
  - 255 schedulers at the interface set level (level 2) per 1-port PFE on a 10-Gigabit Ethernet IOC (4x10GE IOC)
• 15 schedulers at the interface set level (level 2) per 10-port PFE on a 1-Gigabit Ethernet IOC (40x1GE IOC)
• About 400 milliseconds of buffer delay (this varies by packet size and if large buffers are enabled)
• 4 levels of priority (strict-high, high, medium, and low)

**NOTE:** The `exact` option for a `transmit-rate` (transmit-rate rate exact) is not supported on the IOCs on SRX Series devices.

The manner in which the IOC maps a queue to a scheduler depends on whether 8 queues or 4 queues are configured. By default, a scheduler at level 3 has 4 queues. Level 3 scheduler X controls queue X*4 to X*4 + 3, so that scheduler 100 (for example) controls queues 400 to 403. However, when 8 queues per scheduler are enabled, the odd-numbered schedulers are disabled, allowing twice the number of queues per subscriber as before. With 8 queues, level 3 scheduler X controls queue X*4 to X*4 + 7, so that scheduler 100 (for example) now controls queues 400 to 407.

You configure the `max-queues-per-interface` statement to set the number of queues at 4 or 8 at the FPC level of the hierarchy. Changing this statement will result in a restart of the FPC. For more information about the `max-queues-per-interface` statement, see “Example: Configuring Up to Eight Forwarding Classes” on page 841 and the JUNOS Software CLI Reference.

The IOC maps level 3 (customer VLAN) schedulers in groups to level 2 (service VLAN) schedulers. Sixteen contiguous level 3 schedulers are mapped to level 2 when 4 queues are enabled, and 8 contiguous level 3 schedulers are mapped to level 2 when 8 queues are enabled. All the schedulers in the group should use the same queue priority mapping. For example, if the queue priorities of one scheduler are high, medium, low, and low, all members of the group should have the same queue priority.

Groups at level 3 to level 2 can be mapped at any time. However, a group at level 3 can only be unmapped from a level 2 scheduler, and only if all the schedulers in the group are free. Once unmapped, a level 3 group can be remapped to any level 2 scheduler. There is no restriction on the number of level 3 groups that can be mapped to a particular level 2 scheduler. There can be 256 level 3 groups, but fragmentation of the scheduler space can reduce the number of schedulers available. In other words, there are scheduler allocation patterns that might fail even though there are free schedulers.

In contrast to level 3 to level 2 mapping, the IOC maps level 2 (service VLAN) schedulers in a fixed mode to level 1 (physical interface) schedulers. On 40-port Gigabit Ethernet IOCs, there are 16 level 1 schedulers, and 10 of these are used for the physical interfaces. There are 256 level 2 schedulers, or 16 per level 1 scheduler. A level 1 scheduler uses level schedulers X*16 through X*16 + 15. Therefore level 1 scheduler 0 uses level 2 schedulers 0 through 15, level 1 scheduler 1 uses level 2 schedulers 16 through 31, and so on. On 4-port 10 Gigabit Ethernet PICs, there is one level 1 scheduler for the physical interface, and 256 level 2 schedulers are mapped to the single level 1 scheduler.
The maximum number of level 3 (customer VLAN) schedulers that can be used is 4076 (4 queues) or 2028 (8 queues) for the 10-port Gigabit Ethernet Packet Forwarding Engine and 4094 (4 queues) or 2046 (8 queues) for the 10 Gigabit Ethernet Packet Forwarding Engine.

**WRED on the IOC**

Shaping to drop out-of-profile traffic is done on the IOC at all levels except the queue level. However, weighed random early discard (WRED) is done at the queue level with much the same result. With WRED, the decision to drop or send the packet is made before the packet is placed in the queue.

WRED shaping on the IOC involves two levels. The probabilistic drop region establishes a minimum and a maximum queue depth. Below the minimum queue depth, the drop probability is 0 (send). Above the maximum level, the drop probability is 100 (certainty).

There are four drop profiles associated with each queue. These correspond to each of four loss priorities (low, medium-low, medium-high, and high). Sixty-four sets of four drop profiles are available (32 for ingress and 32 for egress). In addition, there are eight WRED scaling profiles in each direction.

An IOC drop profile for expedited forwarding traffic might look like this:

```
[edit class-of-service drop-profiles]
drop-ef {
    fill-level 20 drop-probability 0; # Minimum Q depth
    fill-level 100 drop-probability 100; # Maximum Q depth
}
```

Note that only two fill levels can be specified for the IOC. You can configure the `interpolate` statement, but only two fill levels are used. The `delay-buffer-rate` statement in the traffic control profile determines the maximum queue size. This delay buffer rate is converted to a packet delay buffers, where one buffer is equal to 512 bytes. For example, at 10 Mbps, the IOC will allocate 610 delay buffers when the delay buffer rate is set to 250 milliseconds. The WRED threshold values are specified in terms of absolute buffer values.

The WRED scaling factor multiples all WRED thresholds (both minimum and maximum) by the value specified. There are eight values in all: 1, 2, 4, 8, 16, 32, 64, and 128. The WRED scaling factor is chosen to best match the user-configured drop profiles. This is done because the hardware supports only certain values of thresholds (all values must be a multiple of 16). So if the configured value of a threshold is 500 (for example), the multiple of 16 is 256 and the scaling factor applied is 2, making the value 512, which allows the value of 500 to be used. If the configured value of a threshold is 1500, the multiple of 16 is 752 and the scaling factor applied is 2, making the value 1504, which allows the value of 1500 to be used.

Hierarchical RED is used to support the oversubscription of the delay buffers (WRED is configured only at the queue, physical interface, and PIC level). Hierarchical RED works with WRED as follows:

- If any level accepts the packet (the queue depth is less than the minimum buffer level), this level accepts the packet.
If any level probabilistically drops the packet, then this level drops the packet.

However, these rules might lead to the accepting of packets under loaded conditions that might otherwise have been dropped. In other words, the logical interface will accept packets if the physical interface is not congested.

Due to the limits placed on shaping thresholds used in the hierarchy, there is a granularity associated with the IOCs. The shaper accuracies differ at various levels of the hierarchy, with shapers at the logical interface level (level 3) being more accurate than shapers at the interface set level (level 2) or the port level (level 1). Table 230 on page 933 shows the accuracy of the logical interface shaper at various speeds for Ethernet ports operating at 1 Gbps.

Table 230: Shaper Accuracy of 1-Gbps Ethernet at the Logical Interface Level

<table>
<thead>
<tr>
<th>Range of Logical Interface Shaper</th>
<th>Step Granularity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 4.096 Mbps</td>
<td>16 Kbps</td>
</tr>
<tr>
<td>4.096 to 8.192 Mbps</td>
<td>32 Kbps</td>
</tr>
<tr>
<td>8.192 to 16.384 Mbps</td>
<td>64 Kbps</td>
</tr>
<tr>
<td>16.384 to 32.768 Mbps</td>
<td>128 Kbps</td>
</tr>
<tr>
<td>32.768 to 65.535 Mbps</td>
<td>256 Kbps</td>
</tr>
<tr>
<td>65.535 to 131.072 Mbps</td>
<td>512 Kbps</td>
</tr>
<tr>
<td>131.072 to 262.144 Mbps</td>
<td>1024 Kbps</td>
</tr>
<tr>
<td>262.144 to 1 Gbps</td>
<td>4096 Kbps</td>
</tr>
</tbody>
</table>

Table 231 on page 933 shows the accuracy of the logical interface shaper at various speeds for Ethernet ports operating at 10 Gbps.

Table 231: Shaper Accuracy of 10-Gbps Ethernet at the Logical Interface Level

<table>
<thead>
<tr>
<th>Range of Logical Interface Shaper</th>
<th>Step Granularity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 10.24 Mbps</td>
<td>40 Kbps</td>
</tr>
<tr>
<td>10.24 to 20.48 Mbps</td>
<td>80 Kbps</td>
</tr>
<tr>
<td>10.48 to 40.96 Mbps</td>
<td>160 Kbps</td>
</tr>
<tr>
<td>40.96 to 81.92 Mbps</td>
<td>320 Kbps</td>
</tr>
<tr>
<td>81.92 to 165.84 Mbps</td>
<td>640 Kbps</td>
</tr>
<tr>
<td>165.84 to 327.68 Mbps</td>
<td>1280 Kbps</td>
</tr>
<tr>
<td>327.68 to 655.36 Mbps</td>
<td>2560 Kbps</td>
</tr>
</tbody>
</table>
Table 231: Shaper Accuracy of 10-Gbps Ethernet at the Logical Interface Level (continued)

<table>
<thead>
<tr>
<th>Range of Logical Interface Shaper</th>
<th>Step Granularity</th>
</tr>
</thead>
<tbody>
<tr>
<td>655.36 to 2611.2 Mbps</td>
<td>10240 Kbps</td>
</tr>
<tr>
<td>2611.2 to 5222.4 Mbps</td>
<td>20480 Kbps</td>
</tr>
<tr>
<td>5222.4 to 10 Gbps</td>
<td>40960 Kbps</td>
</tr>
</tbody>
</table>

Table 232 on page 934 shows the accuracy of the interface set shaper at various speeds for Ethernet ports operating at 1 Gbps.

Table 232: Shaper Accuracy of 1-Gbps Ethernet at the Interface Set Level

<table>
<thead>
<tr>
<th>Range of Interface Set Shaper</th>
<th>Step Granularity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 20.48 Mbps</td>
<td>80 Kbps</td>
</tr>
<tr>
<td>20.48 Mbps to 81.92 Mbps</td>
<td>320 Kbps</td>
</tr>
<tr>
<td>81.92 Mbps to 327.68 Mbps</td>
<td>1.28 Mbps</td>
</tr>
<tr>
<td>327.68 Mbps to 1 Gbps</td>
<td>20.48 Mbps</td>
</tr>
</tbody>
</table>

Table 233 on page 934 shows the accuracy of the interface set shaper at various speeds for Ethernet ports operating at 10 Gbps.

Table 233: Shaper Accuracy of 10-Gbps Ethernet at the Interface Set Level

<table>
<thead>
<tr>
<th>Range of Interface Set Shaper</th>
<th>Step Granularity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 128 Mbps</td>
<td>500 Kbps</td>
</tr>
<tr>
<td>128 Mbps to 512 Mbps</td>
<td>2 Mbps</td>
</tr>
<tr>
<td>512 Mbps to 2.048 Gbps</td>
<td>8 Mbps</td>
</tr>
<tr>
<td>2.048 Gbps to 10 Gbps</td>
<td>128 Mbps</td>
</tr>
</tbody>
</table>

Table 234 on page 934 shows the accuracy of the physical port shaper at various speeds for Ethernet ports operating at 1 Gbps.

Table 234: Shaper Accuracy of 1-Gbps Ethernet at the Physical Port Level

<table>
<thead>
<tr>
<th>Range of Physical Port Shaper</th>
<th>Step Granularity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 64 Mbps</td>
<td>250 Kbps</td>
</tr>
</tbody>
</table>
Table 234: Shaper Accuracy of 1-Gbps Ethernet at the Physical Port Level (continued)

<table>
<thead>
<tr>
<th>Range of Physical Port Shaper</th>
<th>Step Granularity</th>
</tr>
</thead>
<tbody>
<tr>
<td>64 Mbps to 256 Mbps</td>
<td>1 Mbps</td>
</tr>
<tr>
<td>256 Mbps to 1 Gbps</td>
<td>4 Mbps</td>
</tr>
</tbody>
</table>

Table 235 on page 935 shows the accuracy of the physical port shaper at various speeds for Ethernet ports operating at 10 Gbps.

Table 235: Shaper Accuracy of 10-Gbps Ethernet at the Physical Port Level

<table>
<thead>
<tr>
<th>Range of Physical Port Shaper</th>
<th>Step Granularity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 640 Mbps</td>
<td>2.5 Mbps</td>
</tr>
<tr>
<td>640 Mbps to 2.56 Gbps</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>2.56 Gbps to 10 Gbps</td>
<td>40 Mbps</td>
</tr>
</tbody>
</table>

For more information about configuring RED drop profiles, see “Configuring RED Drop Profiles for Congestion Control” on page 854.

**MDRR on the IOC**

The guaranteed rate (CIR) at the interface set level is implemented by using modified deficit round-robin (MDRR). The IOC hardware provides four levels of strict priority. There is no restriction on the number of queues for each priority. MDRR is used among queues of the same priority. Each queue has one priority when it is under the guaranteed rate and another priority when it is over the guaranteed rate but still under the shaping rate (PIR). The IOC hardware implements the priorities with 256 service profiles. Each service profile assigns eight priorities for eight queues. One set is for logical interfaces under the guaranteed rate and another set is for logical interfaces over the guaranteed rate but under the shaping rate. Each service profile is associated with a group of 16 level 3 schedulers, so there is a unique service profile available for all 256 groups at level 3, giving 4,096 logical interfaces.

JUNOS Software provides three priorities for traffic under the guaranteed rate and one reserved priority for traffic over the guaranteed rate that is not configurable. JUNOS Software provides three priorities when there is no guaranteed rate configured on any logical interface.

The relationship between JUNOS Software priorities and the IOC hardware priorities below and above the guaranteed rate (CIR) is shown in Table 236 on page 936.
### Table 236: JUNOS Priorities Mapped to IOC Hardware Priorities

<table>
<thead>
<tr>
<th>JUNOS Software Priority</th>
<th>IOC Hardware Priority Below Guaranteed Rate</th>
<th>IOC Hardware Priority Above Guaranteed Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strict-high</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Medium-high</td>
<td>Medium-high</td>
<td>Low</td>
</tr>
<tr>
<td>Medium-low</td>
<td>Medium-high</td>
<td>Low</td>
</tr>
<tr>
<td>Low</td>
<td>Medium-low</td>
<td>Low</td>
</tr>
</tbody>
</table>

The JUNOS Software parameters are set in the scheduler map:

```plaintext
[edit class-of-service schedulers]
best-effort-scheduler {
  transmit-rate percent 30; # if no shaping rate
  buffer-size percent 30;
  priority high;
}
expedited-forwarding-scheduler {
  transmit-rate percent 40; # if no shaping rate
  buffer-size percent 40;
  priority strict-high;
}
```

**NOTE:** The use of both shaping rate and a guaranteed rate at the interface set level (level 2) is not supported.

MDRR is provided at three levels of the scheduler hierarchy of the IOC with a granularity of 1 through 255. There are 64 MDRR profiles at the queue level, 16 at the interface set level, and 32 at the physical interface level.

Queue transmit rates are used for queue-level MDRR profile weight calculation. The queue MDRR weight is calculated differently based on the mode set for sharing excess bandwidth. If you configure the `equal` option for excess bandwidth, then the queue MDRR weight is calculated as:

\[
\text{Queue weight} = \frac{(255 \times \text{Transmit-rate-percentage})}{100}
\]

If you configure the `proportional` option for excess bandwidth, which is the default, then the queue MDRR weight is calculated as:

\[
\text{Queue weight} = \frac{\text{Queue-transmit-rate}}{\text{Queue-base-rate}}, \text{ where}
\]

\[
\text{Queue-transmit-rate} = \frac{(\text{Logical-interface-rate} \times \text{Transmit-rate-percentage})}{100}, \text{ and}
\]

\[
\text{Queue-base-rate} = \frac{\text{Excess-bandwidth-proportional-rate}}{255}
\]
To configure the way that the IOC should handle excess bandwidth, configure the `excess-bandwidth-share` statement at the `[edit interface-set interface-set-name]` hierarchy level. By default, the excess bandwidth is set to `proportional` with a default value of 32.64 Mbps. In this mode, the excess bandwidth is shared in the ratio of the logical interface shaping rates. If set to `equal`, the excess bandwidth is shared equally among the logical interfaces.

This example sets the excess bandwidth sharing to proportional at a rate of 100 Mbps with a shaping rate of 80 Mbps.

```
[edit interface-set example-interface-set]
excess-bandwidth-share proportional 100m;
output-traffic-control-profile PIR-80Mbps;
```

Shaping rates established at the logical interface level are used to calculate the MDRR weights used at the interface set level. The 16 MDRR profiles are set to initial values, and the closest profile with rounded values is chosen. By default, the physical port MDRR weights are preset to the full bandwidth on the interface.

### Configuring Excess Bandwidth Sharing

When using the IOC (40x1GE IOC or 4x10GE IOC) on an SRX Series device, there are circumstances when you should configure excess bandwidth sharing and minimum logical interface shaping. This section details some of the guidelines for configuring excess bandwidth sharing.

- Excess Bandwidth Sharing and Minimum Logical Interface Shaping on page 937
- Selecting Excess Bandwidth Sharing Proportional Rates on page 938
- Mapping Calculated Weights to Hardware Weights on page 938
- Allocating Weight with Only Shaping Rates or Unshaped Logical Interfaces on page 939
- Sharing Bandwidth Among Logical Interfaces on page 940

### Excess Bandwidth Sharing and Minimum Logical Interface Shaping

The default excess bandwidth sharing proportional rate is 32.65 Mbps (128 Kbps x 255). In order to have better weighed fair queuing (WFQ) accuracy among queues, the shaping rate configured should be larger than the excess bandwidth sharing proportional rate. Some examples are shown in Table 237 on page 937.

<table>
<thead>
<tr>
<th>Shaping Rate</th>
<th>Configured Queue Transmit Rate</th>
<th>WFQ Weight</th>
<th>Total Weights</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Mbps</td>
<td>(30, 40, 25, 5)</td>
<td>(22, 30, 20, 4)</td>
<td>76</td>
</tr>
<tr>
<td>35 Mbps</td>
<td>(30, 40, 25, 5)</td>
<td>(76, 104, 64, 13)</td>
<td>257</td>
</tr>
<tr>
<td>40 Mbps</td>
<td>(30, 40, 25, 5)</td>
<td>(76, 104, 64, 13)</td>
<td>257</td>
</tr>
</tbody>
</table>
With a 10-Mbps shaping rate, the total weights are 76. This is divided among the four queues according to the configured transmit rate. Note that when the shaping rate is larger than the excess bandwidth sharing proportional rate of 32.65 Mbps, the total weight on the logical interface is 257 and the WFQ accuracy will be the same.

**Selecting Excess Bandwidth Sharing Proportional Rates**

To determine a good excess bandwidth-sharing proportional rate to configure, choose the largest CIR (guaranteed rate) among all the logical interfaces (units). If the logical units have PIRs (shaping rates) only, then choose the largest PIR rate. However, this is not ideal if a single logical interface has a large WRR rate. This method can skew the distribution of traffic across the queues of the other logical interfaces. To avoid this issue, set the excess bandwidth-sharing proportional rate to a lower value on the logical interfaces where the WRR rates are concentrated. This improves the bandwidth sharing accuracy among the queues on the same logical interface. However, the excess bandwidth sharing for the logical interface with the larger WRR rate is no longer proportional.

As an example, consider five logical interfaces on the same physical port, each with four queues, all with only PIRs configured and no CIRs. The WRR rate is the same as the PIR for the logical interface. The excess bandwidth is shared proportionally with a rate of 40 Mbps. The traffic control profiles for the logical interfaces are shown in Table 238 on page 938.

**Table 238: Example Shaping Rates and WFQ Weights**

<table>
<thead>
<tr>
<th>Shaping Rate</th>
<th>Configured Queue Transmit Rate</th>
<th>WFQ Weight</th>
<th>Total Weights</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Unit 0) 10 Mbps</td>
<td>(95, 0, 0, 5)</td>
<td>(60, 0, 0, 3)</td>
<td>63</td>
</tr>
<tr>
<td>(Unit 1) 20 Mbps</td>
<td>(25, 25, 25, 25)</td>
<td>(32, 32, 32, 32)</td>
<td>128</td>
</tr>
<tr>
<td>(Unit 2) 40 Mbps</td>
<td>(40, 30, 20, 10)</td>
<td>(102, 77, 51, 26)</td>
<td>255</td>
</tr>
<tr>
<td>(Unit 3) 200 Mbps</td>
<td>(70, 10, 10, 10)</td>
<td>(179, 26, 26, 26)</td>
<td>255</td>
</tr>
<tr>
<td>(Unit 4) 2 Mbps</td>
<td>(25, 25, 25, 25)</td>
<td>(5, 5, 5, 5)</td>
<td>20</td>
</tr>
</tbody>
</table>

Even though the maximum transmit rate for the queue on logical interface unit 3 is 200 Mbps, the excess bandwidth-sharing proportional rate is kept at a much lower value. Within a logical interface, this method provides a more accurate distribution of weights across queues. However, the excess bandwidth is now shared equally between unit 2 and unit 3 (total weights = 255).

**Mapping Calculated Weights to Hardware Weights**

The calculated weight in a traffic control profile is mapped to hardware weight, but the hardware only supports a limited WFQ profile. The weights are rounded to the nearest hardware weight according to the values in Table 239 on page 939.
Table 239: Rounding Configured Weights to Hardware Weights

<table>
<thead>
<tr>
<th>Traffic Control Profile Number</th>
<th>Number of Traffic Control Profiles</th>
<th>Weights</th>
<th>Maximum Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>1–16</td>
<td>16</td>
<td>1–16 (interval of 1)</td>
<td>50.00%</td>
</tr>
<tr>
<td>17–29</td>
<td>13</td>
<td>18–42 (interval of 2)</td>
<td>6.25%</td>
</tr>
<tr>
<td>30–35</td>
<td>6</td>
<td>45–60 (interval of 3)</td>
<td>1.35%</td>
</tr>
<tr>
<td>36–43</td>
<td>8</td>
<td>64–92 (interval of 4)</td>
<td>2.25%</td>
</tr>
<tr>
<td>44–49</td>
<td>6</td>
<td>98–128 (interval of 6)</td>
<td>3.06%</td>
</tr>
<tr>
<td>50–56</td>
<td>7</td>
<td>136–184 (interval of 8)</td>
<td>3.13%</td>
</tr>
<tr>
<td>57–62</td>
<td>6</td>
<td>194–244 (interval of 10)</td>
<td>2.71%</td>
</tr>
<tr>
<td>63–63</td>
<td>1</td>
<td>255–255 (interval of 11)</td>
<td>2.05%</td>
</tr>
</tbody>
</table>

From the table, as an example, the calculated weight of 18.9 is mapped to a hardware weight of 18, because 18 is closer to 18.9 than 20 (an interval of 2 applies in the range 18–42).

Allocating Weight with Only Shaping Rates or Unshaped Logical Interfaces

Logical interfaces with only shaping rates (PIRs) or unshaped logical interfaces (units) are given a weight of 10. A logical interface with a small guaranteed rate (CIR) might get an overall weight less than 10. In order to allocate a higher share of the excess bandwidth to logical interfaces with a small guaranteed rate in comparison to the logical interfaces with only shaping rates configured, a minimum weight of 20 is given to the logical interfaces with guaranteed rates configured.

For example, consider a logical interface configuration with five units, as shown in Table 240 on page 939.

Table 240: Allocating Weights with PIR and CIR on Logical Interfaces

<table>
<thead>
<tr>
<th>Logical Interface (Unit)</th>
<th>Traffic Control Profile</th>
<th>WRR Percentages</th>
<th>Weights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit 1</td>
<td>PIR 100 Mbps</td>
<td>95, 0, 0, 5</td>
<td>10, 1, 1, 1</td>
</tr>
<tr>
<td>Unit 2</td>
<td>CIR 20 Mbps</td>
<td>25, 25, 25, 25</td>
<td>64, 64, 64, 64</td>
</tr>
<tr>
<td>Unit 3</td>
<td>PIR 40 Mbps, CIR 20 Mbps</td>
<td>50, 30, 15, 5</td>
<td>128, 76, 38, 13</td>
</tr>
<tr>
<td>Unit 4</td>
<td>Unshaped</td>
<td>95, 0, 0, 5</td>
<td>10, 1, 1, 1</td>
</tr>
<tr>
<td>Unit 5</td>
<td>CIR 1 Mbps</td>
<td>95, 0, 0, 5</td>
<td>10, 1, 1, 1</td>
</tr>
</tbody>
</table>
The weights for these units are calculated as follows:

- Select the excess bandwidth-sharing proportional rate to be the maximum CIR among all the logical interfaces: 20 Mbps (unit 2).
- Unit 1 has a PIR and unit 4 is unshaped. The weight for these units is 10.
- The weight for unit 1 queue 0 is 9.5 (10 x 95%), which translates to a hardware weight of 10.
- The weight for unit 1 queue 1 is 0 (0 x 0%), but although the weight is zero, a weight of 1 is assigned to give minimal bandwidth to queues with zero WRR.
- Unit 5 has a very small CIR (1 Mbps), and a weight of 20 is assigned to units with a small CIR.
- The weight for unit 5 queue 0 is 19 (20 x 95%), which translates to a hardware weight of 18.
- Unit 3 has a CIR of 20 Mbps, which is the same as the excess bandwidth-sharing proportional rate, so it has a total weight of 255.
- The weight for unit 3 queue 0 is 127.5 (255 x 50%), which translates to a hardware weight of 128.

**Sharing Bandwidth Among Logical Interfaces**

As a simple example showing how bandwidth is shared among the logical interfaces, assume that all traffic is sent on queue 0. Assume also that there is a 40-Mbps load on all of the logical interfaces. Configuration details are shown in Table 241 on page 940.

<table>
<thead>
<tr>
<th>Logical Interface (Unit)</th>
<th>Traffic Control Profile</th>
<th>WRR Percentages</th>
<th>Weights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit 1</td>
<td>PIR 100 Mbps</td>
<td>95, 0, 0, 5</td>
<td>10, 1, 1, 1</td>
</tr>
<tr>
<td>Unit 2</td>
<td>CIR 20 Mbps</td>
<td>25, 25, 25, 25</td>
<td>64, 64, 64, 64</td>
</tr>
<tr>
<td>Unit 3</td>
<td>PIR 40 Mbps, CIR 20 Mbps</td>
<td>50, 30, 15, 5</td>
<td>128, 76, 38, 13</td>
</tr>
<tr>
<td>Unit 4</td>
<td>Unshaped</td>
<td>95, 0, 0, 5</td>
<td>10, 1, 1, 1</td>
</tr>
</tbody>
</table>

1. When the port is shaped at 40 Mbps, because units 2 and 3 have a guaranteed rate (CIR) configured, both units 2 and 3 get 20 Mbps of shared bandwidth.

