



**J-series™ Services Router**

## **Basic LAN and WAN Access Configuration Guide**

*Release 7.5*

**Juniper Networks, Inc.**

1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA

408-745-2000

**[www.juniper.net](http://www.juniper.net)**

Part Number: 530-014841-01, Revision 1

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

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

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

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

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

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: ERX, ESP, E-series, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, T-series, and TX Matrix. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

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.

Copyright © 2006, Juniper Networks, Inc. All rights reserved.

*J-series™ Services Router Basic LAN and WAN Access Configuration Guide*, Release 7.5  
Copyright © 2006, Juniper Networks, Inc.  
All rights reserved. Printed in USA.

Writing: Nidhi Bhargava, Michael Bushong, Taffy Everts, Walter Goralski, Joshua Kim, Jerry Isaac, Archana Maheshwari, Hareesh Kumar Kozhippurath  
Narayana Panicker, Laura Phillips, Frank Reade, Selvakumar T. S., and Alan Twigg  
Editing: Taffy Everts and Stella Hackell  
Illustration: Faith Bradford Brown and Nathaniel Woodward  
Cover Design: Edmonds Design

Revision History  
9 January 2006—Revision 1.

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

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 (including the ERX-310, ERX-705, ERX-710, ERX-1410, ERX-1440, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, and T320 routers, T640 routing node, and the JUNOS and SDX-300 software) 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.

## YEAR 2000 NOTICE

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

## 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](http://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 Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and 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, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller.

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 the Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller, unless the applicable Juniper documentation expressly permits installation on non-Juniper equipment.

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.

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, 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. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

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 the Software on non-Juniper equipment where the Juniper documentation does not expressly permit installation on non-Juniper equipment; (j) use the 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 for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

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

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

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

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

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés 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

xvii

### Part 1

#### Using the Configuration Interfaces

Chapter 1	Using J-Web Configuration Tools	3
-----------	---------------------------------	---

### Part 2

#### Configuring Router Interfaces

Chapter 2	Interfaces Overview	39
Chapter 3	Configuring Network Interfaces	99
Chapter 4	Configuring Digital Subscriber Line Interfaces	131
Chapter 5	Configuring Point-to-Point Protocol over Ethernet	165
Chapter 6	Configuring ISDN	187

### Part 3

#### Configuring Routing Protocols

Chapter 7	Routing Overview	233
Chapter 8	Configuring Static Routes	267
Chapter 9	Configuring a RIP Network	279
Chapter 10	Configuring an OSPF Network	295
Chapter 11	Configuring the IS-IS Protocol	315
Chapter 12	Configuring BGP Sessions	323

## Part 4

## Index

---

# Table of Contents

---

## About This Guide xvii

Objectives .....	xvii
Audience.....	xviii
Document Conventions .....	xviii
Related Juniper Networks Documentation.....	xx
Documentation Feedback.....	xxii
Requesting Support.....	xxii

## Part 1

---

## Using the Configuration Interfaces

### Chapter 1

---

### Using J-Web Configuration Tools 3

Configuration Tools Terms .....	3
Configuration Tools Overview .....	4
Editing and Committing a Configuration.....	4
J-Web Configuration Options.....	5
CLI Configuration Commands .....	5
Filtering Configuration Command Output .....	6
Before You Begin.....	6
Using J-Web Quick Configuration.....	7
Using the J-Web Configuration Editor .....	8
Viewing the Configuration Text .....	8
Editing and Committing the Clickable Configuration .....	9
Editing the Clickable Configuration.....	9
Discarding Parts of a Candidate Configuration .....	12
Committing a Clickable Configuration.....	13
Editing and Committing the Configuration Text.....	13
Uploading a Configuration File.....	14
Managing Configuration Files with the J-Web Interface .....	15
Configuration Database and History Overview.....	16
Displaying Users Editing the Configuration .....	18
Comparing Configuration Files .....	18
Downloading a Configuration File .....	19
Loading a Previous Configuration File.....	20
Setting, Viewing, or Deleting the Rescue Configuration .....	20
Using the CLI Configuration Editor .....	21
Entering and Exiting Configuration Mode .....	21
Navigating the Configuration Hierarchy.....	23
Modifying the Configuration .....	24
Adding or Modifying a Statement or Identifier .....	25

Deleting a Statement or Identifier .....	25
Copying a Statement.....	26
Renaming an Identifier .....	26
Inserting an Identifier .....	27
Deactivating a Statement or Identifier.....	28
Committing a Configuration with the CLI.....	29
Verifying a Configuration .....	29
Committing a Configuration and Exiting Configuration Mode .....	30
Committing a Configuration That Requires Confirmation .....	30
Scheduling and Canceling a Commit .....	30
Loading a Previous Configuration File with the CLI .....	31
Setting or Deleting the Rescue Configuration with the CLI .....	32
Disabling the CONFIG Button .....	32
Entering Operational Mode Commands During Configuration.....	33
Managing Configuration Files with the CLI .....	33
Loading a New Configuration File .....	33
Saving a Configuration File.....	36

## Part 2

## Configuring Router Interfaces

---

### Chapter 2

<b>Interfaces Overview</b>	<b>39</b>
Interfaces Terms .....	40
Network Interfaces .....	43
Media Types .....	44
Network Interface Naming .....	44
J-series Interface Naming Conventions .....	45
Understanding CLI Output for J-series Interfaces .....	47
Data Link Layer Overview.....	48
Physical Addressing.....	48
Network Topology.....	48
Error Notification .....	48
Frame Sequencing .....	48
Flow Control.....	49
Data Link Sublayers.....	49
MAC Addressing.....	49
Ethernet Interface Overview .....	50
Ethernet Access Control and Transmission .....	50
Collisions and Detection.....	51
Collision Detection .....	51
Backoff Algorithm .....	51
Collision Domains and LAN Segments .....	52
Repeaters .....	52
Bridges and Switches .....	52
Broadcast Domains .....	53
Ethernet Frames .....	53
T1 and E1 Interfaces Overview .....	54
T1 Overview.....	54
E1 Overview.....	55



T1 and E1 Signals .....	55
Encoding .....	55
AMI Encoding .....	55
B8ZS and HDB3 Encoding .....	56
T1 and E1 Framing .....	56
Superframe (D4) Framing for T1 .....	56
Extended Superframe (ESF) Framing for T1 .....	57
T1 and E1 Loopback Signals .....	57
T3 and E3 Interfaces Overview .....	58
Multiplexing DS1 Signals .....	58
DS2 Bit Stuffing .....	59
DS3 Framing .....	59
M13 Asynchronous Framing .....	59
C-Bit Parity Framing .....	61
Serial Interface Overview .....	63
Serial Transmissions .....	64
Signal Polarity .....	65
Serial Clocking Modes .....	65
Serial Interface Transmit Clock Inversion .....	66
DTE Clock Rate Reduction .....	66
Serial Line Protocols .....	66
EIA-530 .....	67
RS-232 .....	67
RS-422/449 .....	68
V.35 .....	68
X.21 .....	69
ADSL Interface Overview .....	69
ADSL Systems .....	70
ADSL2 and ADSL2+ .....	71
Asynchronous Transfer Mode .....	71
SHDSL Interface Overview .....	72
ISDN Interface Overview .....	72
ISDN Channels .....	72
ISDN Interfaces .....	72
Typical ISDN Network .....	73
NT Devices and S and T Interfaces .....	73
U Interface .....	74
ISDN Call Setup .....	74
Layer 2 ISDN Connection Initialization .....	74
Layer 3 ISDN Session Establishment .....	74
Interface Physical Properties .....	75
Bit Error Rate Testing .....	76
Interface Clocking .....	76
Data Stream Clocking .....	77
Explicit Clocking Signal Transmission .....	77
Frame Check Sequences .....	78
Cyclic Redundancy Checks and Checksums .....	78
Two-Dimensional Parity .....	78
Physical Encapsulation on an Interface .....	79
Frame Relay .....	79
Virtual Circuits .....	80
Switched and Permanent Virtual Circuits .....	80
Data-Link Connection Identifiers .....	80