2. When the port is shaped at 100 Mbps, because units 2 and 3 have a guaranteed rate (CIR) configured, each of them can transmit 20 Mbps. On units 1, 2, 3, and 4, the 60 Mbps of excess bandwidth is shaped according to the values shown in Table 242 on page 941.
Table 242: First Example of Bandwidth Sharing

<table>
<thead>
<tr>
<th>Logical Interface (Unit)</th>
<th>Calculation</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( \frac{10}{10 + 64 + 128 + 10} \times 60 \text{ Mbps} )</td>
<td>2.83 Mbps</td>
</tr>
<tr>
<td>2</td>
<td>( \frac{64}{10 + 64 + 128 + 10} \times 60 \text{ Mbps} )</td>
<td>18.11 Mbps</td>
</tr>
<tr>
<td>3</td>
<td>( \frac{128}{10 + 64 + 128 + 10} \times 60 \text{ Mbps} )</td>
<td>36.22 Mbps</td>
</tr>
<tr>
<td>4</td>
<td>10 ((10 + 64 + 128 + 10) \times 60 \text{ Mbps})</td>
<td>2.83 Mbps</td>
</tr>
</tbody>
</table>

However, unit 3 only has 20 Mbps extra (PIR and CIR) configured. This means that the leftover bandwidth of 16.22 Mbps (36.22 Mbps – 20 Mbps) is shared among units 1, 2, and 4. This is shown in Table 243 on page 941.

Table 243: Second Example of Bandwidth Sharing

<table>
<thead>
<tr>
<th>Logical Interface (Unit)</th>
<th>Calculation</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( \frac{10}{10 + 64 + 128 + 10} \times 16.22 \text{ Mbps} )</td>
<td>1.93 Mbps</td>
</tr>
<tr>
<td>2</td>
<td>( \frac{64}{10 + 64 + 128 + 10} \times 16.22 \text{ Mbps} )</td>
<td>12.36 Mbps</td>
</tr>
<tr>
<td>4</td>
<td>10 ((10 + 64 + 128 + 10) \times 16.22 \text{ Mbps})</td>
<td>1.93 Mbps</td>
</tr>
</tbody>
</table>

Finally, Table 244 on page 941 shows the resulting allocation of bandwidth among the logical interfaces when the port is configured with a 100-Mbps shaping rate.

Table 244: Final Example of Bandwidth Sharing

<table>
<thead>
<tr>
<th>Logical Interface (Unit)</th>
<th>Calculation</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2.83 Mbps + 1.93 Mbps</td>
<td>4.76 Mbps</td>
</tr>
<tr>
<td>2</td>
<td>20 Mbps + 18.11 Mbps + 12.36 Mbps</td>
<td>50.47 Mbps</td>
</tr>
<tr>
<td>3</td>
<td>20 Mbps + 20 Mbps</td>
<td>40 Mbps</td>
</tr>
<tr>
<td>4</td>
<td>2.83 Mbps + 1.93 Mbps</td>
<td>4.76 Mbps</td>
</tr>
</tbody>
</table>

Verifying a CoS Configuration

To verify a CoS configuration on a Services Router, perform the tasks relevant to your CoS configuration from the following:

- Verifying Multicast Session Announcements on page 942
- Verifying a Virtual Channel Configuration on page 942
Verifying Multicast Session Announcements

**Purpose**
Verify that the Services Router is listening to the appropriate groups for multicast Session Announcement Protocol (SAP) session announcements.

**Action**
From the CLI, enter the `show sap listen` command.

**Sample Output**
```
user@host> show sap listen
Group Address   Port
224.2.127.254   9875
```

**Meaning**
The output shows a list of the group addresses and ports that SAP and SDP listen on. Verify the following information:
- Each group address configured, especially the default 224.2.127.254, is listed.
- Each port configured, especially the default 9875, is listed.

**Related Topics**
For a complete description of the `show sap listen` command and output, see the *Junos Routing Protocols and Policies Command Reference*.

Verifying a Virtual Channel Configuration

**Purpose**
Verify the virtual channel configuration on a logical interface. Verify the class-of-service (CoS) configuration associated with an interface on a Services Router.

**Action**
From the CLI, enter the `show class-of-service virtual-channel` command.

**Sample Output**
```
user@host> show class-of-service virtual-channel
Virtual channel: vc-1 Index: 1
```

**Meaning**
Verify that the name of the configured virtual channel is displayed in the output.

**Related Topics**
For a complete description of the `show class-of-service virtual-channel` command and output, see the *Junos System Basics and Services Command Reference*.
Verifying a Virtual Channel Group Configuration

**Purpose**  Verify the virtual channel group configuration on a logical interface. Verify the class-of-service (CoS) configuration associated with an interface on a Services Router.

**Action**  From the CLI, enter the `show class-of-service virtual-channel-group` command.

**Sample Output**  
```
user@host> show class-of-service virtual-channel-group
Virtual channel group: vc-group, Index: 16321    Virtual channel: vc-1
    Scheduler map: sc-map
```

**Meaning**  Verify that the name of the configured virtual channel group is displayed in the output.

**Related Topics**  For a complete description of the `show class-of-service virtual-channel-group` command and output, see the Junos System Basics and Services Command Reference.

Verifying an Adaptive Shaper Configuration

**Purpose**  Verify the adaptive shaper trigger point and its associated transmit rate. Verify the class-of-service (CoS) configuration associated with an interface on a Services Router.

**Action**  From the CLI, enter the `show class-of-service adaptive-shaper` and `show class-of-service interface t1-0/0/2` commands.

**Sample Output**  
```
user@host> show class-of-service adaptive-shaper
Adaptive shaper: fr-shaper, Index: 35320
    Trigger type      Shaping rate
        BECN          64000 bps

user@host> show class-of-service interface t1-0/0/2
Physical interface: t1-0/0/2, Index: 137
    Queues supported: 8, Queues in use: 4
    Scheduler map: <default>, Index: 2

Logical interface: t1-0/0/2.0, Index: 69
Object       Name                Type   Index
Adaptive-shaper fr-shaper 35320
Classifier    ipprec-compatibility ip  11
```

**Meaning**  Verify the following information:

- The trigger type and shaping rate are consistent with the configured adaptive shaper.
- The adaptive shaper applied to the logical interface is displayed under Name.
Related Topics For a complete description of the `show class-of-service adaptive-shaper` and `show class-of-service interface` commands and output, see the Junos System Basics and Services Command Reference.

**Displaying CoS Tunnel Configurations**

**Purpose** Verify the configuration of the CoS tunnel queuing on a Services Router. You can analyze the flow of traffic by displaying the entire configuration. The following output is specific to CoS queuing configuration.

**Action** From the CLI on Router A and B, enter the following `show` commands.

**Router B**
```
user@host# show interfaces gr-0/0/0
per-unit-scheduler
  unit 0 {
    tunnel
      source 70.0.0.1;
      destination 70.0.0.2;
      family inet {
        address 10.80.0.1/24;
      }
  }
}

user@host# show class-of-service interfaces gr-0/0/0
unit 0 {
  scheduler-map SMAP;
  shaping-rate 200m;
}
```

**Router A**
```
user@host# show chassis
  fpc 0 {
    pic 0 {
      tunnel-queuing
    }
  }
[edit]
```

**Verifying a CoS GRE Tunnel Queuing Configuration**

**Purpose** Verify that the Services Router is configured properly for tunnel configuration.

**Action** From the CLI, enter the `show interfaces queue gr-0/0/0.0` command.

**NOTE:** If you enter `gr-0/0/0` only, queue information for all tunnels is displayed. If you enter `gr-0/0/0 unit logical_unit_number` queue information for the specific tunnel is displayed.
### Sample Output

```bash
user@host> show interfaces queue gr-0/0/0.0
Logical interface gr-0/0/0.0 (Index 68) (SNMP ifIndex 112)
Forwarding classes: 8 supported, 4 in use
Egress queues: 8 supported, 4 in use Burst size: 0
```

Queue: 0, Forwarding classes: VOICE

```
Queueed:
   Packets  : 7117734  7998 pps
   Bytes     : 512476848 4606848 bps
Transmitted:
   Packets  : 4548146  3459 pps
   Bytes     : 327466512 1992912 bps
   Tail-dropped packets : 0  0 pps
   RED-dropped packets  : 2569421 4537 pps
   Low           : 0  0 pps
   Medium-low    : 0  0 pps
   Medium-high   : 0  0 pps
   High          : 2569421 4537 pps
   RED-dropped bytes : 184998312 2613640 bps
   Low           : 0  0 bps
   Medium-low    : 0  0 bps
   Medium-high   : 0  0 bps
   High          : 184998312 2613640 bps
```

Queue: 1, Forwarding classes: GOLD

```
Queueed:
   Packets  : 117600  0 pps
   Bytes     : 8467200  0 bps
Transmitted:
   Packets  : 102435  0 pps
   Bytes     : 7375320  0 bps
   Tail-dropped packets : 0  0 pps
   RED-dropped packets  : 15165  0 pps
   Low           : 0  0 pps
   Medium-low    : 0  0 pps
   Medium-high   : 0  0 pps
   High          : 15165  0 pps
   RED-dropped bytes : 1091880  0 bps
   Low           : 0  0 bps
   Medium-low    : 0  0 bps
   Medium-high   : 0  0 bps
   High          : 1091880  0 bps
```

Queue: 2, Forwarding classes: SILVER

```
Queueed:
   Packets  : 0  0 pps
   Bytes     : 0  0 bps
Transmitted:
   Packets  : 0  0 pps
   Bytes     : 0  0 bps
   Tail-dropped packets : 0  0 pps
   RED-dropped packets  : 0  0 pps
   Low           : 0  0 pps
   Medium-low    : 0  0 pps
   Medium-high   : 0  0 pps
   High          : 0  0 pps
   RED-dropped bytes : 0  0 bps
   Low           : 0  0 bps
   Medium-low    : 0  0 bps
   Medium-high   : 0  0 bps
   High          : 0  0 bps
```

Queue: 3, Forwarding classes: BRONZE

```
Queueed:
   Packets  : 0  0 pps
   Bytes     : 0  0 bps
```

---

**Verifying a CoS GRE Tunnel Queuing Configuration**

---

945
Meaning The output lists the egress queues and the corresponding forwarding classes. Assuming that traffic is correctly classified using appropriate classifiers on the ingress port, verify the traffic flow in various queues.

Related Topics For a complete description of the `show interfaces queue` command and output, see the Junos Interfaces Command Reference.

**Verifying a CoS IP-IP Tunnel Configuration**

**Purpose** Verify that the Services Router is configured properly for tunnel configuration.

**Action** From the CLI, enter the `show interfaces queue ip-0/0/0.0` command.

**NOTE:** If you enter `ip-0/0/0` only, queue information for all tunnels is displayed. If you enter `ip-0/0/0 unit logical_unit_number` queue information for the specific tunnel is displayed.

**Sample Output**

```
user@host> show interfaces queue ip-0/0/0.0
Logical interface ip-0/0/0.0 (Index 70) (SNMP ifIndex 56
Forwarding classes: 8 supported, 4 in use
Egress queues: 8 supported, 4 in use
Burst size: 0
Queue: 0, Forwarding classes: q0
Queued:
   Packets: 38802710 22687 pps
   Bytes: 10942364220 51183344 bps
```

Meaning The output lists the egress queues and the corresponding forwarding classes. Assuming that traffic is correctly classified using appropriate classifiers on the ingress port, verify the traffic flow in various queues.
Related Topics For a complete description of the show interfaces queue command and output, see the Junos Interfaces Command Reference.

Configuring Class of Service for IPv6 Traffic

The following topics describe class-of-service functions for IPv6 traffic and provide examples on how to configure classifiers and rewrite rules that use IPv6 DiffServ code points:

- Overview of Class-of-Service Functions for IPv6 Traffic on page 947
- Configuring and Applying a DSCP IPv6 BA Classifier on page 949
- Configuring DSCP IPv6 Rewrite Rules on page 953

Overview of Class-of-Service Functions for IPv6 Traffic

Class-of-service (CoS) processing for IPv6 traffic uses the IPv6 DiffServ code point (DSCP) value. The IPv6 DSCP value is the first six bits in the 8-bit Traffic Class field of the IPv6 header. The DSCP value is used to determine the behavior aggregate (BA) classification for the packet entering the network device. You use classifier rules to map the DSCP code points to a forwarding class and packet loss priority. You use rewrite rules to map the forwarding class and packet loss priority back to DSCP values on packets exiting the device.

Figure 102 on page 947 shows the components of the CoS features for SRX Series and J Series devices, illustrating the sequence in which they interact.

Figure 102: Packet Flow Through an SRX Series or J Series Device

NOTE: Not all features are supported on all SRX Series devices. For information on the set of CoS features supported for your Juniper Networks device, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.
CoS components perform the following operations:

1. BA classifier rules map DSCP code points to a forwarding class and loss priority. The forwarding class and loss priority determine the per-hop behavior of the packet throughout the system. The forwarding class associates a packet with an outbound transmission queue. Loss priority affects the scheduling of a packet without affecting the relative ordering of packets. BA classification is a simple way that “downstream” nodes can honor the CoS objectives that were encoded “upstream”.

   See “Configuring and Applying a DSCP IPv6 BA Classifier” on page 949.

2. Multifield classifier rules overwrite the initial forwarding class and loss priority determination read by the BA classifier rule. You typically use multifield classifier rules on nodes close to the content origin, where a packet might not have been encoded with the desired DSCP values in the headers. A multifield classifier rule assigns packets to a forwarding class and assigns a packet loss priority based on filters, such as source IP, destination IP, port, or application.

   See “Configuring and Applying a Firewall Filter for a Multifield Classifier” on page 835.

3. Input policers meter traffic to see if traffic flow exceeds its service level. Policers might discard, change the forwarding class and loss priority, or set the packet loss priority bit of a packet. A packet for which the packet loss priority bit is set has an increased probability of being dropped during congestion.

   See “Configuring a Policer for a Firewall Filter” on page 834.

4. Scheduler maps are applied to interfaces and associate the outgoing packets with a scheduler and a forwarding class.

   The scheduler manages the output transmission queue, including:

   - Buffer size—Defines the period for which a packet is stored during congestion.
   - Scheduling priority and transmit rate—Determine the order in which a packet is transmitted.
   - Drop profile—Defines how aggressively to drop a packet that is using a particular scheduler.

   See “Configuring Schedulers” on page 857.

5. Output policers meter traffic and might change the forwarding class and loss priority of a packet if a traffic flow exceeds its service level.

   See “Configuring a Policer for a Firewall Filter” on page 834.

6. Rewrite rules map forwarding class and packet loss priority to DSCP values. You typically use rewrite rules in conjunction with multifield classifier rules close to the content origin; or when the device is at the border of a network and must alter the code points to meet the policies of the targeted peer.

   See “Configuring DSCP IPv6 Rewrite Rules” on page 953.
Only BA classification rules and rewrite rules require special consideration to support CoS for IPv6 traffic. The program logic for the other CoS features is not sensitive to differences between IPv4 and IPv6 traffic.

**Configuring and Applying a DSCP IPv6 BA Classifier**

A behavior aggregate (BA) classifier rule maps DSCP code points to a forwarding class and loss priority. The forwarding class and loss priority determine the per-hop behavior of the packet throughout the system. The forwarding class associates a packet with an outbound transmission queue. Loss priority affects the scheduling of a packet without affecting the relative ordering of packets.

BA classification can be applied within one DiffServ domain or between two domains, where each domain honors the CoS results generated by the other domain. Table 245 on page 949 shows the mapping for the default DSCP IPv6 BA classifier.

<table>
<thead>
<tr>
<th>Code Points</th>
<th>DSCP IPv6 Alias</th>
<th>Forwarding Class</th>
<th>Packet Loss Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>101110</td>
<td>ef</td>
<td>expedited-forwarding</td>
<td>low</td>
</tr>
<tr>
<td>001010</td>
<td>af11</td>
<td>assured-forwarding</td>
<td>low</td>
</tr>
<tr>
<td>001100</td>
<td>af12</td>
<td>assured-forwarding</td>
<td>high</td>
</tr>
<tr>
<td>001110</td>
<td>af13</td>
<td>assured-forwarding</td>
<td>high</td>
</tr>
<tr>
<td>010010</td>
<td>af21</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>010100</td>
<td>af22</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>010110</td>
<td>af25</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>011010</td>
<td>af31</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>011100</td>
<td>af32</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>011110</td>
<td>af33</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>100010</td>
<td>af41</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>100100</td>
<td>af42</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>100110</td>
<td>af43</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>000000</td>
<td>be</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>001000</td>
<td>cs1</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>010000</td>
<td>cs2</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>011000</td>
<td>cs3</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>100000</td>
<td>cs4</td>
<td>best-effort</td>
<td>low</td>
</tr>
</tbody>
</table>
You can use the CLI show command to display the settings for the CoS classifiers. The following command shows the settings for the default DSCP IPv6 classifier:

```
user@host# show class-of-service classifier type dscp-ipv6
Classifier: dscp-ipv6-default, Code point type: dscp-ipv6, Index: 8
<table>
<thead>
<tr>
<th>Code point</th>
<th>Forwarding class</th>
<th>Loss priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>000001</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>000010</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>000011</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>000100</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>000101</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>011011</td>
<td>best-effort</td>
<td>low</td>
</tr>
</tbody>
</table>

Classifier: dscp-ipv6-compatibility, Code point type: dscp-ipv6, Index: 9
<table>
<thead>
<tr>
<th>Code point</th>
<th>Forwarding class</th>
<th>Loss priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>000001</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>000010</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>000011</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>000100</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>000101</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>000110</td>
<td>best-effort</td>
<td>low</td>
</tr>
<tr>
<td>000111</td>
<td>best-effort</td>
<td>low</td>
</tr>
</tbody>
</table>
```

**NOTE:** The predefined classifier named `dscp-ipv6-compatibility` maps all code points loss priority to low. It maps 110000 and 111000 (typically seen in network control packets) to the network-control class and all other code points to the best-effort class. The `dscp-ipv6-compatibility` is an implicit classifier similar to the `ipprec-compatibility` provided to map IP precedence bits in IPv4 traffic when no classifier has been configured.

The following example CLI commandassociates the `ge-0/0/0` interface with the default DSCP IPv6 classifier:

```
user@host# set class-of-service interfaces ge-0/0/0 unit 0 classifiers dscp-ipv6
default
user@host# show class-of-service interfaces
ge-0/0/0 {
  unit 0 {
    classifiers {
      dscp-ipv6 default;
    }
  }
```
If necessary, you can create a user-defined DSCP IPv6 BA classifier with the CLI.

The following steps create a classifier named dscp-ipv6-example:

1. Navigate to the [class-of-service] hierarchy:

   ```
   user@host# edit class-of-service
   ```

2. For this example, use the following commands to map queues to user-defined forwarding classes:

   ```
   [edit class-of-service]
   user@host# set forwarding-classes queue 0 be-class
   [edit class-of-service]
   user@host# set forwarding-classes queue 1 ef-class
   [edit class-of-service]
   user@host# set forwarding-classes queue 2 af-class
   [edit class-of-service]
   user@host# set forwarding-classes queue 3 nc-class
   ```

3. Create a new behavior aggregate classifier for DiffServ CoS:

   ```
   [edit class-of-service]
   user@host# edit classifiers dscp-ipv6 dscp-ipv6-example
   ```

4. Import the default DSCP IPv6 classifier so that it can be used to classify the code points you do not explicitly cover in your configuration:

   ```
   [edit class-of-service classifiers dscp-ipv6 dscp-ipv6-example]
   user@host# set import default
   ```

5. Specify a best-effort forwarding class classifier:

   ```
   [edit class-of-service classifiers dscp-ipv6 dscp-ipv6-example]
   user@host# set forwarding-class be-class loss-priority high code-points 000001
   ```

6. Specify an expedited forwarding class classifier:

   ```
   [edit class-of-service classifiers dscp-ipv6 dscp-ipv6-example]
   user@host# set forwarding-class ef-class loss-priority high code-points 101111
   ```

7. Specify an assured forwarding class classifier:

   ```
   [edit class-of-service classifiers dscp-ipv6 dscp-ipv6-example]
   user@host# set forwarding-class af-class loss-priority high code-points 001100
   ```
8. Specify a network control class classifier:

```bash
[edit class-of-service classifiers dscp-ipv6 dscp-ipv6-example]
user@host# set forwarding-class nc-class loss-priority high code-points 110001
```

9. Go to the [class-of-service] level in the hierarchy and apply your user-defined classifier to an interface:

```bash
[edit class-of-service classifiers dscp-ipv6 dscp-ipv6-example]
user@host# up
[edit class-of-service classifiers]
user@host# up
[edit class-of-service]
user@host# set interfaces ge-0/0/0 unit 0 classifiers dscp-ipv6 dscp-ipv6-example
```

10. Use the `show` command to review your configuration. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```bash
[edit class-of-service]
user@host# show
```

```bash
classifiers {
  dscp-ipv6 dscp-ipv6-example {
    import default;
    forwarding-class be-class {
      loss-priority high code-points 000001;
    }
    forwarding-class ef-class {
      loss-priority high code-points 101111;
    }
    forwarding-class af-class {
      loss-priority high code-points 001100;
    }
    forwarding-class nc-class {
      loss-priority high code-points 110001;
    }
  }
}
forwarding-classes {
  queue 0 be-class;
  queue 1 ef-class;
  queue 2 af-class;
  queue 3 nc-class;
}
interfaces {
  ge-0/0/0 {
    unit 0 {
      classifiers {
        dscp-ipv6 dscp-ipv6-example;
      }
    }
  }
}
```

11. Check your changes to the configuration before committing.
Commit the configuration.

```plaintext
[edit class-of-service]
user@host# commit

configuration check succeeds
```

12. Commit the configuration.