Congestion Control and Discard Eligibility .....	80
Point-to-Point Protocol .....	81
Link Control Protocol .....	81
CHAP Authentication .....	82
Network Control Protocols .....	82
Magic Numbers .....	83
CSU/DSU Devices .....	83
Point-to-Point Protocol over Ethernet .....	83
PPPoE Discovery .....	84
PPPoE Sessions .....	84
High-Level Data Link Control .....	85
HDLC Stations .....	85
HDLC Operational Modes .....	85
Interface Logical Properties .....	86
Protocol Families .....	86
Common Protocol Suites .....	87
Other Protocol Suites .....	87
IPv4 Addressing .....	87
IPv4 Classful Addressing .....	88
IPv4 Dotted Decimal Notation .....	88
IPv4 Subnetting .....	89
IPv4 Variable-Length Subnet Masks .....	90
IPv6 Addressing .....	90
IPv6 Address Representation .....	90
IPv6 Address Types .....	91
IPv6 Address Scope .....	91
IPv6 Address Structure .....	91
Virtual LANs .....	92
Special Interfaces .....	93
Discard Interface .....	95
Loopback Interface .....	96
Management Interface .....	96
Services Interfaces .....	97
MLPPP and MLFR .....	97
MLFR Frame Relay Forum .....	97
CRTP .....	97

## Chapter 3

## Configuring Network Interfaces

99

Before You Begin .....	99
Configuring Network Interfaces with Quick Configuration .....	100
Configuring an E1 Interface with Quick Configuration .....	101
Configuring an E3 Interface with Quick Configuration .....	104
Configuring a Fast Ethernet Interface with Quick Configuration .....	109
Configuring a T1 Interface with Quick Configuration .....	111
Configuring a T3 Interface with Quick Configuration .....	115
Configuring a Serial Interface with Quick Configuration .....	118
Configuring Network Interfaces with a Configuration Editor .....	122
Adding a Network Interface with a Configuration Editor .....	122
Configuring Compressed Real-Time Transport Protocol (CRTP) .....	124
Deleting a Network Interface with a Configuration Editor .....	126

Verifying Interface Configuration .....	127
Verifying the Link State of All Interfaces .....	127
Verifying Interface Properties .....	128
<b>Chapter 4</b>	<b>Configuring Digital Subscriber Line Interfaces</b>
	<b>131</b>
DSL Terms .....	131
Before You Begin .....	132
Configuring ATM-over-ADSL Interfaces .....	133
Configuring an ATM-over-ADSL Interface with Quick Configuration .....	133
Adding an ATM-over-ADSL Network Interface with a Configuration Editor .....	138
Configuring ATM-over-SHDSL Interfaces .....	143
Configuring an ATM-over-SHDSL Interface with Quick Configuration .....	144
Adding an ATM-over-SHDSL Interface with a Configuration Editor .....	149
Configuring CHAP on DSL Interfaces (Optional) .....	154
Verifying DSL Interface Configuration .....	156
Verifying ADSL Interface Properties .....	156
Displaying a PPPoA Configuration for an ATM-over-ADSL Interface .....	160
Verifying an ATM-over-SHDSL Configuration .....	161
<b>Chapter 5</b>	<b>Configuring Point-to-Point Protocol over Ethernet</b>
	<b>165</b>
PPPoE Terms .....	165
PPPoE Overview .....	166
PPPoE Interfaces .....	167
Fast Ethernet Interface .....	167
ATM-over-ADSL or ATM-over-SHDSL Interface .....	167
PPPoE Stages .....	168
PPPoE Discovery Stage .....	168
PPPoE Session Stage .....	168
Optional CHAP Authentication .....	169
Before You Begin .....	169
Configuring a PPPoE Interface with Quick Configuration .....	169
Configuring PPPoE with a Configuration Editor .....	172
Setting the Appropriate Encapsulation on the Interface (Required) .....	172
Configuring PPPoE Encapsulation on an Ethernet Interface .....	173
Configuring PPPoE Encapsulation on an ATM-over-ADSL or ATM-over-SHDSL Interface .....	174
Configuring a PPPoE Interface (Required) .....	175
Configuring CHAP on a PPPoE Interface (Optional) .....	178
Verifying a PPPoE Configuration .....	180
Displaying a PPPoE Configuration for an Ethernet Interface .....	180
Displaying a PPPoE Configuration for an ATM-over-ADSL or ATM-over-SHDSL Interface .....	181
Verifying PPPoE Interfaces .....	182
Verifying PPPoE Sessions .....	183
Verifying the PPPoE Version .....	183
Verifying PPPoE Statistics .....	184
<b>Chapter 6</b>	<b>Configuring ISDN</b>
	<b>187</b>

ISDN Terms .....	187
ISDN Overview .....	189
ISDN Interfaces .....	189
Before You Begin .....	190
Configuring ISDN Interfaces with Quick Configuration .....	191
Configuring ISDN Physical Interfaces with Quick Configuration .....	191
Configuring ISDN Dialer Interfaces with Quick Configuration .....	194
Configuring ISDN Interfaces with a Configuration Editor .....	198
Adding an ISDN Interface (Required) .....	198
Configuring a Dialer Interface (Required) .....	201
Configuring Dial Backup .....	204
Configuring a Dialer Filter for Dial-on-Demand Routing Backup .....	205
Configuring the Dialer Filter .....	205
Applying the Dial-on-Demand Dialer Filter to the Dialer Interface .....	206
Configuring Dialer Watch .....	207
Adding a Dialer Watch Interface on the Services Router .....	207
Configuring the ISDN Interface for Dialer Watch .....	208
Configuring Dial-on-Demand Routing Backup with OSPF Support (Optional) .....	209
Configuring Bandwidth on Demand (Optional) .....	210
Configuring a Dialer Interface for Bandwidth on Demand .....	210
Configuring an ISDN Interface for Bandwidth on Demand .....	214
Configuring Dial-In and Callback (Optional) .....	215
Configuring a Dialer Interface for Dial-In and Callback .....	217
Configuring an ISDN Interface to Screen Incoming Calls .....	219
Configuring the Services Router to Reject Incoming ISDN Calls .....	220
Configuring Dialer Profiles (Optional) .....	220
Verifying the ISDN Configuration .....	222
Displaying the ISDN Status .....	222
Verifying an ISDN Interface .....	223
Checking B-Channel Statistics .....	224
Checking D-Channel Interface Statistics .....	225
Displaying the Status of ISDN Calls .....	226
Verifying Dialer Interface Configuration .....	227

## Part 3

## Configuring Routing Protocols

### Chapter 7

### Routing Overview 233

Routing Terms .....	233
Routing Overview .....	237
Networks and Subnetworks .....	238
Autonomous Systems .....	238
Interior and Exterior Gateway Protocols .....	238
Routing Tables .....	239
Forwarding Tables .....	239
Dynamic and Static Routing .....	240
Route Advertisements .....	241
Route Aggregation .....	241

RIP Overview .....	243
Distance-Vector Routing Protocols .....	243
Maximizing Hop Count .....	244
RIP Packets .....	245
Split Horizon and Poison Reverse Efficiency Techniques .....	245
Limitations of Unidirectional Connectivity .....	246
OSPF Overview .....	247
Link-State Advertisements .....	248
Role of the Designated Router .....	248
Path Cost Metrics .....	249
Areas and Area Border Routers .....	249
Role of the Backbone Area .....	250
Stub Areas and Not-So-Stubby Areas .....	251
IS-IS Overview .....	252
IS-IS Areas .....	253
Network Entity Titles and System Identifiers .....	253
IS-IS Path Selection .....	254
Protocol Data Units .....	254
IS-IS Hello PDU .....	254
Link-State PDU .....	254
Complete Sequence Number PDU .....	255
Partial Sequence Number PDU .....	255
BGP Overview .....	255
Point-to-Point Connections .....	256
BGP Messages for Session Establishment .....	256
BGP Messages for Session Maintenance .....	257
IBGP and EBGP .....	257
Route Selection .....	258
Local Preference .....	258
AS Path .....	259
Origin .....	260
Multiple Exit Discriminator .....	260
Scaling BGP for Large Networks .....	261
Route Reflectors—for Added Hierarchy .....	261
Confederations—for Subdivision .....	264

## Chapter 8

## Configuring Static Routes 267

Static Routing Overview .....	267
Static Route Preferences .....	268
Qualified Next Hops .....	268
Control of Static Routes .....	268
Route Retention .....	269
Readvertisement Prevention .....	269
Forced Rejection of Passive Route Traffic .....	269
Default Properties .....	269
Before You Begin .....	270
Configuring Static Routes with Quick Configuration .....	270
Configuring Static Routes with a Configuration Editor .....	272
Configuring a Basic Set of Static Routes (Required) .....	272
Controlling Static Route Selection (Optional) .....	273
Controlling Static Routes in the Routing and Forwarding Tables (Optional) .....	275