```plaintext
[edit class-of-service]
user@host# commit

commit complete
```

### Configuring DSCP IPv6 Rewrite Rules

A rewrite rule maps the forwarding class and loss priority after JUNOS CoS processing to a corresponding DSCP value specified in the rule. Typically, you use rewrite rules to alter the CoS values in outgoing packets to meet the requirements of the targeted peer.

You can use the CLI show command to display the configuration for the CoS classifiers. The following command shows the configuration of the default DSCP IPv6 rewrite rule:

```plaintext
user@host# show class-of-service rewrite-rule type dscp-ipv6
Rewrite rule: dscp-ipv6-default, Code point type: dscp-ipv6, Index: 32

<table>
<thead>
<tr>
<th>Forwarding class</th>
<th>Loss priority</th>
<th>Code point</th>
</tr>
</thead>
<tbody>
<tr>
<td>best-effort</td>
<td>low</td>
<td>000000</td>
</tr>
<tr>
<td>best-effort</td>
<td>high</td>
<td>000000</td>
</tr>
<tr>
<td>expedited-forwarding</td>
<td>low</td>
<td>101110</td>
</tr>
<tr>
<td>expedited-forwarding</td>
<td>high</td>
<td>101110</td>
</tr>
<tr>
<td>assured-forwarding</td>
<td>low</td>
<td>001010</td>
</tr>
<tr>
<td>assured-forwarding</td>
<td>high</td>
<td>001100</td>
</tr>
<tr>
<td>network-control</td>
<td>low</td>
<td>110000</td>
</tr>
<tr>
<td>network-control</td>
<td>high</td>
<td>111000</td>
</tr>
</tbody>
</table>
```

The following example configuration statement associates the `ge-0/0/0` interface with the default DSCP IPv6 rewrite rule:

```plaintext
user@host# set class-of-service interfaces ge-0/0/0 unit 0 rewrite-rules dscp-ipv6 default
user@host# show class-of-service interfaces ge-0/0/0 {
    unit 0 {
        classifiers {
            dscp-ipv6 default;
        }
        rewrite-rules {
            dscp-ipv6 default;
        }
    }
}
```

If necessary, you can use the CLI to create a user-defined rewrite rule.
The following example configuration statements configure a rewrite rule named rewrite-ipv6-dscps:

1. Navigate to the [class-of-service] hierarchy:

```
user@host# edit class-of-service
```

2. Create a user-defined rewrite rule:

```
user@host# edit rewrite-rules dscp-ipv6 rewrite-ipv6-dscps
```

3. Specify rewrite rules for the best-effort forwarding class:

```
[edit class-of-service rewrite-rules dscp-ipv6 rewrite-ipv6-dscps]
user@host# set forwarding-class be-class loss-priority low code-point 000000
[edit class-of-service rewrite-rules dscp-ipv6 rewrite-ipv6-dscps]
user@host# set forwarding-class be-class loss-priority high code-point 000001
```

4. Specify rewrite rules for the expedited-forwarding forwarding class:

```
[edit class-of-service rewrite-rules dscp-ipv6 rewrite-ipv6-dscps]
user@host# set forwarding-class ef-class loss-priority low code-point 101110
[edit class-of-service rewrite-rules dscp-ipv6 rewrite-ipv6-dscps]
user@host# set forwarding-class ef-class loss-priority high code-point 101111
```

5. Specify rewrite rules for the assured-forwarding forwarding class:

```
[edit class-of-service rewrite-rules dscp-ipv6 rewrite-ipv6-dscps]
user@host# set forwarding-class af-class loss-priority low code-point 001010
[edit class-of-service rewrite-rules dscp-ipv6 rewrite-ipv6-dscps]
user@host# set forwarding-class af-class loss-priority high code-point 001100
```

6. Specify rewrite rules for the network-control forwarding class:

```
[edit class-of-service rewrite-rules dscp-ipv6 rewrite-ipv6-dscps]
user@host# set forwarding-class nc-class loss-priority low code-point 110000
[edit class-of-service rewrite-rules dscp-ipv6 rewrite-ipv6-dscps]
user@host# set forwarding-class nc-class loss-priority high code-point 110001
```

7. Go to the [class-of-service] level in the hierarchy and associate an interface with your user-defined rule:

```
[edit class-of-service rewrite-rules dscp-ipv6 rewrite-ipv6-dscps]
```
8. Use the `show` command to review your configuration. The following example shows the classifier rules created in “Configuring and Applying a DSCP IPv6 BA Classifier” on page 949 and the rewrite rules created in this procedure:

```conf
[edit class-of-service]
user@host# show

classifiers {
  dscp-ipv6 dscp-ipv6-example {
    import default;
    forwarding-class be-class {
      loss-priority high code-points 000001;
    }
    forwarding-class ef-class {
      loss-priority high code-points 101111;
    }
    forwarding-class af-class {
      loss-priority high code-points 001100;
    }
    forwarding-class nc-class {
      loss-priority high code-points 110001;
    }
  }
}
forwarding-classes {
  queue 0 be-class;
  queue 1 ef-class;
  queue 2 af-class;
  queue 3 nc-class;
}
interfaces {
  ge-0/0/0 {
    unit 0 {
      classifiers {
        dscp-ipv6 dscp-ipv6-example;
      }
      rewrite-rules {
        dscp-ipv6 rewrite-ipv6-dscps;
      }
    }
  }
}
rewrite-rules {
  dscp-ipv6 rewrite-ipv6-dscps {
    forwarding-class be-class {
      loss-priority low code-point 000000;
      loss-priority high code-point 000001;
    }
    forwarding-class ef-class {
      loss-priority low code-point 101110;
      loss-priority high code-point 101111;
    }
    forwarding-class af-class {
      loss-priority low code-point 001010;
      loss-priority high code-point 001100;
    }
  }
```
9. Check your changes to the configuration before committing.

   [edit class-of-service]
   user@host# commit check
   
   configuration check succeeds

10. Commit the configuration.

    [edit class-of-service]
    user@host# commit
    
    commit complete
Part 7
Power Over Ethernet

- Power Over Ethernet Overview on page 959
- Configuring Power Over Ethernet on page 961
- Verifying PoE Settings Using the CLI on page 963
Chapter 34
Power Over Ethernet Overview

For information about which devices support the features documented in this chapter, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.

This chapter contains the following topics:
- Introduction on page 959
- SRX Series Services Gateway PoE Specifications on page 959
- PoE Classes and Power Ratings on page 960

Introduction

Power over Ethernet (PoE) is the implementation of the IEEE 802.3 AF and IEEE 802.3 AT standards, that allows both data and electrical power to pass over a copper Ethernet LAN cable.

The PoE is supported on SRX210 Services Gateway (PoE and voice models) and SRX240 Services Gateway (PoE and voice models).

The SRX series devices support PoE on Ethernet ports. PoE ports transfer electrical power and data to remote devices over standard twisted-pair cable in an Ethernet network. PoE ports allow you to plug in devices that require both network connectivity and electrical power, such as VOIP and IP phones and wireless LAN access points.

You can configure the SRX series device to act as a power sourcing equipment (PSE) that supplies power to powered devices (PD) that are connected on designated ports.

SRX Series Services Gateway PoE Specifications

Table 246 on page 959 lists the SRX series devices PoE specifications.

Table 246: PoE Specifications on SRX Series Devices

<table>
<thead>
<tr>
<th>Specifications</th>
<th>Values on SRX210 Devices</th>
<th>Values on SRX240 Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported standards</td>
<td>■ IEEE 802.3 AF</td>
<td>■ IEEE 802.3 AF</td>
</tr>
<tr>
<td></td>
<td>■ Legacy (pre-standards)</td>
<td>■ IEEE 802.3 AT (PoE +)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Legacy (pre-standards)</td>
</tr>
</tbody>
</table>
Table 246: PoE Specifications on SRX Series Devices (continued)

<table>
<thead>
<tr>
<th>Specifications</th>
<th>Values on SRX210 Devices</th>
<th>Values on SRX240 Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported ports</td>
<td>Supported on two Gigabit Ethernet ports and two Fast Ethernet ports (ge-0/0/0, ge-0/0/1, fe-0/0/2, and fe-0/0/3).</td>
<td>Supported on all sixteen Gigabit Ethernet ports (ge-0/0/0 to ge-0/0/15).</td>
</tr>
<tr>
<td>Total PoE power sourcing capacity</td>
<td>50 watts</td>
<td>150 watts</td>
</tr>
<tr>
<td>Default per port power limit</td>
<td>15.4 watts</td>
<td>15.4 watts</td>
</tr>
<tr>
<td>Maximum per port power limit</td>
<td>30 watts</td>
<td>30 watts</td>
</tr>
<tr>
<td>Power management modes</td>
<td>■ Static: power allocated for each interface can be configured</td>
<td>■ Static: power allocated for each interface can be configured</td>
</tr>
<tr>
<td></td>
<td>■ Class: power allocation for interfaces is decided based on the class of powered device connected</td>
<td>■ Class: power allocation for interfaces is decided based on the class of powered device connected</td>
</tr>
</tbody>
</table>

PoE Classes and Power Ratings

A powered device is classified based on the maximum power that it draws across all input voltages and operational modes. When Class-based power management mode is configured on the SRX series devices, power is allocated taking into account the maximum power ratings defined for the different classes of devices.

Table 247 on page 960 lists the classes and their power ratings as specified by the IEEE standards.

Table 247: SRX Series Devices PoE Specifications

<table>
<thead>
<tr>
<th>Class</th>
<th>Usage</th>
<th>Minimum Power Levels Output from PoE Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Default</td>
<td>15.4 watts</td>
</tr>
<tr>
<td>1</td>
<td>Optional</td>
<td>4.0 watts</td>
</tr>
<tr>
<td>2</td>
<td>Optional</td>
<td>7.0 watts</td>
</tr>
<tr>
<td>3</td>
<td>Optional</td>
<td>15.4 watts</td>
</tr>
<tr>
<td>4</td>
<td>Reserved</td>
<td>Class 4 PDs are eligible for receiving power up to 30 watts according to IEEE standards.</td>
</tr>
</tbody>
</table>
Chapter 35

Configuring Power Over Ethernet

For information about which devices support the features documented in this chapter, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.

This chapter includes the following topic:
- Configuring PoE Settings on the SRX Series Services Gateway (CLI Procedure) on page 961

### Configuring PoE Settings on the SRX Series Services Gateway (CLI Procedure)

You can modify Power over Ethernet (PoE) settings on the SRX series devices using the CLI configuration editor.

To configure PoE:
1. Navigate to the top of the configuration hierarchy in the CLI configuration editor.
2. Perform the configuration tasks described in Table 248 on page 961.
3. Commit the configuration when you have completed it.

#### Table 248: Configuring PoE Settings Using the CLI

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable PoE</td>
<td>From the [edit] hierarchy level:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For all PoE interfaces user@host&gt; set poe interface all</td>
<td>Enables a PoE interface. The PoE interface must be enabled in order for the port to provide power to a connected powered device.</td>
</tr>
<tr>
<td></td>
<td>For specific PoE interfaces user@host&gt; set poe interface ge-0/0/0</td>
<td></td>
</tr>
<tr>
<td>Disable PoE</td>
<td>From the [edit] hierarchy level:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For all PoE interfaces user@host&gt; set poe interface all disable</td>
<td>Disables a PoE interface.</td>
</tr>
<tr>
<td></td>
<td>For specific PoE interfaces user@host&gt; set poe interface ge-0/0/0 disable</td>
<td></td>
</tr>
</tbody>
</table>
### Table 248: Configuring PoE Settings Using the CLI (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>CLI Configuration Editor</th>
<th>Meaning</th>
<th>Related Topics</th>
</tr>
</thead>
</table>
| Set the power port priority              | From the [edit] hierarchy level:                                                         | Sets the priority of individual ports. When it is not possible to maintain power to all connected ports, lower-priority ports are powered off before higher-priority ports. When a new device is connected on a higher-priority port, a lower-priority port will be powered off automatically if available power is insufficient to power on the higher-priority port.  
**NOTE:** For the ports with the same priority configuration, ports on the left are given higher priority than the ports on the right.  | - Power Over Ethernet Overview on page 959  
- Verifying PoE Settings Using the CLI on page 963 |
| Set the maximum PoE wattage available power for a port | From the [edit] hierarchy level:                                                         | Sets the maximum amount of power that can be supplied to the port.  |                                                                                     |
| Enable logging of PoE power consumption with the default telemetries settings | From the [edit] hierarchy level:                                                         | Allows logging of per-port PoE power consumption. The telemetries section must be explicitly specified to enable logging. If left unspecified, telemetries is disabled by default.  
Default values for telemetries:  
- Duration: 1 hour  
- Interval: 5 minutes |                                                                                     |
| Set the PoE power management mode         | From the [edit] hierarchy level:                                                         |                                                                                                                                                                                                 |                                                                                     |
| Reserve a specified wattage of power for the gateway in case of a spike in PoE consumption (default is 0) | From the [edit] hierarchy level:                                                         | Reserves the specified amount of power for the gateway in case of a spike in PoE consumption.  |                                                                                     |
Chapter 36
Verifying PoE Settings Using the CLI

For information about which devices support the features documented in this chapter, see the Junos OS Feature Support Reference for SRX Series and J Series Devices.

This chapter contains the following topics:
- Verifying the Status of PoE Interfaces on page 963
- Verifying Global Parameters on page 964
- Telemetry Data (History) for the Specified Interface on page 964

Verifying the Status of PoE Interfaces

**Purpose**
Verify that the PoE interfaces on the device are enabled and set to the desired priority settings. (The device used here is SRX240 Services Gateway).

**Action**
To display real-time status for all PoE interfaces, enter `show poe interface` from the configuration mode in the CLI:

For all PoE interfaces:

```
user@host> show poe interface
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin status</th>
<th>Oper status</th>
<th>Max power</th>
<th>Priority</th>
<th>Power consumption</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge-0/0/0</td>
<td>Enabled</td>
<td>Searching</td>
<td>15.4W</td>
<td>Low</td>
<td>0.0W</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/1</td>
<td>Enabled</td>
<td>Powered-up</td>
<td>15.4W</td>
<td>High</td>
<td>6.6W</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/2</td>
<td>Disabled</td>
<td>Disabled</td>
<td>15.4W</td>
<td>Low</td>
<td>0.0W</td>
<td>0</td>
</tr>
<tr>
<td>ge-0/0/3</td>
<td>Disabled</td>
<td>Disabled</td>
<td>15.4W</td>
<td>Low</td>
<td>0.0W</td>
<td>0</td>
</tr>
</tbody>
</table>

For specific PoE interfaces:

```
user@host> show poe interface ge-0/0/1
```

PoE interface status:
- **PoE interface**: ge-0/0/1
- **Administrative status**: Enabled
- **Operational status**: Powered-up
- **Power limit on the interface**: 15.4 W
- **Priority**: High
- **Power consumed**: 6.6 W
- **Class of power device**: 0
Meaning  The show poe interface command lists PoE interfaces configured on the SRX Series device, with their status, priority, power consumption, and class. This output shows that the device has four PoE interfaces of which two are enabled with default values. One port has a device connected which is drawing power within expected limits.

Verifying Global Parameters

Purpose  Verify global parameters such as guard band, power limit, and power consumption.

Action  From the configuration mode in the CLI, enter the show poe controller command from the top level.

```
user@host > show poe controller
```

<table>
<thead>
<tr>
<th>Controller index</th>
<th>Maximum power</th>
<th>Power consumption</th>
<th>Guard band</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>150.0 W</td>
<td>0.0 W</td>
<td>0 W</td>
<td>Static</td>
</tr>
</tbody>
</table>

Meaning  The show poe controller command lists the global parameters configured on the SRX series device such as controller index, maximum power, power consumption, guard band, and management mode along with their status.

Telemetry Data (History) for the Specified Interface

Purpose  To display the PoE interface’s power consumption over a specified period.

Action  Enable telemetries for the interface with the telemetries configuration statement. When telemetries is enabled, you can display the log of the interface’s power consumption by using the CLI command show poe telemetries interface.

For all records:

```
root@xyz-power1> show poe telemetries interface ge-0/0/1 all
```

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Timestamp</th>
<th>Power</th>
<th>Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fri Jan 04 11:41:15 2009</td>
<td>5.1 W</td>
<td>47.3 V</td>
</tr>
<tr>
<td>2</td>
<td>Fri Jan 04 11:40:15 2009</td>
<td>5.1 W</td>
<td>47.3 V</td>
</tr>
<tr>
<td>3</td>
<td>Fri Jan 04 11:39:15 2009</td>
<td>5.1 W</td>
<td>47.3 V</td>
</tr>
<tr>
<td>4</td>
<td>Fri Jan 04 11:38:15 2009</td>
<td>0.0 W</td>
<td>0.0 V</td>
</tr>
<tr>
<td>5</td>
<td>Fri Jan 04 11:37:15 2009</td>
<td>0.0 W</td>
<td>0.0 V</td>
</tr>
<tr>
<td>6</td>
<td>Fri Jan 04 11:36:15 2009</td>
<td>6.6 W</td>
<td>47.2 V</td>
</tr>
<tr>
<td>7</td>
<td>Fri Jan 04 11:35:15 2009</td>
<td>6.6 W</td>
<td>47.2 V</td>
</tr>
</tbody>
</table>

For a specific number of records:

```
root@xyz-power1> show poe telemetries interface ge-0/0/1 5
```

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Timestamp</th>
<th>Power</th>
<th>Voltage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fri Jan 04 11:31:15 2009</td>
<td>6.6 W</td>
<td>47.2 V</td>
</tr>
<tr>
<td>2</td>
<td>Fri Jan 04 11:30:15 2009</td>
<td>6.6 W</td>
<td>47.2 V</td>
</tr>
<tr>
<td>3</td>
<td>Fri Jan 04 11:29:15 2009</td>
<td>6.6 W</td>
<td>47.2 V</td>
</tr>
</tbody>
</table>
Meaning  The telemetry status displays the power consumption history for the specified interface, provided telemetry has been configured for that interface.

Related Topics  ■ Power Over Ethernet Overview on page 959
■ Configuring Power Over Ethernet on page 961
Telemetry Data (History) for the Specified Interface
Part 8
Index

- Index on page 969
Index

Symbols
#, comments in configuration statements....................xxxix
(), in syntax descriptions..................................................xxxix
* .G notation, for multicast forwarding states............561
1-port four-wire mode, SHDSL See ATM-over-SHDSL
interfaces
2-port two-wire mode, SHDSL See ATM-over-SHDSL
interfaces
3G wireless modem See wireless modem
3G wireless modem interface
card activation..........................................................364
802.1X settings
counting.........................................................................666
< >, in syntax descriptions............................................xxxix
[ ], in configuration statements........................................xxxix
{ }, in configuration statements........................................xxxix
| (pipe), in syntax descriptions........................................xxxix

A
AAL5 multiplex encapsulation........................................154
ATM-over-ADSL for PPP-over-ATM (PPPoA)
interfaces.........................................................144
ATM-over-ADSL interfaces.............................................137
ATM-over-SHDSL interfaces.............................................148
ABM (Asynchronous Balance Mode), HDLC......................63
ABRs See area border routers
access concentrator
as a PPPoE server..........................................................291
naming for PPPoE (Quick Configuration).........................296
access control lists (ACLs) See stateless firewall filters
account activation
CDMA cards.....................................................................376
account activation, CDMA
IOTA.............................................................................380
manual.............................................................................379
OTASP provisioning.......................................................378
ACLs See stateless firewall filters
ACT LED...........................................................................250
TIM508............................................................................251
TIM510............................................................................252
TIM514............................................................................254
TIM516............................................................................255
TIM518............................................................................256
TIM521............................................................................257
action modifiers, stateless firewall filters
list of.............................................................................616
actions
default, routing policy......................................................585
final, routing policy.......................................................585
modifiers, list of.............................................................616
route list match types.........................................................591
routing policy.................................................................588
routing policy, summary of.............................................589
stateless firewall filters, list of.............................................616
activation priority
description.....................................................................265
range and default............................................................275
active routes, versus passive routes....................................481
adapter, console port
TGM550..........................................................................248
adaptive shaping
applying CoS rules to logical interfaces.............................875
verifying..........................................................................943
adaptive-shaper statement
usage guidelines...............................................................876
adaptive-shapers statement
usage guidelines...............................................................876
address match conditions..................................................610, 613
address resolution protocol See ARP; static ARP entries
addresses.................................................................526
IS-IS NETs.....................................................................526
See also NETs
IS-IS NSAP addresses.........................................................526
multicast ranges.................................................................561
physical, in data link layer..................................................14
See also IPv4 addressing; IPv6 addressing
adjacencies, IS-IS
hello PDUs.....................................................................527
See also IS-IS
verifying..........................................................................533
verifying (detail)...............................................................533
administrative scoping........................................................563
ADSL interfaces See ATM-over-ADSL interfaces
ADSL ports See ATM-over-ADSL interfaces
ADSL2+ operating mode....................................................143
advertisements See LSAs; route advertisements
AF forwarding class See assured forwarding forwarding
class
aggregated Ethernet
overview.....................................................449
aggregated Ethernet interfaces
configuring..................................................450
verifying....................................................459
aggregated virtual circuits (AVCs), with MLFR FRF.15 ........................................424
See also MLFR FRF 15; multilink bundles
aggregation, route..........................................471
aliases, CoS See CoS value aliases
ALM LED.....................................................250
TIM508.......................................................251
TIM510.......................................................252
TIM514.......................................................254
TIM516.......................................................255
TIM518.......................................................256
TIM521.......................................................257
alternate mark inversion See AMI encoding
always compare, BGP MED option .................541
AMI (alternate mark inversion) encoding
E1 overview..................................................86
T1...................................................................100
analog media module See TIM514
analog telephone (LINE) ports
TGM550, pinouts............................................239
TIM508, possible configurations.....................250
TIM514, pinouts............................................240
TIM514, possible configurations.....................253
TIM516, possible configurations.....................254
TIM518, possible configurations.....................256
analog trunk (TRUNK) ports
TGM550, pinouts............................................239
TIM508, possible configurations.....................250
TIM514, pinouts............................................240
TIM514, possible configurations.....................253
TIM516, possible configurations.....................254
TIM518, possible configurations.....................256
Annex A PIMs
ATM-over-ADSL interfaces..............................140
See also ATM-over-ADSL interfaces
ATM-over-SHDSL interfaces.............................150
See also ATM-over-SHDSL interfaces
ATM-over-SHDSL modes................................146
G.SHDSL PIMs, setting annex type on..............149, 152
operating modes (configuration editor).............143
operating modes (Quick Configuration).............139
Annex B PIMs
ATM-over-ADSL interfaces..............................140
See also ATM-over-ADSL interfaces
ATM-over-SDSL interfaces..............................150
See also ATM-over-SDSL interfaces
ATM-over-SHDSL interfaces.............................146
G.SHDSL PIMs, setting annex type on..............149, 152
operating modes (configuration editor).............143
operating modes (Quick Configuration).............139
ANSI DMT operating mode..............................143
ANSI T1.413 Issue II operating mode................143
anycast IPv6 addresses...................................69
applying a simple filter.................................908
applying a two-rate tricolor marker.................909
applying an interface set..............................916
applying CoS shaping and scheduling
SRX5600 and SRX5800 devices.........................910
applying traffic control for hierarchical example..922
area border routers
adding interfaces.........................................512
area ID (configuration editor)........................512
backbone area See backbone area
description................................................508
areas See area border routers; backbone area; IS-IS,
areas; NSSAs; stub areas
ARM (Asynchronous Response Mode), HDLC........63
ARP (address resolution protocol), for static ARP entries
for Fast Ethernet subnets...............................92
See also static ARP entries
for Gigabit Ethernet subnets.........................95
See also static ARP entries
publish (responding to ARP requests), on Fast
Ethernet subnets.........................................92
publish (responding to ARP requests), on Gigabit
Ethernet subnets.........................................95
AS path
description................................................539
forcing by MED...........................................540
role in BGP route selection.............................537
AS path, prepending.....................................600
ASB LED.....................................................250
ASs (autonomous systems)
area border routers.......................................508
AS number, in VPNs......................................747
breaking into confederations.........................551
description................................................468
IS-IS networks............................................525
LSPs through..............................................710
sample BGP confederation.............................553
stub areas See stub areas
assigning a forwarding class to an interface........840
assured forwarding (AF) forwarding class..........806
RED drop profiles for...................................854
See also CoS, forwarding classes
asymmetric digital subscriber line (ADSL) See
ATM-over-ADSL interfaces
Asynchronous Balance Mode (ABM), HDLC..........63
asynchronous networks
data stream clocking.....................................54
explicit clocking signal transmission...............55
overview..................................................54
Asynchronous Response Mode (ARM), HDLC........63
Asynchronous Transfer Mode (ATM) interfaces See
ATM-over-ADSL interfaces; ATM-over-SHDSL interfaces
at-0/0/0 See ATM-over-ADSL interfaces; ATM-over-SHDSL interfaces
ATM interfaces See ATM-over-ADSL interfaces; ATM-over-SHDSL interfaces
ATM NLPID encapsulation
ATM-over-ADSL interfaces........................................137, 144
ATM-over-SHDSL interfaces........................................148, 154
ATM PPP over AAL5 LLC encapsulation
ATM-over-ADSL interfaces........................................137, 144
ATM-over-SHDSL interfaces........................................148, 154
ATM PVC encapsulation
ATM-over-ADSL interfaces........................................138, 143
ATM-over-SHDSL interfaces........................................149, 152
ATM SNAP encapsulation
ATM-over-ADSL interfaces........................................137, 144
ATM-over-SHDSL interfaces........................................148, 154
ATM VC multiplex encapsulation
ATM-over-ADSL interfaces........................................137, 144
ATM-over-SHDSL interfaces........................................148, 154
ATM-over-ADSL interfaces........................................140
adding.............................................................140
ADSL overview....................................................34
ADSL systems.......................................................35
ADSL2......................................................................37
ADSL2 + ...............................................................37
CHAP for PPPoA....................................................155
description.............................................................135
eventual encapsulation types, logical (configuration editor)........................................144
eventual encapsulation types, logical (Quick Configuration)........................................137
encapsulation types, physical (configuration editor).......................................................143
encapsulation types, physical (Quick Configuration).....................................................138
logical properties (configuration editor).................................................................144
logical properties (Quick Configuration).................................................................136
MTU default and maximum values..............................................................56
operating modes (configuration editor)..........................................................143
operating modes (Quick Configuration)..........................................................139
physical properties..................................................140
PPPoE session on....................................................291
preparation.............................................................135
Quick Configuration..................................................135
statistics..............................................................159
VCI.................................................................137, 145
verifying..............................................................157
verifying a PPPoA configuration........................................160
verifying a PPPoE configuration........................................304
VPI.................................................................138, 141
See also PPPoE, PPPoE over ATM-over-ADSL; PPPoE over ATM-over-SHDSL
ATM-over-SHDSL interfaces........................................38
1-port four-wire mode..............................................146
1-port four-wire mode, setting................................149, 151
2-port two-wire mode, overview................................146
2-port two-wire mode, setting................................149, 151
adding..............................................................150
annex type, setting.................................................149, 152
CHAP for PPPoA....................................................155
description.............................................................145
eventual encapsulation types, logical (configuration editor)........................................154
eventual encapsulation types, logical (Quick Configuration)........................................148
eventual encapsulation types, physical.............................................................149
eventual encapsulation types, physical (configuration editor)........................................152
line speed.............................................................149
logical properties (configuration editor).............................................................153
logical properties (Quick Configuration).............................................................148
loopback testing....................................................150
MTU default and maximum values.............................................................56
overview.............................................................38
PPPoE session on....................................................291
preparation.............................................................135
Quick Configuration..................................................146
SNEXT threshold....................................................150, 153
SNR margin.............................................................150, 153
statistics..............................................................163
status.................................................................163
VCI.................................................................149, 155
verifying..............................................................160
verifying a PPPoE configuration........................................304
VPI.................................................................149, 152
“dying gasp”..........................................................163
See also G.SHDSL PIMs
authentication
CHAP, for PPPoE interfaces........................................293
OSPF, MD5..........................................................516
OSPF, plain-text passwords........................................516
RIPv2, MD5..........................................................498
RIPv2, plain-text passwords........................................498
auto operating mode................................................143
Auto-RP...............................................................563
autonegotiation, Gigabit Ethernet...........................................96
autonomous systems See ASs
Avaya Communication Manager (CM)
CAC-BL requirement for WANS......................................265
description.............................................................264
Avaya IG550 Integrated Gateway See Avaya VoIP modules
Avaya Communication Manager (CM)......................................264
Avaya manuals, list of..............................................263
description.............................................................260
See also Avaya VoIP modules
Index

dynamic CAC  See dynamic CAC ..............................................266
TGM550–JUNOS compatibility .............................................266
Avaya Media Gateway Controller (MGC) ................................ 266
  Avaya Communication Manager (CM) ...............................264
  Avaya manuals, list of .....................................................263
description ......................................................................260
dynamic CAC  See dynamic CAC ...........................................263
MGC list ...........................................................................263
  See also  MGC list .........................................................263
  supported models ..........................................................263
  verifying MGC list ..........................................................285
Avaya MGC  See Avaya Media Gateway Controller ........................ 263
Avaya VoIP .........................................................................263
  Avaya Communication Manager (CM) ...............................264
  Avaya manuals, list of .....................................................263
  Avaya Media Gateway Controllers supported ....................263
  bandwidth management  See dynamic CAC .........................263
  Disk-on-Key configuration ..............................................268
dynamic CAC  See dynamic CAC ...........................................263
EPW configuration ............................................................268
  See also  Avaya VoIP modules ..........................................261
IP addressing guidelines .....................................................261
  modules  See Avaya VoIP modules ....................................261
  network .........................................................................261
description ......................................................................259
prerequisites .....................................................................267
Quick Configuration ...........................................................269
TGM550–JUNOS compatibility .............................................266
troubleshooting ..................................................................286
typical topology ..................................................................261
  verifying available bandwidth .........................................285
  verifying configuration ....................................................283
  version incompatibility, correcting ...................................286
Avaya VoIP modules ............................................................263
  accessing the router from .................................................282
  administration .................................................................278
  Avaya CLI access .............................................................278
  Avaya Communication Manager (CM) ...............................264
  Avaya manuals, list of .....................................................263
  CLI access requirements ..................................................279
  connector pinouts .............................................................238
  console connection ..........................................................279
  Disk-on-Key configuration ..............................................268
dynamic CAC  See dynamic CAC ...........................................263
grounding, 10 AWG replacement cable .................................244
interface types ...................................................................261
IP address, modifying (configuration editor) .........................277
JUNOS configurability .......................................................262
LEDs  See LEDs .................................................................262
MGC list, adding ...............................................................274
MGC list, clearing .............................................................275
non-hot-swappability ..........................................................244
overview ..........................................................................262
prerequisites .....................................................................267
requirements .....................................................................244
resetting TGM550 .............................................................282
saving the configuration .....................................................283
SSH connection ..................................................................280
summary ..........................................................................245
  Telnet access .................................................................280
  TGM550 .........................................................................247
TGM550 IP address, setting (configuration editor) ................272
TGM550 maximum gateway capacities ................................248
TGM550–JUNOS compatibility .............................................266
TIM508 .............................................................................250
TIM510 .............................................................................251
TIM514 .............................................................................253
TIM516 .............................................................................254
TIM518 .............................................................................255
TIM521 .............................................................................256
AVCs (aggregated virtual circuits), multilink bundles, 424
  with MLFR FRF.15 ..........................................................424
  See also  MLFR FRF.15, multilink bundles ..........................424
B-channel allocation order, on ISDN PRI .................................127
B-channels
  description .......................................................................49
  naming convention ..........................................................312
  verifying ..........................................................................346
B8ZS encoding ....................................................................21
BA classifiers  See classifiers ..................................................21
backbone area
  area ID (configuration editor) ............................................510
  configuring .......................................................................509
  description .......................................................................508
  interface ..........................................................................512
backoff algorithm, collision detection ....................................17
backup connection, ISDN .....................................................309
backup connection, wireless modem .....................................373
functions ..........................................................................360
backward-explicit congestion notification (BECN) bits ............58
bandwidth for Avaya VoIP, managing  See dynamic CAC ........285
bandwidth on demand, ISDN
  dialer interface (configuration editor) ...............................332
  dialer pool .......................................................................337
  ISDN BRI interface (configuration editor) ..........................356
  overview ..........................................................................352
BBL (bearer bandwidth limit)
  description .......................................................................265
  range and default ............................................................275
  reported (RBBL), description ............................................265
  verifying available bandwidth .........................................285