Defining Default Behavior for All Static Routes (Optional).....	276
Verifying the Static Route Configuration .....	277
Displaying the Routing Table.....	277

## **Chapter 9                      Configuring a RIP Network                      279**

RIP Overview.....	279
RIP Traffic Control with Metrics.....	279
Authentication.....	280
Before You Begin.....	280
Configuring a RIP Network with Quick Configuration .....	280
Configuring a RIP Network with a Configuration Editor .....	283
Configuring a Basic RIP Network (Required).....	283
Controlling Traffic in a RIP Network (Optional).....	286
Controlling Traffic with the Incoming Metric.....	286
Controlling Traffic with the Outgoing Metric.....	287
Enabling Authentication for RIP Exchanges (Optional) .....	289
Enabling Authentication with Plain-Text Passwords.....	289
Enabling Authentication with MD5 Authentication .....	290
Verifying the RIP Configuration.....	291
Verifying the RIP-Enabled Interfaces .....	291
Verifying the Exchange of RIP Messages.....	291
Verifying Reachability of All Hosts in the RIP Network .....	292

## **Chapter 10                      Configuring an OSPF Network                      295**

OSPF Overview .....	295
Enabling OSPF .....	295
OSPF Areas .....	296
Path Cost Metrics .....	296
OSPF Dial-on-Demand Circuits .....	296
Before You Begin.....	297
Configuring an OSPF Network with Quick Configuration .....	297
Configuring an OSPF Network with a Configuration Editor .....	299
Configuring the Router Identifier (Required).....	300
Configuring a Single-Area OSPF Network (Required) .....	300
Configuring a Multiarea OSPF Network (Optional) .....	302
Creating the Backbone Area.....	303
Creating Additional OSPF Areas.....	303
Configuring Area Border Routers .....	304
Configuring Stub and Not-So-Stubby Areas (Optional) .....	305
Tuning an OSPF Network for Efficient Operation .....	307
Controlling Route Selection in the Forwarding Table.....	308
Controlling the Cost of Individual Network Segments .....	308
Enabling Authentication for OSPF Exchanges .....	309
Controlling Designated Router Election .....	310
Verifying an OSPF Configuration .....	311
Verifying OSPF-Enabled Interfaces .....	311
Verifying OSPF Neighbors.....	312
Verifying the Number of OSPF Routes .....	313

Verifying Reachability of All Hosts in an OSPF Network.....	314
---	-----

**Chapter 11****Configuring the IS-IS Protocol 315**

IS-IS Overview .....	315
ISO Network Addresses.....	315
System Identifier Mapping .....	316
Before You Begin.....	316
Configuring IS-IS with a Configuration Editor .....	317
Verifying IS-IS on a Services Router .....	318
Displaying IS-IS Interface Configuration .....	319
Displaying IS-IS Interface Configuration Detail .....	319
Displaying IS-IS Adjacencies .....	320
Displaying IS-IS Adjacencies in Detail .....	321

**Chapter 12****Configuring BGP Sessions 323**

BGP Overview.....	323
BGP Peering Sessions.....	323
IBGP Full Mesh Requirement.....	324
Route Reflectors and Clusters.....	324
BGP Confederations .....	324
Before You Begin.....	325
Configuring BGP Sessions with Quick Configuration .....	325
Configuring BGP Sessions with a Configuration Editor .....	327
Configuring a Point-to-Point Peering Session (Required).....	327
Configuring BGP Within a Network (Required) .....	330
Configuring a Route Reflector (Optional) .....	331
Configuring BGP Confederations (Optional) .....	334
Verifying a BGP Configuration .....	336
Verifying BGP Neighbors .....	336
Verifying BGP Groups.....	337
Verifying BGP Summary Information .....	338
Verifying Reachability of All Peers in a BGP Network .....	339

**Part 4****Index**

Index.....	343
------------	-----





# About This Guide

This preface provides the following guidelines for using the *J-series™ Services Router Basic LAN and WAN Access Configuration Guide*:

- Objectives on page xvii
- Audience on page xviii
- Document Conventions on page xviii
- Related Juniper Networks Documentation on page xx
- Documentation Feedback on page xxii
- Requesting Support on page xxii

## Objectives

---

This guide contains instructions for configuring the interfaces on a Services Router for basic IP routing with standard routing protocols. It also shows how to create backup ISDN interfaces, configure virtual private networks (VPNs), configure and manage multicast networks, and apply routing techniques such as policies, firewall filters, IP Security (IPSec) tunnels, and class-of-service (CoS) classification for safe, efficient routing.