JUNOS Software Interfaces and Routing Configuration Guide

972  Index
bc-0/0/0

ISDN BRI interface .................................................. 312
See also ISDN BRI interfaces, ISDN PRI interfaces
ISDN PRI interface ..................................................... 313
BE forwarding class See best-effort forwarding class
bearer bandwidth limit See BBL
BECN (backward-explicit congestion notification)
bits ........................................................................... 58
behavior aggregate classifiers See classifiers
BERTs (bit error rate tests)
on channelized interfaces (configuration editor) ........................................ 122
overview ..................................................................... 53
best-effort (BE) forwarding class
default assignment ..................................................... 806
See also CoS; Forwarding classes
typical usage .............................................................. 791
BGP (Border Gateway Protocol)
AS path ...................................................................... 539
See also AS path
confederations See BGP confederations
export policy for CLNS ................................................ 762
external ..................................................................... 536
See also EBGP
for CLNS VPN NLRI .................................................. 764
full mesh requirement ................................................ 536
injecting OSPF routes into BGP .................................. 597
internal .................................................................... 536
See also IBGP
local preference .......................................................... 538
MED metric .................................................................. 540
See also MED
origin value .................................................................. 539
overview ..................................................................... 535
peering sessions See BGP peers; BGP sessions
point-to-point internal peer session (configuration editor) ......................... 545
point-to-point peer session (configuration editor) ..................................... 544
policy to make routes less preferable ........................................ 600
requirements .............................................................. 542
route reflectors See BGP route reflectors
route selection process .................................................. 537
See also route selection
route-flap damping ....................................................... 602
sample BGP peer network ............................................. 544
sample configuration .................................................... 553
sample full mesh ......................................................... 546
sample route reflector ................................................. 550
scaling techniques ....................................................... 542
session establishment .................................................. 535
session maintenance .................................................. 556
verifying BGP configuration .......................................... 556
verifying BGP groups .................................................... 555
verifying BGP peers (neighbors) ..................................... 554
verifying peer reachability ............................................. 556
VPLS ............................................................................ 778, 782
VPNs ........................................................................... 744
BGP confederations
creating (configuration editor) ........................................ 552
description ............................................................... 551
route-flap damping ..................................................... 602
sample network ......................................................... 553
BGP groups
confederations (configuration editor) ........................................ 552
verifying ................................................................. 555
BGP messages
to establish sessions .................................................... 555
update, to maintain sessions ......................................... 536
BGP neighbors See BGP peers
BGP peers
directing traffic by local preference ........................................ 538
external (configuration editor) ........................................ 544
internal (configuration editor) ........................................ 545
internal, sample full mesh .......................................... 546
internal, sample route reflector ...................................... 550
monitor probes .......................................................... 554
peer address, role in route selection ........................................ 537
point-to-point connections .......................................... 543
sample peer network ................................................... 544
sessions between peers ................................................ 535
verifying ................................................................. 554, 556
verifying reachability .................................................... 556
BGP route reflectors
cluster of clusters ....................................................... 548
clusters, role in route selection ........................................ 537
creating (configuration editor) ........................................ 549
description ............................................................... 547
multiple clusters ....................................................... 547
sample IBGP network .................................................. 550
BGP sessions
configured at both ends ............................................... 535
establishment ............................................................ 535
maintenance ............................................................. 536
point-to-point external (configuration editor) ......................... 544
point-to-point internal (configuration editor) .......................... 545
sample peering session ............................................... 543
bipolar with 8–zero substitution (B8ZS) encoding .............................. 21
bit error rate tests (BERTs) See BERTs
bit stuffing .................................................................. 24
bit-field logical operators, stateless firewall filters ......................... 615
bit-field match conditions ............................................. 610
bit-field synonym match conditions .................................. 610
blinking
TIM508 ACT (active) LED state .................................... 251
TIM514 ACT (active) LED state .................................... 254
TIM516 ACT (active) LED state .................................... 255
TIM518 ACT (active) LED state .................................... 256
bootstrap router ......................................................... 563
Border Gateway Protocol See BGP
br-0/0/0 ................................................................. 312
See also B-channels, ISDN BRI interfaces
braces, in configuration statements ...................... xl
brackets
    angle, in syntax descriptions ............................ xxxix
    square, in configuration statements ................. xxxix
branches .......................................................... 560
See also multicast
BRI media module See TIM521
bridge domains ................................................. 677
    configuration .................................................. 680
    default learning .............................................. 698
    forwarding tables .......................................... 696
    integrated routing and bridging interface ............ 692
    SRX Series device support .............................. 678
    transparent mode .......................................... 676
bridges, on LAN segments .................................. 18
bridging
    default forwarding behavior ............................ 691
    terms ........................................................... 678
    transparent mode .......................................... 676
    BSR (bootstrap router) .................................. 563
building a scheduler hierarchy .......................... 919
built-in Ethernet interfaces ............................... 77
See also Fast Ethernet ports, Gigabit Ethernet ports

C

C-bit parity frame format
    enable or disable on T3 ports ......................... 104
    overview ..................................................... 26
cables
    Avaya VoIP 10 AWG replacement grounding
      cable ......................................................... 244
    T1 cable length ............................................ 101
    T3 cable length ............................................ 104
    TGM550 analog pinouts .................................. 239
    TGM550 console port, DB-9 connector
      pinouts ....................................................... 238
    TGM550 console port, RJ-45 connector
      pinouts ....................................................... 238
    TIM508 pinouts ............................................ 239
    TIM510 E1/T1 pinouts .................................... 240
    TIM514 analog pinouts .................................. 240
    TIM516 pinouts ............................................ 241
    TIM518 pinouts ............................................ 242
CAC See dynamic CAC
CAC-BL requirement for dynamic CAC .................. 265
    call admission control See dynamic CAC
    Call Admission Control: Bandwidth Limitation (CAC-BL),
      requirement for dynamic CAC ....................... 265
    call setup, ISDN ............................................ 51
    callback, ISDN
      dialer interface (configuration editor) ............ 339
      encapsulation matching ................................ 338
      overview .................................................. 337
    rejecting incoming calls (configuration editor) .... 341
    screening incoming calls (configuration editor) .... 340
    voice not supported ....................................... 337
    calling number, ISDN ...................................... 316, 323
    card activation
      3G wireless modem interface .......................... 364
      carrier sense multiple access with collision detection
        (CSMA/CD) .................................................. 16
      ccc protocol family ....................................... 65
    CDMA (Code-Division Multiple Access)
      IOTA ........................................................ 380
      manual account activation ............................ 379
      OTASP provisioning ...................................... 378
      supported wireless modem cards ..................... 357, 376
    CE (customer edge) routers ............................. 772
      description ................................................ 737
      See also VPLS
    chained stateless firewall filters ..................... 609
    Challenge Handshake Authentication Protocol See
      CHAP
    channel number, in interface name .................... 12
    channel service unit (CSU) device .................... 61
    channelized E1 interfaces
      adding ....................................................... 120
      BERTs (configuration editor) ......................... 122
      clear-channel operation (configuration editor) ... 121
      drop-and-insert (configuration editor) .............. 123, 124
      FAQ ........................................................ 130
      framing (configuration editor) ....................... 121
      ISDN PRI (configuration editor) ..................... 125
      MTU default and maximum values ..................... 56
      number of channels supported ....................... 120
      overview .................................................. 23
      See also channelized E1 ports
    verifying ...................................................... 128
    verifying clear-channel interfaces ................... 129
    channelized E1 ports
      clocking (configuration editor) ....................... 121, 124
      clocking for drop-and-insert ......................... 123
      configuring ................................................ 120
      drop-and-insert clock combinations
        internal ..................................................... 131
      FAQ ........................................................ 130
      ISDN PRI (configuration editor) ..................... 125
      link hold time (configuration editor) ............... 121
      overview .................................................. 23
      See also channelized E1 interfaces
    per-unit scheduler (configuration editor) ............ 121
    trace options (configuration editor) .................. 122
    channelized interfaces See channelized E1 interfaces;
      channelized T1 interfaces; ISDN PRI interfaces
    channelized Nxds0 interface, maximum delay buffer
      time .......................................................... 900
sample behavior aggregate classification.........810
sample behavior aggregate classifier
assignments.........................................................810, 849
sample, for firewall filter........................................836
strict high-priority queuing (configuration
editor).........................................................................894
strict high-priority queuing, applying classifier to
interface (configuration editor)......................................897
transparent mode.........................................................703
classifiers, defining.....................................................417
clear-channel interface on channelized port
configuring.................................................................121
verifying..................................................................129
clear-channel interfaces, maximum delay buffer
time...............................................................................900
CLI configuration editor
aggregated ethernet interface.................................785
ATM-over-ADSL interfaces........................................140
ATM-over-SHDSL interfaces........................................150
Avaya VoIP.................................................................272
BGP........................................................................544, 545, 549, 552, 744, 782
channelized E1 interfaces............................................120
channelized T1 interfaces.............................................120
CHAP on ATM-over-ADSL interfaces.........................155
CHAP on ATM-over-SHDSL interfaces.........................155
CHAP on dialer interfaces............................................397
CLNS........................................................................759, 761, 762, 763, 764
CoS...........................................................................833
CoS, large delay buffers.............................................900
CoS, strict high priority for queuing............................893
CRTP........................................................................430
gigabit ethernet interface............................................784
IGP.............................................................................745, 746
interfaces..................................................................742, 776, 777
IS-IS...........................................................................529
ISDN connections....................................................321
LDP signaling protocol.............................................745
LDP-signaled LSPs....................................................721
LFI.............................................................................413
MLPPP bundles..........................................................413
MPLS.........................................................................721, 729, 781
MPLS Layer 2 circuit....................................................755
MPLS VPNs..............................................................742, 744, 745, 746, 747, 748, 752
multicast network.....................................................567, 568, 569, 571, 572, 574
network interfaces...................................................109
network interfaces, adding.........................................110
network interfaces, deleting.........................................112
OSPF..........................................................................506, 509, 511, 514, 783
PAP on dialer interfaces.............................................596
RIP.............................................................................492, 494, 496, 498
routing instances.......................................................747, 780
routing options..........................................................747, 781
routing policies.........................................................583, 585, 594, 597, 600, 603
routing policy............................................................748, 752
RSVP signaling protocol............................................746, 782
RSVP-signaled LSPs.....................................................729
stateless firewall filters...........................................618, 624, 632
static routes.............................................................476, 478, 481, 483
USB modem connections..........................................386
VLAN circuit..............................................................785
VLAN encapsulation..................................................784, 785
VoIP..........................................................................272
VPLS.................................................................776, 777, 780, 781, 782, 783, 784, 785
CLI, Avaya VoIP, accessing.........................................278
CLNS (Connectionless Network Service) VPNs
BGP export policy.....................................................762
BGP, to carry CLNS VPN NLRI....................................764
displaying configurations............................................765
ES-IS.........................................................................761
IS-IS.........................................................................762
linking hosts..............................................................757
overview..................................................................757
requirements.............................................................758
static routes (without IS-IS)........................................763
verifying configuration.................................................765
VPN routing instance................................................759
clock rate, serial interface
DTE default reduction..................................................31
clocking
channelized ports......................................................121
data stream clocking...................................................54
E1............................................................................85
E3............................................................................88
explicit clocking signal transmission...........................55
overview..................................................................54
possible combinations for drop-and-insert...............131
requirement for drop-and-insert..................................123
serial interface.........................................................107
serial interface, inverting the transmit
clock........................................................................31, 107
serial interface, modes...............................................30
t1.............................................................................99
t3.............................................................................103
clusters See BGP route reflectors
CM, Avaya See Avaya Communication Manager
Code-Division Multiple Access (CDMA) See CDMA
collision detection
backoff algorithm.........................................................17
overview..................................................................16
combined stations, HDLC............................................63
comments, in configuration statements .........................xxxix
Communication Manager (CM), Avaya See Avaya
Communication Manager
complete sequence number PDU (CSNP)......................528
Compressed Real-Time Transport Protocol See CRTP
congedations See BGP confederations
configuring
802.1X settings.........................................................666
GVRP.......................................................................673
IGMP snooping..........................................................671
LACP.................................................................663
dial-on-demand filter See dialer filter, ISDN

dial-on-demand routing backup, ISDN

dialer filter .......................................................... 328
  See also dialer filter, ISDN

dialer watch .......................................................... 330
  See also dialer watch

OSPF support .......................................................... 331
  See also dialer watch

dial-on-demand routing backup, USB modem

dialer filter .......................................................... 391
  See also dialer filter, USB modem

dialer watch .......................................................... 393
  See also dialer watch

dialer filter, ISDN

applying to the dialer interface .................................. 329
configuring .......................................................... 328
overview ............................................................ 328

dialer filter, USB modem

overview ............................................................ 391

dialer filter, wireless modem

functions ............................................................ 375

dialer interface, ISDN

adding ............................................................... 324
bandwidth on demand (configuration editor) ............... 328
callback (configuration editor) .................................. 332
limitations ........................................................... 338
multiple, ensuring different IPv4 subBRI et
addresses on ........................................................... 339
naming convention .................................................. 341
rejecting incoming calls (configuration editor) .............. 342
restrictions .......................................................... 343
screening incoming calls (configuration editor) ............. 344
secondary (backup) connection .................................. 345
verifying .............................................................. 346

dialer interface, ISDN BRI (Quick Configuration) ............ 317

dialer interface, USB modem

adding ............................................................... 387
dial-in (configuration editor) ..................................... 395
dialer filter .......................................................... 391
  See also dialer filter, USB modem

dialer watch See dialer watch

limitations ........................................................... 384
naming convention .................................................. 384
restrictions .......................................................... 384
secondary (backup) connection .................................. 390

dialer interface, wireless modem ................................ 360

activation delay ..................................................... 361
adding ............................................................... 365
authentication ....................................................... 360
backup interface ................................................... 360

See also backup connection, wireless modem

backup WAN connection ............................................ 373
CHAP authentication ............................................. 371
deactivation delay ................................................... 361
dialer filter .......................................................... 360
  See also dialer filter, wireless modem

dialer watch .......................................................... 360, 374
  See also dialer watch, wireless modem

idle timeout .......................................................... 374
initial route check ................................................... 374
operating parameters ............................................. 361
PAP ................................................................. 370
PAP authentication .................................................. 360
dialer interfaces

CHAP for PPP ....................................................... 397
PAP for PPP .......................................................... 396
dialer options, ISDN

for ISDN BRI service .................................................. 317
for ISDN PRI service ................................................. 128
dialer pools, 3G wireless interface

Quick Configuration .................................................. 364

dialer pools, ISDN

for bandwidth on demand (configuration editor) .............. 337
for dialer watch (configuration editor) .......................... 331
ISDN BRI physical interface (configuration editor) ............. 332
Quick Configuration .................................................. 316
dialer pools, USB modem

for dialer watch (configuration editor) .......................... 394
USB modem physical interface (configuration editor) ............. 394

dialer watch

adding a dialer watch interface (configuration editor) ............ 387
configuring (Quick Configuration—ISDN BRI) ....................... 319
dialer pool (configuration editor) .................................... 331, 394
ISDN interface for (configuration editor) .......................... 330
overview .............................................................. 330, 393
selecting (Quick Configuration—ISDN BRI) ....................... 318
watch list (configuration editor) .................................... 330, 394
watch list (Quick Configuration) ..................................... 320
dialer watch, wireless modem

functions ............................................................ 374

DID on line ports ..................................................... 250, 253, 255

Differentiated Services See DiffServ
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>DiffServ (Differentiated Services)</td>
<td>838</td>
</tr>
<tr>
<td>assigning forwarding classes to output queues</td>
<td>838</td>
</tr>
<tr>
<td>assured forwarding</td>
<td>854</td>
</tr>
<tr>
<td>behavior aggregate classifiers</td>
<td>848</td>
</tr>
<tr>
<td>configuration tasks (configuration editor)</td>
<td>833</td>
</tr>
<tr>
<td>firewall filter for a multifield classifier</td>
<td>835</td>
</tr>
<tr>
<td>interoperability</td>
<td>792</td>
</tr>
<tr>
<td>JUNOS implementation</td>
<td>801</td>
</tr>
<tr>
<td>policer for firewall filter</td>
<td>834</td>
</tr>
<tr>
<td>RED drop profiles</td>
<td>854</td>
</tr>
<tr>
<td>rewrite rules</td>
<td>845</td>
</tr>
<tr>
<td>scheduler maps</td>
<td>860</td>
</tr>
<tr>
<td>schedulers</td>
<td>857</td>
</tr>
<tr>
<td>virtual channels for rules</td>
<td>864</td>
</tr>
<tr>
<td>digital subscriber line (DSL) See ATM-over-ADSL interfaces; ATM-over-SHDSL interfaces; DSLAM connection</td>
<td>250, 253, 255</td>
</tr>
<tr>
<td>direct inward dialing, on line ports</td>
<td>250, 253, 255</td>
</tr>
<tr>
<td>discard eligibility bits See DE bits</td>
<td>76</td>
</tr>
<tr>
<td>discard interface</td>
<td>76</td>
</tr>
<tr>
<td>discard, filter action</td>
<td>609</td>
</tr>
<tr>
<td>automatic, stateless firewall filters</td>
<td>609</td>
</tr>
<tr>
<td>discovery packets, PPPoE</td>
<td>62, 292</td>
</tr>
<tr>
<td>Disk-on-Key configuration</td>
<td>268</td>
</tr>
<tr>
<td>description</td>
<td>268</td>
</tr>
<tr>
<td>procedure</td>
<td>269</td>
</tr>
<tr>
<td>requirements</td>
<td>268</td>
</tr>
<tr>
<td>RESET CONFIG button caution</td>
<td>268</td>
</tr>
<tr>
<td>Distance Vector Multicast Routing Protocol</td>
<td>563</td>
</tr>
<tr>
<td>distance-vector routing protocols</td>
<td>485</td>
</tr>
<tr>
<td>See also RIP</td>
<td>313, 384</td>
</tr>
<tr>
<td>dl0</td>
<td>313, 384</td>
</tr>
<tr>
<td>See also dialer interface, ISDN</td>
<td>313, 384</td>
</tr>
<tr>
<td>DLCIs (data-link connection identifiers) in MLFR FRF 16 bundles (configuration editor)</td>
<td>427</td>
</tr>
<tr>
<td>overview</td>
<td>58</td>
</tr>
<tr>
<td>documentation</td>
<td>58</td>
</tr>
<tr>
<td>comments on</td>
<td>58</td>
</tr>
<tr>
<td>domains</td>
<td>18</td>
</tr>
<tr>
<td>broadcast domains</td>
<td>18</td>
</tr>
<tr>
<td>collision domains</td>
<td>17</td>
</tr>
<tr>
<td>DoS (denial-of-service) attacks, preventing</td>
<td>624</td>
</tr>
<tr>
<td>dotted decimal notation</td>
<td>66</td>
</tr>
<tr>
<td>downstream interfaces</td>
<td>560</td>
</tr>
<tr>
<td>See also multicast</td>
<td>560</td>
</tr>
<tr>
<td>DR See designated router</td>
<td>922</td>
</tr>
<tr>
<td>drop profiles See CoS, RED drop profiles</td>
<td>922</td>
</tr>
<tr>
<td>drop profiles for hierarchical example</td>
<td>922</td>
</tr>
<tr>
<td>drop-and-insert of time slots, on channelized ports</td>
<td>123</td>
</tr>
<tr>
<td>clock source requirement</td>
<td>123</td>
</tr>
<tr>
<td>configuring</td>
<td>124</td>
</tr>
<tr>
<td>overview</td>
<td>119, 123</td>
</tr>
<tr>
<td>possible clock combinations</td>
<td>131</td>
</tr>
<tr>
<td>sample configuration</td>
<td>131</td>
</tr>
<tr>
<td>signaling channel requirement</td>
<td>123</td>
</tr>
<tr>
<td>DS0 interfaces, maximum delay buffer time</td>
<td>900</td>
</tr>
<tr>
<td>DS0 time slots channelization</td>
<td>23</td>
</tr>
<tr>
<td>See also channelized E1 interfaces; channelized T1 interfaces drop-and-insert, on channelized T1/E1 interfaces</td>
<td>123</td>
</tr>
<tr>
<td>DS1 interfaces See E1 interfaces; T1 interfaces</td>
<td>20</td>
</tr>
<tr>
<td>DS1 ports See E1 ports; T1 ports</td>
<td>20</td>
</tr>
<tr>
<td>DS1 signals E1 and T1</td>
<td>20</td>
</tr>
<tr>
<td>See also E1 interfaces; T1 interfaces multiplexing into DS2 signal</td>
<td>24</td>
</tr>
<tr>
<td>DS2 signals bit stuffing</td>
<td>24</td>
</tr>
<tr>
<td>frame format</td>
<td>24</td>
</tr>
<tr>
<td>DS3 interfaces See E3 interfaces; T3 interfaces</td>
<td>26</td>
</tr>
<tr>
<td>DS3 ports See E3 ports; T3 ports</td>
<td>26</td>
</tr>
<tr>
<td>DS3 signals</td>
<td>26</td>
</tr>
<tr>
<td>DS3 C-bit parity frame format</td>
<td>26</td>
</tr>
<tr>
<td>M13 frame format</td>
<td>25</td>
</tr>
<tr>
<td>dsc interface</td>
<td>76</td>
</tr>
<tr>
<td>DSCP IPv6 See CoS; DSCPs</td>
<td>804</td>
</tr>
<tr>
<td>DSCPs (DiffServ code points) default behavior aggregate classifiers</td>
<td>807</td>
</tr>
<tr>
<td>DSCP aliases and values</td>
<td>804</td>
</tr>
<tr>
<td>See also CoS replacing with rewrite rules</td>
<td>846</td>
</tr>
<tr>
<td>rewrites</td>
<td>810</td>
</tr>
<tr>
<td>sample behavior aggregate classification</td>
<td>810</td>
</tr>
<tr>
<td>DSL See ATM-over-ADSL interfaces; ATM-over-SHDSL interfaces; DSLAM connection</td>
<td>140</td>
</tr>
<tr>
<td>DSL access multiplexer See DSLAM connection</td>
<td>150</td>
</tr>
<tr>
<td>DSLAM connection</td>
<td>291</td>
</tr>
<tr>
<td>ATM-over-ADSL interface for</td>
<td>140</td>
</tr>
<tr>
<td>ATM-over-SHDSL interface for</td>
<td>150</td>
</tr>
<tr>
<td>PPPoE over ATM-over-ADSL topology</td>
<td>291</td>
</tr>
<tr>
<td>DSU (data service unit) device</td>
<td>61</td>
</tr>
<tr>
<td>DTE (data terminal equipment) default clock rate reduction</td>
<td>31</td>
</tr>
<tr>
<td>serial connection process</td>
<td>29</td>
</tr>
<tr>
<td>serial device</td>
<td>28</td>
</tr>
<tr>
<td>DTE clocking mode See internal clocking mode</td>
<td>563</td>
</tr>
<tr>
<td>DVMRP (Distance Vector Multicast Routing Protocol)</td>
<td>563</td>
</tr>
<tr>
<td>dynamic CAC</td>
<td>265</td>
</tr>
<tr>
<td>activation priority, description</td>
<td>265</td>
</tr>
<tr>
<td>BBL, description</td>
<td>265</td>
</tr>
<tr>
<td>CAC-BL requirement for WANs</td>
<td>265</td>
</tr>
<tr>
<td>configuring on WAN interfaces (configuration editor)</td>
<td>275</td>
</tr>
<tr>
<td>overview</td>
<td>264</td>
</tr>
</tbody>
</table>
ES-IS (End System-to-Intermediate System)..........................760
for a PE router in a CLNS island....................................761
overview..................................................................757
ESF (extended superframe) framing..................................22
Ethernet cable
  TGM550 console DB-9 connector pinouts...............................238
  TGM550 console, RJ-45 connector pinouts............................238
Ethernet interfaces: access control......................................16
  broadcast domains ....................................................18
  collision detection ...................................................16
  collision domains ....................................................17
  CSMA/CD..................................................................16
  enabling promiscuous mode...........................................108
  frame format ................................................................18
  IS-IS, NET address .....................................................529
  overview ....................................................................15
  Quick Configuration ....................................................90, 94
  See also Fast Ethernet ports
  See also Fast Ethernet ports; Gigabit Ethernet ports
  See also Gigabit Ethernet ports
Ethernet link aggregation
  overview .................................................................449
Ethernet over ATM encapsulation ......................................143
  ATM-over-ADSL interfaces ............................................137, 138
  ATM-over-SHDSL interfaces .........................................149, 152
Ethernet over ATM LLC encapsulation
  ATM-over-ADSL interfaces ..........................................144
  ATM-over-SHDSL interfaces .........................................148, 154
Ethernet ports See Ethernet interfaces; Fast Ethernet ports
  as switches ..................................................................641
Ethernet switches
  configuring ports as ....................................................641
  ETR LED .................................................................250
  ETSI TS 101 388 V1.3.1 operating mode ............................143
  EU-64 addresses .......................................................15
  exact route list match type ............................................591
  excess bandwidth sharing ..........................................937
  explicit clocking signal transmission ................................55
  export routing policy, for Layer 2 VPNs ............................748
  export statement, for routing policies ...............................583
  extended superframe (ESF) framing ................................22
  exterior gateway protocols ..........................................468
  external BGP See EBGP
  external paths, role in BGP route selection .......................537
FAQ (frequently asked questions)
  Are LFI and load balancing working correctly?..................441
  What causes jitter and latency on multilink bundles? ..........440
  What clock combinations are possible for channelized T1/E1 drop-and-insert? ..................................131
  Which CoS components apply on link services interface? .......439
  Why Are Packets Dropped on a PVC Between a J Series Device and Another Vendor? ..................447
  Why is the VoIP interface unavailable? .........................286
Fast Ethernet ports
  ARP address..............................................................91
  CHAP for PPPoA ......................................................155
  logical interfaces .....................................................91
  MAC address ..........................................................91
  MTU .....................................................................93
  MTU default and maximum values ...................................56
  overview ...............................................................15
  PPPoE session on .....................................................291
  Quick Configuration ....................................................90
  static ARP entries (configuration editor) .........................111
FCS (frame check sequence)
  checksums ..................................................................55
  CRCs .......................................................................55
  overview ....................................................................55
  two-dimensional parity .................................................55
FEAC C-bit condition indicators..............................................27
FECN (forward-explicit congestion notification) bits .............58
firewall filters
  applying CoS rules to logical interfaces ..........................864
  multifield classifier filter terms .....................................836
  policer for ..................................................................834
  sample classifier terms .................................................836
  stateless firewall filters ..............................................607
  See also stateless firewall filters
term number caution ....................................................609
  verifying fragment handling .......................................636
firewall user authentication
  transparent mode .......................................................693
flap damping ..................................................................602
parameters ....................................................................603
flooding, preventing .....................................................624
flow control
  data link layer ..........................................................14
  flow control, actions in routing policies .........................589
  font conventions ..........................................................xxxix
forward-explicit congestion notification (FECN) bits ............58
forwarding classes
  assigning to an interface .............................................840
  assigning to logical interfaces (Quick Configuration) .........833

F
failover connection, ISDN..................................................309

Index
<table>
<thead>
<tr>
<th>topic</th>
<th>pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>assigning to output queues (configuration editor)</td>
<td>839</td>
</tr>
<tr>
<td>assigning to output queues (Quick Configuration)</td>
<td>819</td>
</tr>
<tr>
<td>configuring</td>
<td>840</td>
</tr>
<tr>
<td>configuring up to eight</td>
<td>841</td>
</tr>
<tr>
<td>default assignments</td>
<td>807</td>
</tr>
<tr>
<td>default values</td>
<td>806</td>
</tr>
<tr>
<td>defining (Quick Configuration)</td>
<td>819</td>
</tr>
<tr>
<td>description</td>
<td>796</td>
</tr>
<tr>
<td>mapping to schedulers (configuration editor)</td>
<td>861</td>
</tr>
<tr>
<td>policy to group source and destination prefixes</td>
<td>594</td>
</tr>
<tr>
<td>queue assignments, default</td>
<td>806</td>
</tr>
<tr>
<td>sample behavior aggregate classification</td>
<td>810</td>
</tr>
<tr>
<td>sample mappings</td>
<td>860</td>
</tr>
<tr>
<td>forwarding classes, defining</td>
<td>417</td>
</tr>
<tr>
<td>forwarding policy options</td>
<td>797</td>
</tr>
<tr>
<td>forwarding states, multicast notation</td>
<td>561</td>
</tr>
<tr>
<td>forwarding tables</td>
<td>561</td>
</tr>
<tr>
<td>controlling OSPF routes in</td>
<td>519</td>
</tr>
<tr>
<td>controlling static routes in</td>
<td>480, 481</td>
</tr>
<tr>
<td>description</td>
<td>469</td>
</tr>
<tr>
<td>MED to determine routes in</td>
<td>540</td>
</tr>
<tr>
<td>forwarding tables</td>
<td>561</td>
</tr>
<tr>
<td>default learning</td>
<td>698</td>
</tr>
<tr>
<td>Layer 2 bridge domain</td>
<td>696</td>
</tr>
<tr>
<td>four-wire mode (1 port), SHDSL See ATM-over-SHDSL interfaces</td>
<td>540</td>
</tr>
<tr>
<td>FPC (PIM slot on a Services Router) See PIMs fragmentation</td>
<td>405</td>
</tr>
<tr>
<td>configuration by forwarding class</td>
<td>405</td>
</tr>
<tr>
<td>fragmentation, verifying on the link services interface</td>
<td>442</td>
</tr>
<tr>
<td>frame check sequence See FCS</td>
<td>442</td>
</tr>
<tr>
<td>Frame Relay</td>
<td>442</td>
</tr>
<tr>
<td>CoS classification of traffic</td>
<td>876, 878</td>
</tr>
<tr>
<td>Frame Relay encapsulation</td>
<td>876, 878, 879</td>
</tr>
<tr>
<td>congestion control</td>
<td>876, 878, 879</td>
</tr>
<tr>
<td>DLCIs</td>
<td>876, 878, 879</td>
</tr>
<tr>
<td>overview</td>
<td>876, 878, 879</td>
</tr>
<tr>
<td>PVCs</td>
<td>876, 878, 879</td>
</tr>
<tr>
<td>SVCs</td>
<td>876, 878, 879</td>
</tr>
<tr>
<td>virtual circuits</td>
<td>876, 878, 879</td>
</tr>
<tr>
<td>Frame Relay network, typical</td>
<td>876, 878, 879</td>
</tr>
<tr>
<td>Frame Relay, CoS adaptive shaping for</td>
<td>876, 878, 879</td>
</tr>
<tr>
<td>frame-relay-de statement usage guidelines</td>
<td>876, 878, 879</td>
</tr>
<tr>
<td>frames</td>
<td>876, 878, 879</td>
</tr>
<tr>
<td>T3</td>
<td>876, 878, 879</td>
</tr>
<tr>
<td>T1</td>
<td>876, 878, 879</td>
</tr>
<tr>
<td>T3</td>
<td>876, 878, 879</td>
</tr>
</tbody>
</table>

**S**

<table>
<thead>
<tr>
<th>topic</th>
<th>pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>ds2 M-frame format</td>
<td>24</td>
</tr>
<tr>
<td>ds3 c-bit parity frame format</td>
<td>26</td>
</tr>
<tr>
<td>ds3 M13 frame format</td>
<td>25</td>
</tr>
<tr>
<td>Ethernet frame format</td>
<td>18</td>
</tr>
<tr>
<td>sequencing, data link layer</td>
<td>14</td>
</tr>
<tr>
<td>framing</td>
<td>876, 878, 879</td>
</tr>
<tr>
<td>channelized E1 (configuration editor)</td>
<td>122</td>
</tr>
<tr>
<td>channelized T1 (configuration editor)</td>
<td>122</td>
</tr>
<tr>
<td>E1</td>
<td>86</td>
</tr>
<tr>
<td>T1</td>
<td>100</td>
</tr>
<tr>
<td>T3</td>
<td>104</td>
</tr>
<tr>
<td>frequently asked questions See FAQ</td>
<td>587</td>
</tr>
<tr>
<td>FRF.15 and FRF.16 See MLFR FRF.15, MLFR FRF.16</td>
<td>587</td>
</tr>
<tr>
<td>from statement, routing policy match conditions</td>
<td>587</td>
</tr>
<tr>
<td>full mesh requirement</td>
<td>556</td>
</tr>
<tr>
<td>description</td>
<td>556</td>
</tr>
<tr>
<td>fulfilling with confederations</td>
<td>551</td>
</tr>
<tr>
<td>fulfilling with route reflectors</td>
<td>547</td>
</tr>
<tr>
<td>sample network</td>
<td>546</td>
</tr>
<tr>
<td>fxp interfaces, for chassis clusters</td>
<td>74</td>
</tr>
</tbody>
</table>

**G**

<table>
<thead>
<tr>
<th>topic</th>
<th>pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.992.1 Deutsche Telekom UR-2 operating mode</td>
<td>143</td>
</tr>
<tr>
<td>G.992.1 Non-UR-2 operating mode</td>
<td>143</td>
</tr>
<tr>
<td>G.SHDSL interfaces</td>
<td>143</td>
</tr>
<tr>
<td>G.SHDSL interfaces logical properties (configuration editor)</td>
<td>166</td>
</tr>
<tr>
<td>G.SHDSL interfaces physical properties</td>
<td>166</td>
</tr>
<tr>
<td>G.SHDSL PIMs</td>
<td>38</td>
</tr>
<tr>
<td>Annex A or Annex B modes</td>
<td>146</td>
</tr>
<tr>
<td>configuring</td>
<td>145</td>
</tr>
<tr>
<td>default mode</td>
<td>151</td>
</tr>
<tr>
<td>standard supported</td>
<td>38</td>
</tr>
<tr>
<td>See also ATM-over-SHDSL interfaces</td>
<td>38</td>
</tr>
<tr>
<td>Gateway Module See TGM550</td>
<td>38</td>
</tr>
<tr>
<td>ge-0/0/0, disabling PIM on</td>
<td>570</td>
</tr>
<tr>
<td>ge-0/0/0, management interface</td>
<td>77</td>
</tr>
<tr>
<td>See also Gigabit Ethernet ports</td>
<td>77</td>
</tr>
<tr>
<td>Gigabit Ethernet ports</td>
<td>77</td>
</tr>
<tr>
<td>(copper) manual speed and link mode configuration</td>
<td>276</td>
</tr>
<tr>
<td>ARP address</td>
<td>95</td>
</tr>
<tr>
<td>as switches</td>
<td>641</td>
</tr>
<tr>
<td>autonegotiation</td>
<td>96</td>
</tr>
<tr>
<td>CHAP for PPPoA</td>
<td>155</td>
</tr>
<tr>
<td>dynamic CAC for voice packets (configuration editor)</td>
<td>276</td>
</tr>
<tr>
<td>See also Avaya VoIP</td>
<td>276</td>
</tr>
<tr>
<td>logical interfaces</td>
<td>95</td>
</tr>
<tr>
<td>MAC address</td>
<td>95</td>
</tr>
<tr>
<td>MTU</td>
<td>96</td>
</tr>
<tr>
<td>MTU default and maximum values</td>
<td>56</td>
</tr>
<tr>
<td>overview</td>
<td>15</td>
</tr>
<tr>
<td>PPPoE session on</td>
<td>291</td>
</tr>
<tr>
<td>Quick Configuration</td>
<td>94</td>
</tr>
<tr>
<td>source filtering, for MAC addresses</td>
<td>96</td>
</tr>
<tr>
<td>static ARP entries (configuration editor)</td>
<td>111</td>
</tr>
<tr>
<td>Global System for Mobile Communications (GSM) See GSM</td>
<td>111</td>
</tr>
<tr>
<td>global unicast IPv6 addresses</td>
<td>69</td>
</tr>
</tbody>
</table>
glossary
Avaya VoIP ..........................................................257
channelized T1/E1/ISDN PRI ....................................117
CoS ....................................................................790
DSL .....................................................................133
interfaces ................................................................4
ISDN ......................................................................309
link services ..........................................................399
ports .....................................................................4
PPPoE ....................................................................290
USB modern ..........................................................385
gr-0/0/0 interface ....................................................74
gre interface ...........................................................74
GRE tunnels, configuring CoS queuing .......................884
grounding
Avaya VoIP 10 AWG replacement cable .......................244
grounding cable required for TGM550 .........................267
groups
BGP See BGP groups
OSPF areas ................................................................511
RIP routers ............................................................492
GSM (Global System for Mobile Communications)
profile ....................................................................361, 368
supported wireless modem cards ..............................357
unlocking SIM .......................................................381
GVRP
configuring ............................................................673

H
handling packet fragments ........................................632
hardware
Avaya VoIP module overview ....................................244
supported platforms .................................................xxxviii
hardware capabilities and limitations
SRX3400 and SRX3600 devices ..................................913
hardware features
Avaya VoIP modules ................................................244
HDB3 encoding .......................................................21
HDLC (High-Level Data Link Control)
encapsulation .........................................................63
HDLC operational modes .........................................63
HDLC stations ........................................................63
hello PDUs ............................................................527
hierarchical schedulers
controlling remaining traffic ......................................923
example ...................................................................918
introduction ...........................................................917
nodes ......................................................................915
priority propagation ................................................927
terminology ............................................................912
high-density bipolar 3 code (HDB3) encoding .......... 21
High-Level Data Link Control See HDLC
high-priority CoS queuing ........................................893
hold time, to maintain a session ................................536
hop count, maximizing .............................................486
See also RIP
host reachability
verifying for an OSPF network ..................................522
verifying for RIP network hosts ...............................501
hostname
for PPPoE CHAP ...................................................156
for PPPoE CHAP (Quick Configuration) ..................295
IS-IS identifier-to-hostname mapping .......................526
IVBGP (internal BGP)
description .............................................................556
full mesh (configuration editor) ...............................543
sample network .....................................................546
sample route reflector .............................................550
ICMP (Internet Control Message Protocol),
policers ....................................................................624
IEEE 802.1 CoS value type, aliases and values ..............805
See also CoS
IEEE 802.3ad standard
Ethernet link aggregation .........................................449
IG550 Integrated Gateway See Avaya IG550 Integrated
Gateway, Avaya VoIP modules See Avaya VoIP
modules
IGMP (Internet Group Management Protocol)
IGMPv1 ..................................................................563
IGMPv2 ..................................................................563
IGMPv3 ..................................................................563
setting the version ..................................................567
verifying the version ...............................................576
IGMP Snooping .......................................................651
working ....................................................................651
IGMP snooping
configuring ............................................................671
IGP plus MED, BGP option .......................................541
IGP route metric, role in BGP route selection ...............537
IGPs (interior gateway protocols) ..................468, 737
VPNs ......................................................................737
See also OSPF
import routing policy, for Layer 2 VPNs .....................748
import statement, for routing policies .......................585
inbound router, in an LSP .......................................711
incoming calls
rejecting ...................................................................341
screening ..................................................................340
incoming metric (RIP)
description .............................................................493
modifying .............................................................495
inet protocol family ..................................................64
inet routing table .....................................................573
inet6 protocol family ................................................64
ingress router See inbound router, LSPs
integrated routing and bridging interface ....................692
configuration ........................................................694
### Index

**Integrated Services Digital Network** See ISDN
- interface naming conventions ........................................ 9
- interface set caveats ..................................................... 916

**Interfaces**
- aggregated Ethernet .................................................. 450
- ATM-over-ADSL interfaces ............................................ 34
- ATM-over-SHDSL interfaces .......................................... 38
- Avaya VoIP ................................................................. 261
  - See also Avaya VoIP modules
- channelized T1/E1/ISDN PRI interfaces ......................... 23
- clocking ................................................................. 54
- data link layer ......................................................... 14
- E1 interfaces ............................................................ 19
- E3 interfaces ............................................................ 23
- Ethernet interfaces ..................................................... 15
- G.SHDSL interfaces .................................................... 38
- IPv4 addressing .......................................................... 65
- IPv6 addressing ........................................................ 68
- ISDN interfaces .......................................................... 49
- logical properties ....................................................... 64
- MTU values ............................................................... 56
- overview ................................................................. 3
  - See also ATM-over-ADSL interfaces;
    ATM-over-SHDSL interfaces; channelized interfaces;
    ISDN interfaces; link services interface; loopback interface;
    management interfaces; network interfaces; ports;
    special interfaces

- physical encapsulation ............................................. 57
  - See also encapsulation type
- physical properties ................................................... 52
- protocol families ....................................................... 64
- Quick Configuration ................................................... 82
- redundant Ethernet ..................................................... 454
- serial interfaces ........................................................ 28
- special interfaces ....................................................... 74
- supported for dynamic CAC, for Avaya VoIP .................. 264
  - See also dynamic CAC
- T1 interfaces ............................................................ 19
- T3 interfaces ............................................................ 23
- VLANs ....................................................................... 72
- VoIP ........................................................................ 261
  - See also Avaya VoIP modules
- VPLS ......................................................................... 774, 777
- VPLS encapsulation types ............................................ 775

**Interfaces page**
- for E1 ................................................................. 84
- for E3 ................................................................. 87
- for Fast Ethernet ....................................................... 91
- for serial interfaces .................................................. 105
- for T1 ................................................................. 98
- for T3 (DS3) .......................................................... 102

**Intermediate System-to-Intermediate System** See IS-IS
- internal BGP See IBGP
- internal clocking mode ................................................. 30
- internal scheduler nodes ............................................. 926
- Internet Control Message Protocol policers .................. 624
- Internet Group Management Protocol See IGMP
- Internet routing, with BGP .......................................... 535
- Internet-based over the air See IOTA
- introduction to hierarchical schedulers ...................... 917
- inverting the transmit clock ....................................... 107
- IOC hardware properties .......................................... 930
- IOCs (I/O Cards) See IOC number
  - slot number .......................................................... 11
- IOCs (Input/Output Cards)
  - abbreviations ....................................................... 13
  - names ................................................................. 13
- IOTA (Internet-based over the air), account activation .... 380
- IP addresses ........................................................... 65
  - as IS-IS system identifiers ..................................... 526
  - Avaya VoIP module, guidelines for ......................... 266
  - TGM550, guidelines for ....................................... 266
  - See also addresses; IPv4 addressing; IPv6 addressing
- IP precedence CoS value type, aliases and values ........ 805
  - See also CoS
- ip telnet port command ............................................... 281
- ip telnet-client command ........................................... 281
- ip-0/0/0 interface ..................................................... 74
  - ip-interf command ................................................ 74
- overview ............................................................... 74
- IPv4 addressing
  - assigning for PPPoE (Quick Configuration) ................. 295
  - classful addressing .............................................. 65
  - dotted decimal notation ....................................... 66
  - MAC-48 address format ........................................ 15
  - overview ........................................................... 65
  - subnets ............................................................... 66
  - VLSMs ................................................................. 67

**IPv6**
- BA classifier .......................................................... 949
- Class of Service ....................................................... 947

**IPv6 addressing**
- address format ......................................................... 68
- address scope ........................................................ 69
- address structure ..................................................... 69
- address types ........................................................ 69
- overview ............................................................... 68

**IPv6, enabling** ....................................................... 71

**IS-IS (Intermediate System-to-Intermediate System)**
- adjacency establishment with hello PDUs ...................... 527
- areas ................................................................. 525
- ASs ................................................................. 525
- CSNPs .............................................................. 528
- enabling on router interfaces .................................... 529
- enabling on routers in secure context ......................... 529
- for CLNS route exchange ....................................... 762
- hello PDUs ......................................................... 527
LSPs..........................................................528
NETs..........................................................526
See also NETs
NSAP addresses.................................526
path selection........................................527
preparation...........................................529
PSNPs.....................................................528
system identifiers..............................526
See also system identifiers
verifying adjacencies..........................533
verifying adjacencies (detail).............533
verifying interface configuration.........531
verifying interface configuration (detail)........532
verifying neighbors..........................533
verifying neighbors (detail)...............533
with CLNS.............................................757
ISDN BRI Dialer Logical Interface page..319
ISDN BRI interfaces
adding an interface.........................321
B-channel interface..........................312
bandwidth on demand (configuration
editor).............................................336
call setup...........................................51
callback See callback
calling number..................................316, 323
connection initialization...................51
D-channel interface.........................312
dial backup.................................318, 327 See dial backup
dial-in See dial-in
dial-on-demand routing backup, with OSPF........331
dialer filter See dialer filter
dialer interface See dialer interface, ISDN
dialer watch See dialer watch
disabling dial-out (configuration editor).....342
disabling ISDN signaling (configuration
editor).............................................343
ISDN channels.....................................49
MTU default and maximum values.........56
naming conventions..........................312
NT1 devices........................................51
overview..........................................50

See also ISDN connections
PIMs supported.................................312
Q.931 timer.......................................317, 323
Quick Configuration.........................314
requirements.......................................313
S/T interfaces.................................51, 312
screening incoming calls...................540
session establishment.......................52
SPID.................................................316, 323
static TEI..........................................317, 323
switch types....................................316, 323
TEI option......................................317, 324
typical network.................................50
U interface........................................51, 312
verifying B-channels.........................346
verifying call status..........................349
verifying D-channels..........................347
verifying ISDN interfaces.................345
verifying ISDN status.........................344
ISDN BRI Physical Interface page........314
ISDN BRI ports
for TIM521 See TIM521
ISDN connections
adding an ISDN BRI interface.............321
adding an ISDN PRI interface...............125
bandwidth on demand.......................332
callback See callback
calling number..................................316, 323
configuring.......................................309
dial backup See dial backup
dial-in See dial-in
dial-on-demand routing backup, with OSPF........331
dialer filter See dialer filter
dialer interface See dialer interface, ISDN
dialer watch See dialer watch
disabling dial-out (configuration editor).....342
disabling ISDN signaling (configuration
editor).............................................343
interface naming conventions.............312
ISDN interface types........................312
overview..........................................312