**NOTE:** This guide documents Release 7.5 of the JUNOS software. For additional information about J-series Services Routers—either corrections to or omissions from this guide—see the *J-series Services Router Release Notes* at <http://www.juniper.net>.

---

J-series Services Router operations are controlled by the JUNOS Internet software. You direct the JUNOS software through either a Web browser or a command-line interface (CLI) to perform the tasks shown in Table 1.

**Table 1: Capabilities of J-series Interfaces**

<b>J-series Interface</b>	<b>Capabilities</b>
J-Web graphical browser interface	<ul style="list-style-type: none"> <li>■ Quick (basic) configuration</li> <li>■ Monitoring, configuration, diagnosis, and management</li> </ul>
JUNOS CLI	Monitoring, configuration, diagnosis, and management

J-series Services Router guides provide complete instructions for using the J-Web interface, but they are not a comprehensive resource for using the JUNOS CLI. For CLI information, see the JUNOS software manuals listed in “Related Juniper Networks Documentation” on page xx.

## Audience

This guide is designed for anyone who installs and sets up a J-series Services Router or prepares a site for Services Router installation. The guide is intended for the following audiences:


- Customers with technical knowledge of and experience with networks and the Internet
- Network administrators who install, configure, and manage Internet routers but are unfamiliar with the JUNOS software
- Network administrators who install, configure, and manage products of Juniper Networks

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

## Document Conventions

Table 2 defines the notice icons used in this guide.

**Table 2: Notice Icons**

<b>Icon</b>	<b>Meaning</b>	<b>Description</b>
	Informational note	Indicates important features or instructions.



Icon	Meaning	Description
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.

Table 3 defines the text and syntax conventions used in this guide.

**Table 3: Text and Syntax Conventions**

Convention	Description	Examples
<b>Bold sans serif typeface</b>	Represents text that you type.	To enter configuration mode, type the <code>configure</code> command:  user@host> <b>configure</b>
Fixed-width typeface	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic typeface</i>	<ul style="list-style-type: none"> <li>Introduces important new terms.</li> <li>Identifies book names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>JUNOS System Basics Configuration Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>
<i>Italic sans serif typeface</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# <b>set system domain-name</b> <i>domain-name</i>
Sans serif typeface	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit protocols ospf area <i>area-id</i>] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast   multicast ( <i>string1</i>   <i>string2</i>   <i>string3</i> )
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [ <i>community-ids</i> ]

Convention	Description	Examples
Indention and braces ( { } )	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop address; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
<b>J-Web GUI Conventions</b>		
Bold typeface	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"><li>■ In the Logical Interfaces box, select <b>All Interfaces</b>.</li><li>■ To cancel the configuration, click <b>Cancel</b>.</li></ul>
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select <b>Protocols &gt; Ospf</b> .

## Related Juniper Networks Documentation

J-series Services Routers are documented in four guides. Although the J-series guides provide instructions for configuring and managing a Services Router with the JUNOS CLI, they are not a comprehensive JUNOS software resource. For complete documentation of the statements and commands described in J-series guides, see the JUNOS software manuals listed in Table 4.