See also dialer interfaces; ISDN BRI interfaces;
ISDN PRI interfaces
Q.931 timer.......................................317, 323
Quick Configuration (ISDN BRI)............314
requirements.......................................313
SPID...............................................316, 323
static TEI..........................................317, 323
switch types....................................119, 316, 323
TEI option......................................317, 324
verifying B-channels.........................346
verifying call status..........................349
verifying D-channels..........................347
verifying dialer interfaces...............345
verifying ISDN BRI interfaces............345
verifying ISDN PRI interfaces..........345
verifying ISDN status.........................344
ISDN PRI interfaces
adding............................................125
B-channel allocation order...............127
B-channel interface.........................313
bandwidth on demand.......................356
callback See callback
channelized interface.......................312
D-channel interface.........................313
dial backup.................................327
dial-in See dial-in
dialer filter...................................328
dialer interface See dialer interface, ISDN
dialer options.................................128
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya VoIP connectivity</td>
<td>237</td>
</tr>
<tr>
<td>Avaya VoIP modules</td>
<td>244</td>
</tr>
<tr>
<td>USB modem</td>
<td>383</td>
</tr>
<tr>
<td>ATM-over-ADSL interfaces</td>
<td>140</td>
</tr>
<tr>
<td>ATM-over-SHDSL interfaces</td>
<td>150</td>
</tr>
<tr>
<td>Avaya VoIP</td>
<td>272</td>
</tr>
<tr>
<td>channelized E1 interfaces</td>
<td>120</td>
</tr>
<tr>
<td>channelized T1 interfaces</td>
<td>120</td>
</tr>
<tr>
<td>CHAP on ATM-over-ADSL interfaces</td>
<td>155</td>
</tr>
<tr>
<td>CHAP on ATM-over-SHDSL interfaces</td>
<td>155</td>
</tr>
<tr>
<td>CHAP on dialer interfaces</td>
<td>397</td>
</tr>
<tr>
<td>CoS</td>
<td>833</td>
</tr>
<tr>
<td>CoS, large delay buffers</td>
<td>900</td>
</tr>
<tr>
<td>CoS, strict high priority for queuing</td>
<td>893</td>
</tr>
<tr>
<td>CRTP</td>
<td>450</td>
</tr>
<tr>
<td>ISDN connections</td>
<td>321</td>
</tr>
<tr>
<td>LPI</td>
<td>413</td>
</tr>
<tr>
<td>MLPPP bundles</td>
<td>413</td>
</tr>
<tr>
<td>network interfaces</td>
<td>109</td>
</tr>
<tr>
<td>network interfaces, adding</td>
<td>110</td>
</tr>
<tr>
<td>network interfaces, deleting</td>
<td>112</td>
</tr>
<tr>
<td>PAP on dialer interfaces</td>
<td>396</td>
</tr>
<tr>
<td>USB modem connections</td>
<td>386</td>
</tr>
<tr>
<td>VoIP</td>
<td>272</td>
</tr>
<tr>
<td>ITU G.992.1 operating mode</td>
<td>143</td>
</tr>
<tr>
<td>ITU DMT bis operating mode</td>
<td>143</td>
</tr>
<tr>
<td>ITU DMT operating mode</td>
<td>143</td>
</tr>
<tr>
<td>ITU Annex B non-UR-2 operating mode</td>
<td>143</td>
</tr>
<tr>
<td>ITU Annex B UR-2 operating mode</td>
<td>143</td>
</tr>
<tr>
<td>IS-IS (Intermediate System-to-Intermediate System)</td>
<td>526</td>
</tr>
<tr>
<td>ISO protocol family</td>
<td>64</td>
</tr>
<tr>
<td>verifying B-channels</td>
<td>346</td>
</tr>
<tr>
<td>verifying call status</td>
<td>349</td>
</tr>
<tr>
<td>verifying configuration</td>
<td>130</td>
</tr>
<tr>
<td>verifying D-channels</td>
<td>347</td>
</tr>
<tr>
<td>verifying ISDN interfaces</td>
<td>346</td>
</tr>
<tr>
<td>verifying ISDN status</td>
<td>344</td>
</tr>
<tr>
<td>J-Web configuration editor</td>
<td>383</td>
</tr>
<tr>
<td>PIM supported</td>
<td>118</td>
</tr>
<tr>
<td>Q 931 timers</td>
<td>128</td>
</tr>
<tr>
<td>screening incoming calls</td>
<td>340</td>
</tr>
<tr>
<td>supported switch types</td>
<td>119</td>
</tr>
<tr>
<td>transmission</td>
<td>119</td>
</tr>
<tr>
<td>J2320</td>
<td></td>
</tr>
<tr>
<td>Avaya VoIP modules</td>
<td>244</td>
</tr>
<tr>
<td>TGM550</td>
<td>247</td>
</tr>
<tr>
<td>TIM508</td>
<td>250</td>
</tr>
<tr>
<td>TIM510</td>
<td>251</td>
</tr>
<tr>
<td>TIM514</td>
<td>253</td>
</tr>
<tr>
<td>TIM516</td>
<td>254</td>
</tr>
<tr>
<td>TIM518</td>
<td>255</td>
</tr>
<tr>
<td>TIM521</td>
<td>256</td>
</tr>
<tr>
<td>J2350</td>
<td></td>
</tr>
<tr>
<td>Avaya VoIP modules</td>
<td>244</td>
</tr>
<tr>
<td>TGM550</td>
<td>247</td>
</tr>
<tr>
<td>TIM508</td>
<td>250</td>
</tr>
<tr>
<td>TIM510</td>
<td>251</td>
</tr>
<tr>
<td>TIM514</td>
<td>253</td>
</tr>
<tr>
<td>TIM516</td>
<td>254</td>
</tr>
<tr>
<td>TIM518</td>
<td>255</td>
</tr>
<tr>
<td>TIM521</td>
<td>256</td>
</tr>
<tr>
<td>J4350</td>
<td></td>
</tr>
<tr>
<td>Avaya VoIP modules</td>
<td>244</td>
</tr>
<tr>
<td>J4350 routers</td>
<td></td>
</tr>
<tr>
<td>Avaya VoIP connectivity</td>
<td>237</td>
</tr>
<tr>
<td>manual copper Gigabit Ethernet speed and link mode configuration</td>
<td>97</td>
</tr>
<tr>
<td>MTU values</td>
<td>56</td>
</tr>
<tr>
<td>slot number</td>
<td>11</td>
</tr>
<tr>
<td>T3 (DS3) and E3 support</td>
<td>7</td>
</tr>
<tr>
<td>J6500</td>
<td></td>
</tr>
<tr>
<td>TGM550</td>
<td>247</td>
</tr>
<tr>
<td>TIM508</td>
<td>250</td>
</tr>
<tr>
<td>TIM510</td>
<td>251</td>
</tr>
<tr>
<td>TIM514</td>
<td>253</td>
</tr>
<tr>
<td>TIM516</td>
<td>254</td>
</tr>
<tr>
<td>TIM518</td>
<td>255</td>
</tr>
<tr>
<td>TIM521</td>
<td>256</td>
</tr>
<tr>
<td>J6550</td>
<td></td>
</tr>
<tr>
<td>Avaya VoIP modules</td>
<td>244</td>
</tr>
<tr>
<td>J6550 routers</td>
<td></td>
</tr>
<tr>
<td>Avaya VoIP connectivity</td>
<td>237</td>
</tr>
<tr>
<td>manual copper Gigabit Ethernet speed and link mode configuration</td>
<td>97</td>
</tr>
<tr>
<td>MTU values</td>
<td>56</td>
</tr>
<tr>
<td>slot number</td>
<td>11</td>
</tr>
<tr>
<td>T3 (DS3) and E3 support</td>
<td>7</td>
</tr>
</tbody>
</table>
jitter, removing on multilink bundles.........................440
JUNOS Internet software
  Avaya VoIP configurability with..........................262
  Avaya VoIP connectivity.................................237
  TGM550 firmware compatibility with......................266
JUNOS Software
  CoS components...........................................793
  CoS implementation.........................................801
  ISDN connections...........................................309
  USB modem...................................................383

K
  keepalive messages, for session hold time..............536

L
  Label Distribution Protocol See LDP
  label switching.............................................710
  label-switched paths See LSPs
  label-switching routers (LSRs).............................711
  labels, MPLS..................................................712
    label operations...........................................712
    PHP..................................................................713
  LACP
    configuring..................................................663
  LACP (Link Aggregation Control Protocol)
    configuring on chassis clusters.......................458
    configuring on standalone devices....................457
    understanding...............................................455
    understanding in chassis cluster mode.................456
  LANs
    bridges on LAN segments................................18
    collision domains..........................................17
    repeaters on LAN segments...............................17
    topology.....................................................73
  latency, reducing on multilink bundles..................440
  Layer 2 bridging
    default forwarding behavior............................691
    integrated routing and bridging interface..........692
      SRX3400, SRX3600, SRX5600, SRX5800
        devices.....................................................678
      SRX3400, SRX3600, SRX5600, SRX5800 services
        devices.....................................................676
        terms.......................................................678
  Layer 2 circuits
    AS number...................................................747
    basic, description.........................................755
    encapsulation..............................................742
    IGPsin................................................................737
    MPLS..........................................................744
    neighbor address..........................................744
    participating interfaces................................742
    signaling protocols........................................737
    verifying PE router connections.......................756
    verifying PE router interfaces.........................756
    virtual circuit ID...........................................755
  Layer 2 forwarding tables..................................696
  Layer 2 interfaces
    configuration................................................682
    security zones..............................................684
    SRX3400, SRX3600, SRX5600, and SRX5800
      devices.......................................................680
  Layer 2 security zones.....................................684
  Layer 2 switching
    supported devices.........................................642
  Layer 2 VPNs
    AS number...................................................747
    basic, description.........................................750
    BGP.............................................................744
    encapsulation..............................................742
    export routing policies..................................748
    IGPsin................................................................737
    import routing policies...................................748
    MPLS..........................................................744
    participating interfaces.................................742
    routing instance.............................................747
    signaling protocols........................................737
    verifying PE router connections.......................749
    verifying PE router interfaces.........................749
  Layer 3 VPNs
    AS number...................................................747
    basic, description.........................................750
    BGP.............................................................744
    encapsulation..............................................742
    export routing policies..................................748
    IGPsin................................................................737
    import routing policies...................................748
    MPLS..........................................................744
    participating interfaces.................................742
    route target.................................................739
    routing instance.............................................747
    routing policies.............................................752
    signaling protocols........................................737
    verifying PE router connections.......................753
  LCP (Link Control Protocol), connection process.......59
  LDP (Label Distribution Protocol)
    and OSPF for VPNs...........................................745
    overview.......................................................720
    requirements..................................................721
    leaves..........................................................560
    See also multicast
  LEDs
    ACT (TGM550 active)........................................250
    ACT (TIM508 active).........................................251
    ACT (TIM510 active).........................................252
    ACT (TIM514 active).........................................254
    ACT (TIM516 active).........................................255
    ACT (TIM518 active).........................................256
    ACT (TIM521 active).........................................257
    ALM (TGM550 alarm)........................................250
    ALM (TIM508 alarm).........................................251
    ALM (TIM510 alarm).........................................252
ALM (TIM514 alarm) ........................................... 254
ALM (TIM516 alarm) ........................................... 255
ALM (TIM518 alarm) ........................................... 256
ALM (TIM521 alarm) ........................................... 257
ASB (alternate software bank) .................................. 250
ETR (emergency transfer relay) .................................. 250
SIG (signal) .......................................................... 252
TGM550 port status ............................................... 250
TIM508 link status .................................................. 251
TIM510 link status .................................................. 252
TIM514 link status .................................................. 254
TIM516 link status .................................................. 255
TIM518 link status .................................................. 256
TIM521 link status .................................................. 257
TST (test) ............................................................... 252
Level 1 areas, IS-IS ................................................. 525
Level 2 areas, IS-IS ................................................. 525
LFI (link fragmentation and interleaving)
  enabling (configuration editor) .................................. 416
  overview ........................................................... 403
See also link services interface
  with CoS components .......................................... 409
LINE and TRUNK ports, on Avaya VoIP TGM550 ............. 247
  line buildout .......................................................... 101
  T1 ................................................................. 104
LINE ports, TIM514 .................................................. 253
  line speed
    ATM-over-SHDSL interfaces .................................... 149
    serial interfaces .................................................. 108
  line timing ............................................................ 30
Link Aggregation Control Protocol See LACP
link aggregation, Ethernet
  overview ............................................................... 449
link fragmentation and interleaving See LFI
link hold time, channelized ports .................................. 121
link services ........................................................... 78
See also link services interface: lsq-0/0/0
link services intelligent queuing interface
  channels, with MLFR FRF.16 (configuration editor) ............... 427
  classifiers and forwarding classes (configuration editor) .......... 417
  CRTP (configuration editor) ......................................... 430
  MLFR FRF.16 bundles (configuration editor) .......................... 427
  scheduler maps (configuration editor) ............................... 420
  shaping rates, applying (configuration editor) ...................... 423
  verifying .............................................................. 431
link services interface
  applying CoS components on constituent links .................. 439
  configuring .......................................................... 399
  CoS components ........................................................ 409
  See also CoS components for link services displaying CoS configurations ....... 432
  FAQ ................................................................. 439
  fragmentation, troubleshooting ...................................... 442
  J Series implementation exceptions ................................ 402
  LFI See LFI
  load balancing, troubleshooting .................................... 444
  MLFR bundles (Quick Configuration) .................................. 410
  MLFR FRF.15 bundles (configuration editor) ......................... 424
  MLPPP bundles (Quick Configuration) .................................. 410
  MLPPP header overhead ............................................. 443
  multilink bundles See multilink bundles
  overview ............................................................... 400
  See also lsq-0/0/0
  packet encapsulation, troubleshooting ................................ 443
  PPP header overhead .................................................. 445
  preventing dropped packets on PVCs .................................. 447
  Quick Configuration ................................................... 410
  reducing jitter and latency on multilink bundles ................. 440
  requirements ......................................................... 410
  sample CoS configuration ........................................... 432
  services on ........................................................... 401
  troubleshooting ....................................................... 439
  troubleshooting LFI and load balancing .............................. 441
  verifying CoS configuration .......................................... 437
  verifying status ....................................................... 434
  link states, verifying ............................................... 113
  link-layer overhead
    configuration ......................................................... 406
  link-local unicast IPv6 addresses .................................... 69
  link-state advertisements See LSAs
  link-state PDUs See LSPs
  lo0 interface functions .............................................. 76
  See also loopback interface
  lo0.16385, internal loopback address .................................. 75
load balancing on link services interfaces
  FAQ ................................................................. 441
  troubleshooting ....................................................... 441
  verifying .............................................................. 444
local preference
  description ........................................................... 538
  high value preferred ............................................... 538
  role in BGP route selection ......................................... 537
logical interfaces
  adaptive shaping for ................................................. 875
  adding (configuration editor) ........................................ 111
  assigning CoS components to (Quick Configuration) ............... 831
  ATM-over-ADSL (configuration editor) ................................ 144
  ATM-over-ADSL (Quick Configuration) ................................ 156
  ATM-over-SHDSL .................................................... 153
  ATM-over-SHDSL (Quick Configuration) ................................ 148
  CoS rules for ......................................................... 864, 875
  E1 ................................................................. 85
  E3 ................................................................. 88
  Fast Ethernet ......................................................... 91
  Gigabit Ethernet ..................................................... 95
serial ............................................................ 106
T1 ................................................................. 99
T3 ................................................................. 103
virtual channels for ....................................... 864
logical units
adding (configuration editor) ......................... 111
ATM-over-ADSL interface (Quick
Configuration) .................................................. 136
ATM-over-SHDSL interface (Quick
Configuration) .................................................. 148
E1 interface .................................................... 85
E3 interface .................................................... 88
Fast Ethernet interface .................................. 91
Gigabit Ethernet interface ............................. 95
number in interface name ................................ 12
serial interface .............................................. 106
T1 interface .................................................... 99
T3 interface .................................................... 103
loop clocking mode ........................................ 30
loopback address, internal, lo0.16385 ...... 75
loopback interface
functions ....................................................... 76
NET on for IS-IS .............................................. 529
loopback interface, applying stateless firewall filters to
(configuration editor) ........................................... 624
loopback signals, E1 and T1 ......................... 22
loopback testing, SHDSL ............................... 150
loss priorities .................................................. 796
loss-priority-maps statement ............................. 877
LSAs (link-state advertisements)
description ..................................................... 503
two-way handshake ....................................... 503
li interface ...................................................... 75
LSPs (label-switched paths)
description ..................................................... 710
dynamic LSPs .................................................. 713
for RSVP in a VPN .......................................... 744
label operations ............................................ 712
label switching .............................................. 710
labels ........................................................... 712
LSR types ...................................................... 711
PHP ............................................................ 713
static LSPs .................................................... 713
LSPs (link-state PDUs)
CSNPs .......................................................... 528
overview ....................................................... 528
PSNPs .......................................................... 528
lsq-0/0/0
configuring ..................................................... 399
See also link services interface
interface description ....................................... 75
LSRs (label-switching routers) ...................... 711
I/O-0/0/0 interface .......................................... 75
M
M13 frame format ............................................. 25
MAC (media access control) addresses
as IS-IS system identifiers .................................. 526
associating with IP addresses on Ethernet
subnets .......................................................... 111
EUI-64 addresses .......................................... 15
for static ARP on Fast Ethernet subnets .......... 92
See also static ARP entries
for static ARP on Gigabit Ethernet subnets ...... 95
See also static ARP entries
in static ARP entries (configuration editor) .... 111
MAC-48 address format .................................... 15
overview ....................................................... 15
physical addressing ........................................ 14
source filtering on Gigabit Ethernet ports ... 96
MAC-48 addresses ........................................... 15
magic numbers, PPP ........................................ 61
management interfaces
overview ..................................................... 77
management interfaces, disabling PIM on ...... 570
manuals
Avaya VoIP .................................................... 263
comments on ................................................. xl
mapping calculated weights ......................... 938
mapping, CoS forwarding classes to
schedulers ..................................................... 824, 861
match conditions
routing policy ............................................... 587
routing policy, summary of ............................ 587
stateless firewall filters ................................. 610
stateless firewall filters, summary .......... 610, 613
match types .................................................... 591
maximum hop count, RIP .................................. 486
maximum transmission unit See MTU
MDRR on the IOC ............................................. 935
MED (multiple exit discriminator)
always compare option .................................. 541
Cisco non-deterministic option ............. 541
default use ................................................... 540
description ..................................................... 540
path selection options ................................. 541
plus IGP option ............................................... 541
role in BGP route selection ......................... 537
media access control See MAC addresses
Media Gateway Controller See Avaya Media Gateway
Controller; MGC list
media types supported .................................... 9
memory stick, USB, for Avaya VoIP
configuration ............................................... 268
metrics See MED; path cost metrics
MP classifier ............................................... 835
MGC See Avaya Media Gateway Controller; MGC list
MGC list
clearing ....................................................... 275
configuring ................................................... 273
multicast routing modes
- dense mode .................................................. 562
- dense mode, caution for use ........................ 561
- sparse mode ............................................... 562
Multicast Source Discovery Protocol .................. 563
multiclass MLPPP
- configuration ............................................. 407
- multfield classifier ...................................... 835
multilink bundles
- classifiers and forwarding classes (configuration editor) ........................................ 417
- displaying configurations ............................. 431
- LFI (configuration editor) .............................. 416
- MLFR FRF.15 (configuration editor) .............. 424
- MLFR FRF.16 (configuration editor) .............. 427
- overview .................................................. 402
- preventing dropped packets ......................... 447
- queuing, on Q2 of constituent links .............. 409
Quick Configuration options .......................... 411
- reducing latency ........................................ 440
- removing jitter .......................................... 440
- sample configuration ................................ 431
- sample topology ......................................... 414
- scheduler maps (configuration editor) .......... 420
- scheduling priority .................................... 410
- shaping rate ............................................. 409
- shaping rates (configuration editor) ............ 423
Multilink Frame Relay See MLFR
Multilink Frame Relay end-to-end See MLFR FRF.15
Multilink Frame Relay Forum See MLFR FRF.15; MLFR FRF.16
Multilink Point-to-Point Protocol See MLPPP
multilink services
- configuring ................................................. 399
- overview .................................................. 78
- See also CRTP, link services interface, MLFR, MLPPP
multiple exit discriminator See MED
multiple push label operation .......................... 712

n-selectors, in IS-IS NET addresses ................. 526
names, of network interfaces .......................... 10
NC forwarding class ...................................... 806
See also CoS, forwarding classes
NCPs (Network Control Protocols) ....................... 60
neighbors See adjacencies, IS-IS, BGP peers; OSPF neighbors; RIP neighbors
NETs (network entity titles)
- n-selectors .................................................. 526
- on an Ethernet interface ............................. 529
- on the loopback interface ............................ 529
- parts ......................................................... 526
- system identifier ....................................... 526

network control (NC) forwarding class .......... 806
See also CoS, forwarding classes
Network Control Protocols (NCPs) ...................... 60
network entity titles See NETs
network interfaces
- adding ....................................................... 110
- assigning CoS components to (Quick Configuration) ................. 831
- ATM-over-ADSL configuration ...................... 140
- ATM-over-ADSL interfaces .......................... 34
- ATM-over-SHDSL configuration .................... 150
- ATM-over-SHDSL interfaces ......................... 38
- channelized E1 configuration ....................... 120
- channelized T1 configuration ....................... 120
- channelized T1/E1/ISDN PRI interfaces .......... 23
- clocking ................................................... 54
- deleting .................................................... 112
- DS3 configuration ....................................... 101
- E1 configuration ....................................... 84
- E1 interfaces ............................................ 19
- E3 configuration ....................................... 87
- E3 interfaces ............................................ 23
- enabling PIM on ....................................... 570
- Ethernet interfaces .................................... 15
- Fast Ethernet configuration ......................... 90
- FCS ......................................................... 55
- G.SHDSL interfaces .................................... 38
- Gigabit Ethernet configuration ..................... 94
- IPv4 addressing ........................................ 65
- IPv6 addressing ........................................ 68
- ISDN interfaces ........................................ 49
- link services interface ................................ 399
- logical properties ...................................... 64
- media types .............................................. 9
- MTU values ............................................... 56
- multicast, upstream and downstream ............. 560
- names ..................................................... 10
- naming conventions ................................... 9
- output, understanding ................................ 12
- physical encapsulation ............................... 57
- See also encapsulation type
- physical properties .................................... 52
- preparation .............................................. 81, 120
- protocol families ...................................... 64
- Quick Configuration .................................. 82
- sample name ............................................ 12
- serial configuration ................................... 104
- serial interfaces ....................................... 28
- supported ................................................ 8
- T1 configuration ....................................... 97
- T1 interfaces .......................................... 19
- T3 configuration ....................................... 101
- T3 interfaces .......................................... 23
- verifying ATM-over-ADSL properties .......... 157
- verifying ATM-over-SHDSL configuration ...... 160
- verifying channelized interfaces ................. 128
network layer reachability information See NLRI
network service access point (NSAP) addresses for IS-IS routers.................................................................526
network service access points See NSAPs
networks
Avaya VoIP.....................................................................261
designated router See designated router, OSPF
IPV4 subnets ....................................................................66
path cost metrics See path cost metrics
PPPoe session on an ATM-over-ADSL loop..................292
PPPoe session on an Ethernet loop..........................291
sample BGP AS path..................................................539
sample BGP confederation........................................553
sample BGP confederations........................................552
sample BGP external and internal links.......................546
sample BGP local preference use...........................538
sample BGP MED use................................................540
sample BGP peer network........................................544
sample BGP peer session..........................................543
sample BGP route reflector (one cluster)...............547, 550
sample BGP route reflectors (cluster of clusters)........549
sample BGP route reflectors (multiple clusters)........548
sample distance-vector routing..................................486
sample LFI and multilink bundle topology...............414
sample LSP topology................................................711
sample multiarea OSPF routing.................................508
sample multilink bundle and LFI topology...............414
sample OSPF backbone area..................................509
sample OSPF network with stubs and NSSAs.................513
sample OSPF single-area network............................510
sample OSPF stub areas and NSSAs........................514
sample OSPF topology...............................................521
sample poison reverse routing.................................488
sample RIP network with incoming metrics...............494
sample RIP network with outgoing metrics...............496
sample RIP topology................................................492
sample route advertisement....................................471
sample route aggregation.....................................472
sample routing topology........................................469
sample RSVP topology............................................727
sample split horizon routing..................................487
sample static route, preferred path..........................479
sample stub network for static routes.....................476
sample unidirectional routing.................................488
static routing......................................................470
VoIP........................................................................261
next hop
defining for static routes..................................477
qualified, defining for static routes.......................479
qualified, for static routes..................................477
role in BGP route selection..................................537
NLRI (network layer reachability information), BGP
for CLNS.............................................................764
for VPNs ..........................................................739
no ip telnet command............................................281
no ip telnet-client command..................................281
nodes
hierarchical schedulers........................................913
non-LFI packets See data packets
non-UR-2 operating mode........................................143
Normal Response Mode, HDLC...............................63
not-so-stubby areas See NSSAs
notice icons................................................................xxviii
NRM, HDLC..............................................................63
NSAP (network service access point) addresses for IS-IS routers.................................................................526
NSAPs (network service access points)
overview...............................................................757
sample configurations...........................................763
NSSAs (not-so-stubby areas)
area ID (configuration editor)...................................512
creating (configuration editor).............................514
description........................................................513
example............................................................514
sample topology...................................................514
NT1 devices...........................................................51
numeric range match conditions............................610, 613

O
Open Shortest Path First protocol See OSPF
Open Systems Interconnection (OSI) networks, CLNS
VPNs..................................................................757
origin, of BGP route................................................539
orlonger route list match type..................................591
OSI (Open Systems Interconnection) networks, CLNS
VPNs..................................................................757
OSPF (Open Shortest Path First)
and LDP for VPNs................................................745
and RSVP for VPNs.............................................746
area border routers See area border routers
areas.....................................................................508
See also area border routers; backbone area;
NSSAs; stub areas
authenticating exchanges (OSPFv2 only)..................515
backbone area See backbone area
to controlling designated router election.................507
controlling route cost.................................................518
designated router See designated router, OSPF
designating OSPF interfaces (configuration editor)........510, 512
dial-on-demand routing backup support,
  ISDN..................................................................331
  enabling, description.........................................506, 509, 511, 514
  ensuring efficient operation..................................517
injecting OSPF routes into BGP...............................597
ISDN dial-on-demand routing backup support.............331
LSAs..................................................................503
multiarea network (configuration editor)....................511
NSSAs See NSSAs
overview................................................................503
path cost metrics See path cost metrics
requirements................................................................504
route preferences.............................................519
router ID (configuration editor)...............................506, 507
sample network topology.......................................521
sample NSSAs......................................................514
sample single-area network....................................510
sample stub areas.............................................514
single-area network (configuration editor)..................509
stub areas See stub areas
tunneled links..........................................................503
validating an OSPF network......................................517
verifying host reachability.....................................522
verifying OSPF neighbors.......................................520
verifying RIP-enabled interfaces..............................519
verifying routes................................................521
VPLS..................................................................783
OSPF interfaces
  enabling (configuration editor).........................510, 512
  enabling, for area border routers.......................512
  verifying...........................................................519
OSPF neighbors, verifying.........................................520
OTASP (over the air service provisioning), account
  activation................................................................378
out-of-band management interfaces...........................77
outbound router, in an LSP.........................................711
outgoing metric (RIP)
  description........................................................549
  modifying..........................................................497
output queues
  assigning forwarding classes (configuration editor)....839
  sample assignments..........................................839
over the air service provisioning See OTASP

P
packet encapsulation
  Layer 2 circuits.............................................742
  Layer 2 VPNs................................................742

overview..................................................................57
See also encapsulation type
troubleshooting on the link services
  interface................................................................441
  verifying on the link services interface...............443
packet flooding
  bridge domains..............................................698
packet fragmentation
  troubleshooting on the link services
  interface................................................................441
  verifying on the link services interface...............442
packet-mode
  action modifier................................................616
packets
  applying CoS scheduling rules.........................864
  handling packet fragments.............................607
  handling packet fragments (configuration editor)....632
  PPPoE discovery.............................................62, 292
  RIP, description.........................................486
PAD packets.........................................................62
PAD packets.........................................................62
PADR packets.......................................................62
PADT packets.........................................................62
PAP (Password Authentication Protocol)
  enabling for dialer interfaces...........................396
  enabling on dialer interfaces..........................396
parentheses, in syntax descriptions..........................xxxix
partial sequence number PDU (PSNP).........................528
passive routes, rejection, in static routing.................481
password
  for OSPFv2 authentication...............................516
  for RIPv2 authentication...............................498
  for TGM550 access...........................................279
path cost metrics
  for BGP, description........................................540
  See also MED
  for OSPF routes, description............................517
  for OSPF routes, modifying.............................518
  for RIP routes, description...............................493
  for RIP routes, modifying.................................494, 496
path selection, IS-IS...............................................527
path-vector protocol See BGP
pc-pim/0/0 interface.............................................75
pd-0/0/0 interface................................................75
PDUs (protocol data units)
  CSNPs..............................................................528
  hello PDUs.......................................................527
  LSPs.................................................................528
  overview.........................................................527
  PSNPs..............................................................528
PE (provider edge) routers.........................................770
  description......................................................737
ES-IS for a CLNS island........................................761
route distinguishers...............................................739
verifying Layer 2 circuit connections ........................................ 756
verifying Layer 2 circuit interfaces ........................................ 756
verifying Layer 2 VPN connections ........................................ 749
verifying Layer 2 VPN interfaces ........................................ 749
verifying Layer 3 VPN connections ........................................ 753
See also VPLS
pe-0/0/0 interface .................................................................. 76
peering sessions See BGP peers; BGP sessions
penultimate hop popping (PHP) ............................................. 713
penultimate router, in an LSP .............................................. 711
per-unit scheduler, channelized ports .................................... 121
permanent routes, adding .................................................. 476
permanent virtual circuits See PVCs
PGM (Pragmatic General Multicast) ........................................ 563
PHP (penultimate hop popping) ........................................... 713
physical interface properties
BERT ................................................................................. 53
capsulation ....................................................................... 57
FCS ................................................................................... 55
interface clocking .......................................................... 54
key properties ................................................................... 52
MTU values ........................................................................ 56
physical interfaces
assigning CoS components to (Quick Configuration) .......... 831
PIC (PIM on a Services Router) See PIMs
PIM (Protocol Independent Multicast)
dense mode ......................................................................... 563
disabling on the network management interface ................. 569
register messages See PIM register messages
RPF routing table group ................................................... 573
source-specific multicast (SSM) .......................................... 563
sparse mode ........................................................................ 563
static RP router ................................................................ 569
supported versions .......................................................... 559
verifying the mode .......................................................... 576
verifying the RP ............................................................... 577
PIM register messages
filtering ............................................................................... 571
incoming, rejecting on an RP ........................................... 571
outgoing, rejecting on a designated router ....................... 572
reject policy on designated router .................................... 572
reject policy on RP router ................................................ 571
pimd interface ................................................................. 76
pime interface ..................................................................... 76
PIMs (Physical Interface Cards)
names ................................................................................ 13
PIMs (Physical Interface Modules)
abbreviations ..................................................................... 13
Avaya VoIP modules See Avaya VoIP modules
G.SHDSL ............................................................................ 146
See also G.SHDSL PIMs
initial configuration of interfaces ....................................... 110
output about, understanding ........................................... 12
PIM number, always 0 ....................................................... 11
slot number ........................................................................ 11
ping command (stateless firewall filter) ............................... 629
explanation ........................................................................ 629
Ping Host page, output for BGP ........................................... 557
ping mpls l2circuit interface command ......................... 756
ping mpls l2circuit virtual-circuit command .................... 756
ping mpls l2vpn instance .................................................. 749
ping mpls l3vpn command ................................................ 753
ping, verifying link states ................................................... 113
pinouts
Avaya VoIP modules .......................................................... 238
RJ-45 TGM550 console connector .................................. 238
TGM550 analog RJ-11 connector ...................................... 239
TGM550 console DB-9 connector .................................... 238
TGM550 console port ....................................................... 238
TIM508 ............................................................................ 239
TIM510 E1/T1 RJ-45 ......................................................... 240
TIM514 analog RJ-11 connector ...................................... 240
TIM516 ............................................................................ 241
TIM518 ............................................................................ 242
PIM-only and CIR mode ..................................................... 927
plesiochronous networks .................................................. 54
PoE
classes and power ratings ................................................... 960
configuring ........................................................................ 961
Specifications ................................................................... 959
SRX210 Services Gateway .................................................. 959
SRX240 Services Gateway .................................................. 959
verifying settings using the CLI ......................................... 963
Point-to-Point Protocol See PPP
Point-to-Point Protocol over ATM See PPPoA
Point-to-Point Protocol over Ethernet See PPPoE
poison reverse technique ....................................................... 487
polarity, signal ................................................................. 30
policers
configuring ......................................................................... 909
for CoS traffic classes ....................................................... 801
for firewall filter ................................................................ 834
for stateless firewall filters ............................................... 624
strict high-priority queuing (configuration editor) ............ 898
policy See routing policies
pop label operation ............................................................ 712
ports
Avaya VoIP .......................................................................... 261
See also Avaya VoIP modules
console (TGM550) .......................................................... 247
DS1 See E1 ports; T1 ports
DS3 See E3 ports; T3 ports
E1 See E1 ports
E3 See E3 ports
Fast Ethernet See Fast Ethernet ports
Gigabit Ethernet See Gigabit Ethernet ports
interfaces overview..................................................3
  See also ATM-over-ADSL interfaces;
  ATM-over-SHDSL interfaces; ISDN
  interfaces; link services interface; loopback
  interface; management interfaces; network
  interfaces; special interfaces
LINE and TRUNK, on Avaya VoIP TGM550........247
serial See serial ports
T1 See T1 ports
T3 See T3 ports
telephone and trunk, on Avaya VoIP
  TGM550..........................................................247
  TGM550..........................................................247
  TIM510..........................................................251
  TIM514..........................................................253
  TIM521..........................................................256
verifying status of uPIM ports in switching
  mode..................................................................656
VoIP.................................................................261
  See also Avaya VoIP modules
power over ethernet
  overview................................................................959
  See also PoE
pp0
  information about.................................................305
  interface description............................................76
  logical Ethernet interface on (Quick
  Configuration).....................................................295
PPP
  CHAP...............................................................397
  PAP....................................................................396
PPP (Point-to-Point Protocol) See MLPPP, PPP
  encapsulation; PPPoA, PPPoE
PPPoE (Point-to-Point Protocol over Ethernet)
  address assignment (Quick Configuration)...............295
  CHAP (Quick Configuration)..................................295
  CHAP local identity (Quick Configuration)...............295
  CHAP, overview..................................................293
  client and server ..............................................291
discovery packets.............................................62, 292
encapsulation on an Ethernet interface..................61
interfaces (Quick Configuration).........................293
interfaces, overview..........................................291
logical interfaces (Quick Configuration)...............295
overview..........................................................291
  See also PPPoE over ATM-over-ADSL, PPPoE
  over ATM-over-SHDSL
preparation.........................................................293
radio-router protocol...........................................302
sample topology..................................................291
service type (Quick Configuration).......................296
session limit (Quick Configuration).......................296
session overview................................................296
session reconnection time (Quick
  Configuration)...................................................296
underlying interface (Quick Configuration).............296
verifying interfaces..............................................305
verifying sessions...............................................307
verifying statistics..............................................308
verifying version information..............................307
PPPoE Active Discovery Initiation (PADI) packets.....62
PPPoE Active Discovery Offer (PADO) packets..........62
PPPoE Active Discovery Request (PADR) packets.....62
PPPoE Active Discovery Session-Confirmation (PADS)
  packets..........................................................62
PPPoE Active Discovery Termination (PADT)
  packets..........................................................62
PPPoE encapsulation See PPPoE
PPPoE interfaces See PPPoE
PPPoE Interfaces Quick Configuration page.............294
PPPoE over ATM LLC encapsulation
  ATM-over-ADSL interfaces.................................137, 144
  ATM-over-SHDSL interfaces.................................148, 154
PPPoE over ATM-over-ADSL
  overview..........................................................291
  See also PPPoE
preparation.........................................................293
sample topology..................................................291
verifying configuration........................................304
PPPoE over ATM-over-SHDSL
  overview..........................................................291
  See also PPPoE
preparation.........................................................293
verifying configuration........................................304
PPPoEoA See PPPoE over ATM-over-ADSL, PPPoE over
  ATM-over-SHDSL
Pragmatic General Multicast.................................563
preferences
for OSPF routes .................................................. 519
for static routes .................................................... 477
setting for static routes ........................................ 479
prefix-length-range match type ............................. 591
primary stations, HDLC ........................................... 63
priority propagation ............................................... 927
priority scheduling
configuration example .......................................... 883
profile
GSM ..................................................................... 361, 368
profile, GSM .......................................................... 361, 368
promiscuous mode
enabling on Ethernet interfaces ............................. 108
propagation, suppressing ....................................... 602
properties, verifying
for ATM-over-ADSL network interfaces ................ 157
for ATM-over-SHDSL network interfaces ............... 160
for network interfaces .......................................... 114
protocol data units See PDUs
protocol families
ccc ....................................................................... 65
common protocol suites ........................................ 64
inet ................................................................. 64
inet6 ................................................................. 64
ISO ....................................................................... 64
mlfr-end-to-end .................................................... 65
mlfr-uni-nni ......................................................... 65
mlppp ................................................................. 65
MPLS overview ..................................................... 64
tcc ........................................................................ 65
tnp ........................................................................ 65
Protocol Independent Multicast See PIM
protocols
ARP ................................................................. 111
Auto-RP ............................................................ 563
BGP See BGP
CRTP ................................................................. 404, 430
distance vector See RIP
DVMRP .................................................................. 563
EGPs .................................................................... 468
EIA-530 .............................................................. 32
IGMP See IGMP
IGPs .................................................................... 468
IS-IS See IS-IS
LDP See LDP
MSDP .................................................................... 563
multicast See multicast
OSPF See OSPF
overview ............................................................ 467
path vector See BGP
PGM ..................................................................... 563
PIM dense mode See PIM
PIM source-specific multicast (SSM) ....................... 563
PIM sparse mode See PIM
PPPoE See PPPoE
RIP See RIP
RS-232 ................................................................... 32
RS-422/449 .......................................................... 33
RSVP See RSVP
SAP and SDP See SAP, SDP
serial ....................................................................... 31
V.35 ...................................................................... 33
X.21 ...................................................................... 34
provider edge routers See PE routers
provider routers
description .......................................................... 737
PSNP (partial sequence number PDU) ..................... 528
publishing responses to ARP requests
on Fast Ethernet subnets (Quick Configuration) .... 92
on Gigabit Ethernet subnets (Quick Configuration) .... 95
static ARP entries (configuration editor) ............... 111
push label operation ............................................... 712
PVCs (permanent virtual circuits)
in multilink bundles, with MLFR FRF 15 ............... 424
See also MLFR FRF 15; multilink bundles
in multilink bundles, with MLFR FRF 16 ............... 427
See also MLFR FRF 16; multilink bundles
overview ............................................................. 58
preventing dropped packets on .................... 447
Q
Q.931 timer, ISDN ............................................ 128, 317, 323
queues ................................................................. 797
See also CoS; output queues; queuing
queuing
CoS rules ............................................................ 864
starvation prevention (configuration editor) ........ 893
strict high priority (configuration editor) ............. 893
queuing with LFI
on Q2 of constituent links ................................... 409
Quick Configuration
ATM-over-ADSL Interfaces page ....................... 135
ATM-over-SHDSL Interfaces page ..................... 146
Avaya VoIP ......................................................... 269
Class of Service Interfaces page ......................... 831
CoS classifiers page ............................................. 820
CoS forwarding classes page ............................. 819
CoS RED drop profiles page ............................... 824
CoS scheduler maps page .................................. 824
CoS schedulers page .......................................... 824
CoS value aliases page ....................................... 817
E1 Interfaces page ............................................ 84
E3 Interfaces page ............................................ 87
Fast Ethernet Interfaces page ......................... 891
ISDN BRI Dailer Logical Interface page ............. 319
ISDN BRI Physical Interface page ...................... 314
network interfaces ........................................... 82
Rewrite rules page........................................ 822
serial Interfaces page............................. 105
T1 Interfaces page................................... 98
T3 (DS3) Interfaces page........................ 102
TGM550............................................... 269
virtual channel groups page...................... 829
VoIP................................................. 269

R
RADIUS authentication, of PPP sessions........ 293
random early detection See RED drop profiles
RBBL See BBL
reachability........................................... 739
verifying for a RIP network....................... 501
verifying for BGP peers............................ 556
verifying for OSPF network hosts............... 522
See also NLRI
real-time performance monitoring (RPM), for BGP
peers.................................................. 554
RED (random early detection) drop profiles
 defining (configuration editor)..................... 854
defining (Quick Configuration)...................... 824
description........................................... 799
sample configurations................................ 854
red drop profiles
 configuration example................................ 856
redundant Ethernet interfaces...................... 700
transparent mode chassis clusters................. 700
understanding......................................... 454
verifying............................................... 459
See also Layer 2 interfaces
rejecting
 unauthorized PIM registration.................... 571
rejecting incoming calls, ISDN.................... 341
Remote Authentication Dial-In User Service (RADIUS)
authentication, of PPP sessions................. 293
remote connection to router
 connecting USB modem to router.................. 385
remote management, USB modem.................. 383
repeaters, on LAN segments....................... 17
reported bearer bandwidth limit See BBL
request chassis fpc slot slot-number restart
command............................................ 282
Resource Reservation Protocol See RSVP
reverse-path forwarding See RPF
rewrite rules
 assigning to logical interfaces (configuration
tool).................................................. 845
assigning to logical interfaces (Quick
 Configuration)..................................... 833
defining (configuration editor)..................... 845
defining (Quick Configuration)...................... 822
description........................................... 801
replacing DSCP's (configuration editor)......... 846
sample rules.......................................... 845
transparent mode..................................... 704, 705
when applied........................................ 810
rewrite-rules statement
usage guidelines...................................... 879
RIB See routing table
RIP (Routing Information Protocol)
 authentication (RIPv2 only)....................... 497
authentication (RIPv2 only), configuring......... 498
basic network (configuration editor).............. 492
distance vector protocol............................ 485
efficiency techniques............................... 487
maximum hop count................................ 486
overview............................................ 485, 492
packets................................................ 486
path cost metrics See path cost metrics
poison reverse technique.......................... 487
requirements.......................................... 491
routing policy (configuration editor).............. 492
sample network with incoming metric............ 494
sample network with outgoing metric............. 496
sample topology...................................... 492
split horizon technique............................ 487
traffic control with metrics See path cost metrics
traffic control with metrics, configuring........ 494, 496
unidirectional limitations......................... 488
verifying host reachability......................... 501
verifying RIP message exchange.................. 499
verifying RIP-enabled interfaces............... 500
RIP neighbors, verifying......................... 500
RIPng (Routing Information Protocol next generation)
overview............................................ 489
Rj-11 connector pinouts
TGM550 analog ports............................... 239
TIM514 analog ports............................... 240
Rj-45 connector pinouts
TGM550 console port............................... 238
TIM510 E1/T1 ports................................. 240
Rj-45 to DB-9 serial port adapter
TGM550 console port............................... 248
route advertisements
 AS path in.......................................... 539
 BGP, update messages............................ 536
description.......................................... 470
external, EBGP..................................... 536
internal, IBGP..................................... 556
LSAs.................................................. 503
stub areas and NSSAs, to control................. 513
route aggregation.................................... 471
route distinguishers
description........................................... 739
formats for......................................... 739
route injection........................................ 597
route list match types............................... 591
route manipulation actions, routing policies..... 589
route origin, role in BGP route selection..................................537
route redistribution..........................................................597
route reflectors See BGP route reflectors
route selection
  BGP process for..........................................................537
  BGP, determining by AS path..........................................539
  BGP, determining by local preference...............................538
  BGP, determining by MED metric.......................................540
  BGP, lowest origin value preferred...................................539
static routes, defining.....................................................478
route targets, VPN
  in a routing instance..................................................739
route-flap damping..........................................................602
parameters........................................................................603
router ID, role in BGP route selection.................................537
routing..........................................................467
  advertisements..................................................................470
  aggregation....................................................................471
BGP See BGP
  configuring PPPoE..........................................................289
  configuring VPNs............................................................737
  dynamic...........................................................................470
filtering routes with policies.................................................581
filtering traffic through a stateless firewall..........................607
forwarding tables............................................................469
from one source to many destinations..................................559
in multiple ASs with BGP...................................................535
in one AS with OSPF..........................................................503
in one AS with RIP............................................................492
IS-IS See IS-IS
MPLS traffic engineering.....................................................719
multicast See multicast neighbors See BGP peers, OSPF neighbors, RIP neighbors
OSPF See OSPF
overriding default packet forwarding with
  CoS..................................................................................815
protocol overview.............................................................467
RIP See RIP
RIP statistics........................................................................499
RIPng See RIPng
routing tables.................................................................468
static See static routing
VPNs..................................................................................737
See also protocols, routing policies, routing solutions
Routing Engine
  handling packet fragments for (configuration editor)..................632
  protecting against DoS attacks.........................................624
  protecting against untrusted services and protocols
    (configuration editor)......................................................618
routing information base See routing table
Routing Information Protocol See RIP

routing instance
for CLNS static routes (with IS-IS)........................................759
for CLNS static routes (without IS-IS)....................................763
VPLS...........................................................................773, 777, 780
VPN configuration...............................................................747
VPN route target.................................................................739
VRF instances.................................................................738
VRF table...........................................................................739
routing mode, multi-port uPIMs............................................653
routing policies
  actions..............................................................................588
  applying.............................................................................583
  BGP export, for CLNS.........................................................762
configuration
  tasks...........................................................583, 585, 594, 597, 600, 603
default actions.....................................................................585
export statement....................................................................583
final actions........................................................................585
forwarding class with source and destination........................594
grouping source and destination prefixes................................594
import statement...................................................................583
injecting routes from one protocol into another........................597
Layer 2 VPN export policy....................................................748
Layer 2 VPN import policy....................................................748
Layer 3 VPNs.......................................................................752
making BGP routes less preferable.........................................600
match conditions...................................................................587
overview.............................................................................581
PIM register messages See PIM register messages
  policy name.......................................................................583
preparation............................................................................582
prepending AS paths............................................................600
reducing update messages with flap damping..........................602
RIP routing policy (configuration editor)..................................492
route redistribution..............................................................597
route-flap damping..............................................................602
terms.................................................................................585
terms, creating.......................................................................585
routing solutions
  applying CoS components on link services
    interface...........................................................................439
BGP confederations, for scaling problems................................552
BGP route reflectors, for scaling problems..............................549
BGP scaling techniques.........................................................542
controlling designated router election....................................507
controlling OSPF route cost..................................................518
controlling OSPF route selection..........................................519
controlling RIP traffic with the incoming metric.......................494
controlling RIP traffic with the outgoing metric.......................496
CoS....................................................................................789, 815
designated router, to reduce flooding.......................................506
directing BGP traffic by local preference........538
drop-and-insert clock combinations..............131
filtering unwanted services and protocols.....618
handling packet fragments.........................607
handling packet fragments (configuration editor)..........................632
load balancing on link services interfaces.......441
making BGP routes less preferable..............600
managing VoIP bandwidth See dynamic CAC
MPLS traffic engineering...............................719
multicast administrative scoping.................563
multicast reverse-path forwarding (RPF)........562
multicast shortest-path tree (SPT).................562
NSSAs, to control route advertisement..........513
path cost metrics, for packet flow control See path cost metrics
point-to-point sessions over Ethernet............289
poison reverse, for traffic reduction.............487
preventing dropped packets on PVCs..............447
preventing multicast routing loops..............562
protecting against DoS attacks....................624
reducing jitter and latency on multilink bundles.........440
reducing update messages with flap damping........................................602
routing policies........................................581
securing OSPF routing (OSPFv2 only).............515
split horizon, for traffic reduction................487
stateless firewall filters..............................607
static route control techniques..................480
stub areas, to control route advertisement........513
VPNs............................................................737
routing table
controlling static routes in.......................480, 481
description...............................................468
displaying static routes in..........................483
RPF group, for multicast.........................573
sample distance-vector routing..................486
updates, limitations in RIP.......................488
verifying for RPF........................................577
verifying OSPF routes.................................521
verifying RSVP-signaled LSPs......................732
VPLS..............................................................779
RP (rendezvous point)
PIM register messages, incoming, rejecting.......571
PIM register messages, outgoing, stopping........572
reject policy for incoming PIM register messages........................................572
same reject policy on RP routers in a network.........................571
static..................................................569
verifying...............................................577
RP router See RP

RPF (reverse-path forwarding)
description..............................................562
routing table group.....................................573
verifying the routing table.........................577
RPM, for BGP peers.................................554
RS-232.......................................................32
RS-422/449..................................................33
RS-530.......................................................32
RST (reset) button, TGM550.........................282
RSVP (Resource Reservation Protocol)
and OSPF for VPNs......................................746
overview...............................................725
requirements...........................................721
verifying LSPs...........................................732
verifying neighbors..................................731
verifying sessions....................................732
verifying the routing table on the entry router..732
VPLS.........................................................782
RSVP neighbors, verifying.........................731

S
S,G notation, for multicast forwarding states......561
S/T interface
overview...............................................51
PIMs.........................................................512
sample configuration
scheduler maps........................................863
sample configurations
CLNS VPN configuration.............................765
CoS behavior aggregate classification forwarding classes and queues.................810
firewall filter configurations.....................621, 629, 635
samples
drop-and-insert clock combinations..............131
link services CoS........................................432
multilink bundle........................................431
PPPoA for ATM-over-ADSL configuration........160
PPPoE over ATM-over-ADSL configuration........305
PPPoE over ATM-over-SHDSL configuration......305
PPPoE over Ethernet configuration...............304
SAP (Session Announcement Protocol)
description..............................................563
session announcements..........................566
verifying.................................................575
scaling BGP See BGP confederations; BGP route reflectors
scheduler hierarchy example....................918
applying traffic control profiles................922
drop profiles...........................................922
interface sets.........................................919
interfaces...............................................920
scheduler maps.......................................922
 schedulers.............................................921
traffic control profiles............................920