**Table 4: J-series Guides and Related JUNOS Software Publications**

Chapter in a J-series Guide	Corresponding JUNOS Software Manual
<b>J-series Services Router Getting Started Guide</b>	
“J-series User Interface Overview”	<i>JUNOS System Basics Configuration Guide</i>
“Establishing Basic Connectivity”	
“Configuring Autoinstallation”	
<b>J-series Services Router Basic LAN and WAN Access Configuration Guide</b>	
“Using J-Web Configuration Tools”	<i>JUNOS System Basics Configuration Guide</i>
“Interfaces Overview”	■ <i>JUNOS Network Interfaces Configuration Guide</i>
“Configuring Network Interfaces”	■ <i>JUNOS Interfaces Command Reference</i>
“Configuring Digital Subscriber Line Interfaces	
“Configuring Point-to-Point Protocol over Ethernet”	
“Configuring ISDN”	

Chapter in a J-series Guide	Corresponding JUNOS Software Manual
“Routing Overview”	■ <i>JUNOS Routing Protocols Configuration Guide</i>
“Configuring Static Routes”	■ <i>JUNOS Routing Protocols and Policies Command Reference</i>
“Configuring a RIP Network”	
“Configuring an OSPF Network”	
“Configuring the IS-IS Protocol”	
“Configuring BGP Sessions”	
<b>J-series Services Router Advanced WAN Access Configuration Guide</b>	
“Multiprotocol Label Switching Overview”	■ <i>JUNOS MPLS Applications Configuration Guide</i>
“Configuring Signaling Protocols for Traffic Engineering”	■ <i>JUNOS Routing Protocols and Policies Command Reference</i>
“Configuring Virtual Private Networks”	■ <i>JUNOS VPNs Configuration Guide</i>
“Configuring CLNS VPNs”	
“Configuring IPSec for Secure Packet Exchange”	■ <i>JUNOS System Basics Configuration Guide</i> ■ <i>JUNOS Services Interfaces Configuration Guide</i> ■ <i>JUNOS System Basics and Services Command Reference</i>
“Multicast Overview”	<i>JUNOS Multicast Protocols Configuration Guide</i>
“Configuring a Multicast Network”	<i>JUNOS Routing Protocols and Policies Command Reference</i>
“Configuring Data Link Switching”	■ <i>JUNOS Services Interfaces Configuration Guide</i> ■ <i>JUNOS System Basics and Services Command Reference</i>
“Policy Framework Overview”	<i>JUNOS Policy Framework Configuration Guide</i>
“Configuring Routing Policies”	<i>JUNOS Routing Protocols and Policies Command Reference</i>
“Configuring Stateful Firewall Filters and NAT”	■ <i>JUNOS Network Interfaces Configuration Guide</i>
“Configuring Stateless Firewall Filters”	■ <i>JUNOS Policy Framework Configuration Guide</i> ■ <i>JUNOS Services Interfaces Configuration Guide</i> ■ <i>JUNOS System Basics and Services Command Reference</i> ■ <i>JUNOS Routing Protocols and Policies Command Reference</i>
“Class-of-Service Overview”	■ <i>JUNOS Class of Service Configuration Guide</i>
“Configuring Class of Service”	■ <i>JUNOS System Basics and Services Command Reference</i>
<b>J-series Services Router Administration Guide</b>	
“Managing Users and Operations”	<i>JUNOS System Basics Configuration Guide</i>
“Configuring SNMP for Network Management”	<i>JUNOS Network Management Configuration Guide</i>
“Configuring the DHCP Server”	<i>JUNOS System Basics Configuration Guide</i>
“Configuring and Monitoring Alarms”	<i>JUNOS System Basics Configuration Guide</i>

Chapter in a J-series Guide	Corresponding JUNOS Software Manual
"Monitoring a Services Router"	■ <i>JUNOS System Basics and Services Command Reference</i>
"Using Services Router Diagnostic Tools"	■ <i>JUNOS Interfaces Command Reference</i> ■ <i>JUNOS Routing Protocols and Policies Command Reference</i>
"Configuring Packet Capture"	<i>JUNOS Services Interfaces Configuration Guide</i>
"Monitoring Real-Time Performance"	<i>JUNOS System Basics and Services Command Reference</i>

## 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](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <http://www.juniper.net/techpubs/docbug/docbugreport.html>. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version

## Requesting Support

For technical support, open a support case with the Case Manager link at <http://www.juniper.net/support/> or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

## **Part 1**

# **Using the Configuration Interfaces**

- Using J-Web Configuration Tools on page 3





## Chapter 1

# Using J-Web Configuration Tools

Use J-Web configuration tools to configure all services on a router, including system parameters, routing protocols, interfaces, network management, and user access.