Index
scheduler maps
assigning (configuration editor).......................... 860
assigning to logical interfaces (Quick
Configuration)...................................................... 833
assigning to physical interfaces (Quick
Configuration)...................................................... 832
defining (configuration editor).............................. 860
defining (Quick Configuration).............................. 824
defining and applying........................................ 420
sample configuration......................................... 863
scheduling priority, overview.............................. 410
strict high-priority queuing (configuration
editor).................................................................... 895
strict high-priority queuing, applying scheduler
map to interface (configuration editor)............... 897
scheduler maps for hierarchical example.............. 922
scheduler-map statement
usage guidelines................................................ 871
schedulers.......................................................... 797
assigning resources (configuration editor)............. 858
buffer size.......................................................... 798
default settings.................................................. 807
defining (configuration editor).............................. 857
defining (Quick Configuration).............................. 824
description......................................................... 797
mapping to forwarding classes (configuration
editor).................................................................... 861
mapping to forwarding classes (Quick
Configuration)...................................................... 824
RED drop profiles................................................. 799
sample mappings................................................ 860
sample schedulers................................................. 857
scheduler maps See scheduler maps
shaping rate........................................................ 799
transmission priority............................................. 799
transmit rate......................................................... 798
voice and data for strict high-priority queuing
(configuration editor)............................................. 896
voice, for strict high-priority queuing (configuration
editor).................................................................... 895
See also transmission scheduling
schedulers for hierarchical example.................... 921
scheduling
strict-high priority
example configuration......................................... 881
scheduling priority................................................. 799
See also CoS, scheduler maps, schedulers
scope, IPv6 addresses
global unicast...................................................... 69
link-local unicast................................................... 69
multicast types....................................................... 69
site-local unicast................................................... 69
scoping, administrative......................................... 563
screening incoming calls, ISDN............................. 340
SDP (Session Discovery Protocol)
description......................................................... 563
session announcements...................................... 566
verifying............................................................. 575
secondary stations, HDLC.................................... 63
secret, CHAP See CHAP, local identity
secure context
enabling IS-IS in.................................................. 529
security
MD5 authentication for OSPF......................... 516
MD5 authentication for RIPv2......................... 498
password authentication for OSPFV2.............. 516
password authentication for RIPv2................. 498
stateless firewall filters........................................ 607
security policies
transparent mode............................................... 685, 687
self-near-end crosstalk See SNEXT
serial interfaces
clocking modes.................................................. 30
connection process............................................. 29
DTE default clock rate reduction...................... 31
EIA-530............................................................ 32
inverting the transmit clock.............................. 31
line protocols...................................................... 31
MLPPP bundles and LFI (configuration
editor).................................................................... 413
multilink bundles (Quick Configuration).............. 410
overview.............................................................. 28
See also serial ports
Quick Configuration............................................ 104
RS-232............................................................... 32
RS-422/449............................................................ 33
signal polarity....................................................... 30
transmission signals............................................. 29
V.35................................................................. 33
X.21................................................................. 34
serial numbers, in MAC addresses...................... 15
serial ports
CHAP............................................................... 106
clock rate.......................................................... 108
clocking............................................................ 107
clocking, inverting the transmit clock................ 107
capsulation type.................................................. 106
line speed.......................................................... 108
logical interfaces............................................... 106
MTU................................................................. 106
MTU default and maximum values..................... 56
overview.......................................................... 28
See also serial interfaces
Quick Configuration............................................ 104
service provider ID See SPIID
Services Gateway
network interfaces............................................... 81
services interfaces, overview.............................. 78
See also link services interface; multilink services
Services Router
  as a PPPoE client........................................291
  Avaya VoIP connectivity.............................237
  channelized T1/E1/ISDN PRI interfaces.............117
  CoS..........................................................815
  interfaces overview.....................................3
  ISDN connections........................................117, 309
  link services interface..................................399
  link services interface, implementation
    exceptions...........................................402
  network interfaces......................................81
  USB modern connections...............................583
Session Announcement Protocol See SAP, SDP
  announcements, multicast..............................566
  BGP session establishment...........................535
  BGP session maintenance..............................536
  ISDN session establishment..........................52
  limit on PPPoE sessions................................292
  PPPoE.........................................................62, 292
  PPPoE, reconnection time (Quick
    Configuration)........................................296
  RSVP, verifying..........................................732
set igmp fpc slot media-gateway-controller
  command..................................................274
  shaping rate............................................799
  applying..................................................423
  overview..................................................409
  requirement.............................................423
  See also CoS, scheduler maps, schedulers
shaping-rate statement
  usage guidelines........................................871, 876
SHDSL interfaces See ATM-over-SHDSL interfaces
  SHDSL page.................................................147
  SHDSL ports See ATM-over-SHDSL interfaces
  shortest path first algorithm......................503
  shortest-path tree......................................562
  show access command....................................160
  show bgp group command................................555
  show bgp neighbor command............................554
  explanation..............................................555
  show bgp summary command.............................556
  explanation..............................................556
  show chassis hardware command......................12
  show class-of-service adaptive-shaper command....943
  show class-of-service classifier name command......437
  show class-of-service command........................943
  show class-of-service interface command..........437, 943
  show class-of-service scheduler-map command.......437
  show class-of-service virtual-channel command.....942
  show class-of-service virtual-channel-group
    command..................................................943
  show firewall command.................................621, 629, 635
  show firewall filter protect-RE command............630
  show firewall log command.............................622
show igmp interface command..........................576
  explanation...............................................576
show interfaces ae0 extensive command.................460
show interfaces ae0 terse command......................459
show interfaces at-3/0/0 command........................160
show interfaces bc-0/0/4.1 extensive command.........346
show interfaces br-6/0/0 extensive command............345
show interfaces command
  for channelized interfaces.........................128
  for clear-channel interfaces........................129
  for multilink bundles.................................451
  for PPPoE over ATM-over-ADSL.........................505
  for PPPoE over Ethernet................................504
  for the link services interface.....................431
show interfaces ct1-3/0/1 command......................128
show interfaces dc-0/0/4 extensive command............347
show interfaces detail command........................114
show interfaces dl0 extensive command................350
show interfaces el-3/0/1 command........................129
show interfaces extensive command.....................157
  explanation, for ATM-over-ADSL interfaces........158
  explanation, for ATM-over-SHDSL
    interfaces...............................................160, 162
  explanation, for ISDN interfaces....................345, 347, 348
  explanation, for VoIP interfaces.....................284
show interfaces lo0 command.............................624
show interfaces lqo-0/0/0 statistics detail
  command..................................................434
  explanation.............................................435
show interfaces pppoe command.........................306
show interfaces queue command..........................944, 946
  explanation.............................................946
show interfaces switch-port command...................656
show interfaces vp-3/0/0 extensive command............283
show isdn calls command................................349
show isdn status command................................344
show isis adjacency brief command.....................533
show isis adjacency extensive command................533
  explanation.............................................534
show lacp interfaces ae0 command.......................461
show lacp interfaces reth0 command.....................462
show lacp statistics interfaces ae0 command..........461
show ldp neighbor command................................723
show ldp session detail command........................723
show multicast rpf command..............................577
  explanation.............................................577
show ospf interface command............................519
  explanation.............................................519
show ospf neighbor command.............................520
show ospf route command..................................521
  explanation.............................................521
show pim interface command................................576
  explanation.............................................576
show pim rps command.....................................577
  explanation.............................................577
show poe controller command ..........................285
show poe interface command ..........................285
show poe telemetries ..................................285
show pppoe interfaces command .....................307
show pppoe statistics command .......................308
show pppoe version command ..........................307
show rip neighbor command ...........................500
show rip statistics command ...........................499
show route summary command ...........................622
show route table int. 3 command .......................724
show route terse command ...............................483
show rsvp neighbor command ............................731
show rsvp session detail command .....................732
show sap listen command ..................................575
show igm dynamic-call-admission-control command ...........................................622
show igm fpc slot-number media-gateway-controller command ...........................................622
show isis interface brief command .....................531
show isis interface detail command ....................532
signal-to-noise ratio See SNR
signaling protocols ........................................737
signals ..........................................................20
DS1 ..............................................................20
E1 loopback (control) .......................................22
explicit clocking signal transmission ......................55
ISDN, disabling .................................................343
multiplexing DS1 into DS2 signal .........................24
serial polarity .....................................................30
serial transmission .............................................29
T1 loopback (control) .........................................22
V.35 ..............................................................33
X.21 ..............................................................34
SIM (subscriber identity module) .........................381
unlocking ..........................................................908
simple filters .......................................................907
applying ..........................................................908
configuring .......................................................907
SRX3400 and SRX3600 devices ...........................907
single-area network, OSPF ..................................509
site identifier, VPLS .............................................778
site name, VPLS ..................................................778
site preference, VPLS .............................................778
site range, VPLS ..................................................778
site-local unicast IPv6 addresses ..........................69
SNEXT (self-near-end crosstalk) threshold, SHDSL..............150, 153
SNR (signal-to-noise ratio) margin, SHDSL .................150, 153
source filtering, Gigabit Ethernet ............................96
for MAC addresses ...............................................96
source-specific multicast .....................................563
Spanning Tree .........................................................660
configuring ..........................................................660
sparse mode See multicast routing modes
special interfaces ..................................................78
CRTP ..............................................................79, 404, 430
dsc interface .......................................................76
IPv4 addressing ....................................................65
IPv6 addressing ....................................................68
logical properties ..................................................64
loopback interface .................................................76
management interface ..........................................77
MLFR ..............................................................78
MLFR FRF. 15 and FRF. 16 .......................................78
MLPPP ..............................................................78
MLPPP FRF. 15 and FRF. 16 .....................................78
SRX3400 Services Gateways ...............................11
slot number .........................................................11
SRX3600 Services Gateways ...............................11
slot number .........................................................11
SRX5600 Services Gateways ...............................11
slot number .........................................................11
SRX5800 Services Gateways ...............................11
slot number .........................................................11
SSH command .......................................................622
SSH connection to TGM550 .....................................280
st0 interface .........................................................76
starvation prevention, on CoS queues .........................893
stateless firewall filters .........................................616
actions and action modifiers ..................................616
applying to an interface (configuration editor) ............624
automatic discard rule .........................................608
bit-field logical operators .....................................615
chained multiple filters .......................................609
displaying configurations .................................621, 629, 635
displaying statistics .............................................. 630
handling packet fragments ..................................... 607
handling packet fragments (configuration editor) ........... 632
match conditions .................................................. 610
multiple filters, chained ......................................... 609
overview ................................................................ 607
planning .................................................................. 607, 608
policers for ............................................................. 624
preparation ................................................................ 608
protecting the Routing Engine against TCP floods ...... 624
protecting the Routing Engine against untrusted services (configuration editor) ................................ 618
sample terms, to filter fragments ............................... 632
sample terms, to filter services and protocols ................. 618
sequences ................................................................ 609
strict high-priority queuing (configuration editor) .......... 899
terms, overview ...................................................... 609
typical, planning ....................................................... 607
verifying actions ....................................................... 622
verifying configuration ............................................. 621, 629, 635
verifying flood protection .......................................... 629
verifying packet logging ........................................... 622
static ARP entries
Fast Ethernet interface .............................................. 91
Gigabit Ethernet interface ......................................... 95
overview ................................................................ 111
static LSPs ................................................................ 713
static routes
CLNS VPNs (with IS-IS) .......................................... 759
CLNS VPNs (without IS-IS) ....................................... 763
configuring basic routes (configuration editor) ............. 476
controlling ............................................................... 480
controlling in routing and forwarding tables ................... 481
default properties ...................................................... 482
default properties, setting .......................................... 483
defining route selection ............................................. 478
preferences ................................................................ 477
preventing readvertisement ........................................ 481
qualified next hops ..................................................... 477
rejecting passive traffic ............................................ 481
requirements ............................................................ 475
route retention .......................................................... 480
sample preferred path .............................................. 479
sample preferred path .............................................. 479
static routing
description ............................................................. 470
overview ................................................................. 476
See also static routes

static RP router ................................................................ 569
See also RP
static TEI (terminal endpoint identifier), ISDN .................. 317, 323

statistics
ATM-over-ADSL interfaces ........................................ 159
ATM-over-SHDSL interfaces ...................................... 163
ISDN B-channel interfaces .......................................... 346
ISDN D-channel interfaces .......................................... 347
link services interface ................................................. 434
PPPoE ..................................................................... 508
RIP .......................................................................... 499
stateless firewall filters .............................................. 650
VoIP interface ............................................................ 283

status
ATM-over-SHDSL interfaces, verifying .......................... 163
ISDN calls, verifying .................................................. 549
ISDN interfaces, verifying ......................................... 344
link services interface, verifying .................................. 434
link states, verifying .................................................. 113
VoIP interface ............................................................ 283

strict high-priority queuing, CoS
applying a scheduler map to interface (configuration editor) .................. 897
applying classifier to interface (configuration editor) ............... 897
assigning queues ......................................................... 895
classifying traffic ........................................................ 894
configuring a scheduler map and schedulers (configuration editor) .................. 895
configuring policiers (configuration editor) ......................... 898
creating a stateless firewall filter (configuration editor) ............. 899
defining voice and data schedulers (configuration editor) ........ 896
overview ................................................................. 893

strict-high priority, explained
eexample configuration .............................................. 881
stub areas
area ID (configuration editor) ..................................... 512
controlling OSPF route cost ........................................ 518
creating (configuration editor) ..................................... 514
description ............................................................... 513
eexample ................................................................. 514
sample topology ....................................................... 514
sub-ASs, BGP ............................................................ 551
subautonomous systems, BGP ..................................... 551
subnet masks ............................................................ 67
subnets See subnetworks
subnetworks
description ............................................................. 468
IPv4 subnet addresses for multiple ISDN dialer interfaces ... 320
IPv4 subnets ............................................................ 66
route aggregation ....................................................... 472
subnetworks, multicast leaves and branches ..................... 560
subscriber identity module  
See SIM
superframe framing ......................................................21
support, technical  
See technical support
SVCs (switched virtual circuits) ......................................58
swap and push label operation ......................................712
swap label operation ....................................................712
switch types, supported, ISDN
for ISDN BRI service ..................................................316, 323
for ISDN PRI service ..................................................119
switched virtual circuits (SVCs)....................................58
switches
configuring ports as ..................................................641
on LAN segments .....................................................18
switching
configuring ...............................................................657, 660, 663, 671, 673
supported devices ......................................................642
switching mode, multi-port uPIMs ..................................653
symmetric high-speed digital subscriber line (SHDSL)
See ATM-over-SHDSL interfaces
synchronous networks ..............................................54
syntax conventions ....................................................xxxix
system clock  
See clocking
system identifier, IS-IS
all zeros not supported ..............................................526
formats, MAC or IP address ......................................526
identifier-to-hostname mapping ..................................526
overview ...............................................................526

T

T1 interfaces
AMI encoding ...........................................................21
B8ZS encoding ..........................................................21
CRTP (configuration editor) .........................................430
D4 framing ...............................................................21
data stream ............................................................19
dynamic CAC for voice packets (configuration
editor) .................................................................276
See also Avaya VoIP
encoding .................................................................20
ESF framing .............................................................22
framing ..................................................................21
loopback .................................................................22
multilink bundles (Quick Configuration) ..................410
overview ...............................................................19
See also T1 ports; channelized T1 interfaces
Quick Configuration ..................................................97
signals .................................................................20
superframe framing ..................................................21
T1 ports
cable length ...........................................................101
CHAP .................................................................99
clocking ...............................................................99
data inversion ........................................................100
encapsulation type ....................................................99
fractional, channel number ......................................12
frame checksum .......................................................100
framing .................................................................100
logical interfaces ....................................................99
MTU .................................................................99
MTU default and maximum values .........................123, 124
overview ...............................................................19
See also T1 interfaces; channelized T1 ports
Quick Configuration ..................................................97
time slots .............................................................100
T1 trunk ports, TIM510
description ............................................................251
pinouts .................................................................240
T1/E1 media module  
See TIM508  See TIM510  See TIM516  See TIM518
T3 interfaces
bit stuffing ...............................................................24
data stream ............................................................23
DS3 framing ............................................................25
multilink bundles (Quick Configuration) ..................410
multiplexing on ........................................................25
overview ...............................................................23
See also T3 interfaces
Quick Configuration ..................................................101
tap interface ...........................................................76
TCP protocol family ..................................................65
TCP policers ...........................................................624
technical support
contacting JTAC .........................................................xl
TEI option, ISDN .....................................................317, 324
telephone and trunk ports, on Avaya VoIP
telm550 .................................................................247
telephone calls
rejecting incoming ISDN ..........................................341
screening incoming ISDN ..........................................340
verifying status .........................................................349
Telephony Gateway Module  
See TGM550
Telephony Interface Module  
See TIM510; TIM514; TIM521
Telephony Interface Modules  
See TIM508; TIM510; TIM514; TIM516; TIM518; TIM521
Telnet access to TGM550
- connecting to TGM550 ................................................................. 281
- disabling Telnet service .............................................................. 281
- enabling Telnet service ............................................................... 280
- overview ....................................................................................... 280
- security caution ........................................................................... 280

telnet command ............................................................................. 281, 629
terminal endpoint identifier: See static TEI, TEI option terminology
- Avaya VoIP .................................................................................... 257
- channelized T1/E1/ISDN PRI .......................................................... 117
- CoS .............................................................................................. 790
- DSL ............................................................................................. 133
- hierarchical schedulers ................................................................. 912
- interfaces ...................................................................................... 4
- ISDN ............................................................................................ 309
- link services .................................................................................. 399
- ports ............................................................................................ 4
- PPPoE .......................................................................................... 290
- USB modem .................................................................................. 383
- wireless modem .......................................................................... 357

terms
- firewall filter, for multfield classifier ........................................... 836
- in a routing policy ......................................................................... 585
- in a routing policy, creating ......................................................... 585
- stateless firewall filters, overview .................................................. 609

TGM550
- accessing the router from ............................................................. 282
- administration ............................................................................. 278
- analog port pinouts ....................................................................... 239
- Avaya CLI access .......................................................................... 278
- Avaya Media Gateway Controllers
  - supported .................................................................................... 263
  - CLI access requirements ............................................................ 279
  - console connection .................................................................. 279
  - console port pinouts ................................................................. 238
  - description ................................................................................. 247
  - grounding cable requirement ..................................................... 267
  - interfaces .................................................................................... 262
  - IP address change caution ......................................................... 277
  - IP address, modifying (configuration editor) ............................ 277
  - IP address, setting (configuration editor) .................................... 272
  - IP addressing guidelines .......................................................... 266
  - JUNOS compatibility ................................................................. 266
  - maximum gateway capacities .................................................... 248
  - MGC list, adding ........................................................................ 274
  - MGC list, clearing ................................................................. 275
  - MGCs supported ....................................................................... 263
  - port LED states ........................................................................ 250
  - ports .......................................................................................... 247
  - Quick Configuration .................................................................. 269
  - reset on address change ............................................................ 277
  - resetting .................................................................................... 282
  - RST (reset) button ..................................................................... 282
  - saving the configuration ............................................................ 283
  - SSH connection ........................................................................ 280

Telnet access .................................................................................. 280
Telnet connection to router ............................................................ 282
verifying MGC list ........................................................................... 285
verifying VoIP interface ................................................................. 283
three-way handshake .................................................................... 503
through route list match type ......................................................... 591

TIM508
- connector port pinouts ................................................................. 239
- description .................................................................................... 250
- port configurations ....................................................................... 250
- ports, LED states ......................................................................... 251

TIM510
- description .................................................................................... 251
- E1 trunk ports .............................................................................. 251
- ports, LED states ......................................................................... 252
- RJ-45 connector port pinouts ....................................................... 240
- T1 trunk ports .............................................................................. 251

TIM510 interfaces ........................................................................... 262

TIM514
- analog port pinouts ..................................................................... 240
- analog telephone ports ................................................................ 253
- analog trunk ports ....................................................................... 253
- description .................................................................................... 253
- port configurations ....................................................................... 253
- ports, LED states ......................................................................... 254

TIM514 interfaces ........................................................................... 262

TIM516
- connector port pinouts ................................................................. 241
- description .................................................................................... 254
- port configurations ....................................................................... 254
- ports, LED states ......................................................................... 255

TIM518
- connector port pinouts ................................................................. 242
- description .................................................................................... 255
- port configurations ....................................................................... 256
- ports, LED states ......................................................................... 256

TIM521
- description .................................................................................... 256
- ISDN BRI ports ............................................................................. 256
- ports, LED states ......................................................................... 257

TIM521 interfaces ........................................................................... 262

time slots
- dropping and inserting, on channelized T1/E1 interfaces ............ 123
- E1 .............................................................................................. 86
- number in interface name .......................................................... 12
- T1 .............................................................................................. 100

TIMs: See TIM508, TIM510, TIM514, TIM516, TIM518, TIM521

trunk protocol family ..................................................................... 65
to statement, routing policy match conditions ............................... 587
topology
- Avaya VoIP .................................................................................. 261
data link layer ................................................................................ 14
- IPv4 subnets .................................................................................. 67
- point-to-multipoint LSPs ................................................................ 734
PPPoe session on an ATM-over-ADSL loop ........................................ 292
PPPoe session on an Ethernet loop ........................................... 291
sample BGP AS path ................................................................ 539
sample BGP confederation ..................................................... 553
sample BGP confederations .................................................... 552
sample BGP external and internal links .................................. 546
sample BGP local preference use ......................................... 538
sample BGP MED use .......................................................... 540
sample BGP peer network .................................................... 544
sample BGP peer session ...................................................... 543
sample BGP route reflector (one cluster) .................................. 547, 550
sample BGP route reflectors (cluster of clusters) .................... 549
sample BGP route reflectors (multiple clusters) ....................... 548
sample distance-vector routing ............................................. 486
sample Frame Relay network ................................................ 57
sample ISDN network .......................................................... 50
sample LAN ........................................................................... 73
sample LFI and multilink bundle network .................................. 414
sample LSP network ............................................................. 711
sample multiarea OSPF routing ............................................. 508
sample multilink bundle and LFI network ............................... 414
sample OSPF backbone area .................................................. 509
sample OSPF network .......................................................... 521
sample OSPF network with stubs and NSSAs .......................... 513
sample OSPF single-area network ......................................... 510
sample OSPF stub areas and NSSAs ...................................... 514
sample poison reverse routing .............................................. 488
sample RIP network ............................................................. 492
sample RIP network with incoming metric ................................ 494
sample RIP network with outgoing metric ................................ 496
sample route advertisement .................................................. 471
sample route aggregation ...................................................... 472
sample router network .......................................................... 469
sample RSVP-signaled LSP .................................................... 727
sample split horizon routing ................................................... 487
sample static route ............................................................... 470
sample static route, preferred path ....................................... 479
sample stub network for static routes ..................................... 476
sample unidirectional routing ............................................... 488
sample VLAN ...................................................................... 73
VoIP .................................................................................... 261
topology database, OSPF ...................................................... 503
trace options ........................................................................ 780
trace options, channelized ports .......................................... 122
Traceroute page
 results for OSPF .................................................................. 522
 results for RIP ..................................................................... 501
traceroute source bypass-routing gateway command .............. 724
traffic controlling with incoming RIP metric ......................... 494
 controlling with outgoing RIP metric .................................. 496
 filtering through a stateless firewall .................................... 607
traffic control profiles for hierarchical example .................... 920
traffic engineering See MPLS traffic engineering, traffic engineering database
 transit routers, in an LSP ................................................... 711
transmission priority ............................................................ 799
See also CoS; scheduler maps; schedulers
transmission scheduling ........................................................ 811
transmit clock source See clocking
transmit rate description ....................................................... 798
See also CoS; schedulers; transmission scheduling
transparent mode BA classifier ............................................. 703
 blocking non-ARP traffic .................................................... 685
 blocking non-IP traffic ....................................................... 685
 broadcast traffic ................................................................. 685
 chassis clusters ................................................................. 699
 Class of Service .................................................................. 702
 conditions ........................................................................... 679
 firewall user authentication .................................................. 693
 redundant Ethernet interfaces ............................................. 700
 rewrite rules ....................................................................... 704, 705
 security policies ................................................................. 685, 687
 VLAN retagging ................................................................. 689
trigger statement usage guidelines .......................................... 876
troubleshooting applying CoS components on link services interface ........................................ 439
 Avaya VoIP ........................................................................ 286
 channelized T1/E1 interfaces .............................................. 130
dialer interfaces, packet loss due to duplicate IP subnet addresses ........................................... 320
dropped packets on PVCs .................................................... 447
jitter and latency on multilink bundles ................................. 440
LFI and load balancing on multilink bundles ......................... 441
link services interface .......................................................... 439
TRUNK and LINE ports, on Avaya VoIP TGM550 ................. 247
trunk ports, TIM508 ............................................................. 239
 pinouts .............................................................................. 239
TRUNK ports, TIM514 .......................................................... 253
trunk ports, TIM516 ............................................................. 241
 pinouts .............................................................................. 241
trunk ports, TIM518 ............................................................. 242
 pinouts .............................................................................. 242
TST LED ................................................................................ 252
tunnels CoS queuing ............................................................. 812
two-dimensional parity .......................................................... 55
two-rate tricolor marking policer applying to a firewall ............. 909
OSPF-enabled interfaces........................................................................................................519
packet encapsulation on link services
interface..................................................................................................................................443
 PIM mode and interface configuration ..................................................................................576
 PIM RP address ....................................................................................................................577
 PIM RPF routing table ...........................................................................................................577
 PPPoA for ATM-over-ADSL configuration ............................................................................160
 PPPoE interfaces ..................................................................................................................305
 PPPoE over ATM-over-ADSL configuration .........................................................................304
 PPPoE over ATM-over-SHDSL configuration .........................................................................304
 PPPoE sessions .....................................................................................................................307
 PPPoE statistics .....................................................................................................................308
 PPPoE version .......................................................................................................................307
 RIP host reachability .............................................................................................................501
 RIP message exchange .........................................................................................................499
 RIP-enabled interfaces ..........................................................................................................500
 RSVP neighbors .....................................................................................................................731
 RSVP sessions .......................................................................................................................732
 RSVP-signed LSP .....................................................................................................................732
 stateless firewall filter actions .............................................................................................622
 stateless firewall filter flood protection ................................................................................629
 stateless firewall filter operation ..........................................................................................622
 stateless firewall filters .........................................................................................................621, 629, 655
 stateless firewall statistics .....................................................................................................630
 static routes in the routing table ............................................................................................483
 virtual channel groups ..........................................................................................................943
 virtual channels ...................................................................................................................942
 virtual link, through the backbone area ..................................................................................508
 VLAN CCC example configuration ......................................................................................784, 785
 VLAN encapsulation configuring ..........................................................................................783
 VLAN retagging transparent mode .......................................................................................689
 VLAN VPLS example configuration ......................................................................................784, 785
 VLANs configuring .................................................................................................................657
 VLANs (virtual LANs)
 LAN comparison.......................................................................................................................73
 overview .................................................................................................................................72
 rewrite....................................................................................................................................776
 tagging .....................................................................................................................................776
 topology.....................................................................................................................................73
 VLSMs (variable-length subnet masks)..................................................................................67
 voice calls, not supported in dial-in .......................................................................................383
 voice calls, not supported in dial-in or callback ....................................................................337
 voice over IP See Avaya VoIP See Avaya VoIP modules voice packets
 integrating with data, with drop-and-insert ........................................................................123
 LFI handling...........................................................................................................................403
 speeding transmission with CRTP.......................................................................................404, 430
 voice traffic latency, controlling with shaping rates ................................................................423
 See also multilink bundling
 voice traffic, prioritizing packets for, in CoS queues ................................................................893
 VoIP See Avaya VoIP modules
 VoIP (voice over IP) See Avaya VoIP; VoIP interface
 VoIP interface
 addressing guidelines..............................................................................................................266
 correcting version incompatibility problem .........................................................................286
 IP address, modifying (configuration editor) .........................................................................277
 IP address, setting (configuration editor) ..............................................................................272
 naming convention ...............................................................................................................262
 Quick Configuration.............................................................................................................269, 270
 unavailability, correcting .....................................................................................................286
 verifying....................................................................................................................................283
 vp-0/0/0.....................................................................................................................................262
 See also VoIP interface
 VPI (virtual path identifier)
 ATM-over-ADSL interfaces ...............................................................................................138, 141
 ATM-over-SHDSL interfaces ..............................................................................................149, 152
WAN interfaces, configuring dynamic CAC on for Avaya VoIP ................................................. 275
watch list, for ISDN backup ................................ 320, 330
watch list, for USB modem backup ...................... 394
watch list, for wireless modem .......................... 374
wireless modem ........................................... 360
configuration overview .................................. 362
logical interface ........................................... 360
physical interface ....................................... 359
supported cards .......................................... 357
supported devices ......................................... 357
WAN connection ......................................... 355
WAN connection overview .............................. 356
See also dialer interface, wireless modem
wireless modem interface
adding ....................................................... 367
dialer pool .................................................. 359
GSM profile .................................................. 359, 361
modem initialization string .............................. 359
WRED on the IOC ......................................... 932

X
X.21 .................................................................. 34