This chapter contains the following topics:

- Configuration Tools Terms on page 3
- Configuration Tools Overview on page 4
- Before You Begin on page 6
- Using J-Web Quick Configuration on page 7
- Using the J-Web Configuration Editor on page 8
- Managing Configuration Files with the J-Web Interface on page 15
- Using the CLI Configuration Editor on page 21
- Managing Configuration Files with the CLI on page 33

## Configuration Tools Terms

Before using the Services Router configuration tools, become familiar with the terms defined in Table 5.

**Table 5: Configuration Tools Terms**

Term	Definition
candidate configuration	A working copy of the configuration that can be edited without affecting the Services Router until it is committed.
configuration group	Group of configuration statements that can be inherited by the rest of the configuration.
commit a configuration	Have the candidate configuration checked for proper syntax, activated, and marked as the current configuration file running on the Services Router.
configuration hierarchy	The JUNOS software configuration consists of a hierarchy of <i>statements</i> . There are two types of statements: <i>container statements</i> , which contain other statements, and <i>leaf statements</i> , which do not contain other statements. All the container and leaf statements together form the configuration hierarchy.

**Table 5: Configuration Tools Terms (continued)**

Term	Definition
rescue configuration	Configuration that recovers a Services Router from a configuration that denies management access. You set a current committed configuration through the J-Web interface or CLI for emergency use. To load and commit the rescue configuration, you press and release the CONFIG button.
roll back a configuration	Return to a previously committed configuration.

## Configuration Tools Overview

The J-Web interface provides a Quick Configuration tool for basic configuration and a configuration editor for complete configuration. You can also use the JUNOS CLI configuration mode as a configuration editor to create and modify a complete configuration hierarchy. For a comparison of configuration interfaces, see the *J-series Services Router Getting Started Guide*.

This section contains the following topics:

- Editing and Committing a Configuration on page 4
- J-Web Configuration Options on page 5
- CLI Configuration Commands on page 5

### Editing and Committing a Configuration

When you edit a configuration, you work in a copy of the current configuration to create a candidate configuration. The changes you make to the candidate configuration are visible through the user interface immediately, but do not take effect on the Services Router until you *commit* the changes. When you commit the configuration, the candidate file is checked for proper syntax, activated, and marked as the current, operational software configuration file. If multiple users are editing the configuration when you commit the candidate configuration, all changes made by all the users take effect.

If you are editing the configuration with the CLI, you can edit an *exclusive* or *private* candidate configuration. For more information, see “Entering and Exiting Configuration Mode” on page 21.

When you commit a configuration, the Services Router saves the current operational version and the previous 49 versions of committed configurations. The most recently committed configuration is version 0 (the current operational version), and the oldest saved configuration is version 49. You can roll back the configuration to any saved version. Version 0 is stored in the file `juniper.conf`, and the last three committed configurations are stored in the files `juniper.conf.1.gz`, `juniper.conf.2.gz`, and `juniper.conf.3.gz`. These four files are located in the `/config` directory, and the

remaining 46 previous versions of committed configurations—files `juniper.conf.4.gz` through `juniper.conf.49.gz`—are stored in the `/var/db/config` directory.

## J-Web Configuration Options

You access the J-Web interface configuration tools by selecting **Configuration** in the task bar. Table 6 describes the J-Web configuration options.

**Table 6: J-Web Configuration Options**

Option	Purpose	Description
Quick Configuration	Basic configuration	Displays options for quick Services Router configuration— <b>Set Up</b> , <b>SSL</b> , <b>Interfaces</b> , <b>Users</b> , <b>SNMP</b> , <b>Routing</b> , <b>Firewall/NAT</b> , and <b>IPSec Tunnels</b> . You can access these options in both the side and main panes. For more information, see “Using J-Web Quick Configuration” on page 7.
View and Edit	Complete configuration	Displays the configuration editor options— <b>View Configuration</b> , <b>Edit Configuration</b> , <b>Edit Configuration Text</b> , and <b>Upload Configuration File</b> . For more information, see “Using the J-Web Configuration Editor” on page 8.
History	File management	Displays the Services Router configuration history and a list of users currently editing the configuration. You can compare, roll back, or download specific versions of the configuration. For more information, see “Managing Configuration Files with the J-Web Interface” on page 15.
Rescue	Configuration recovery	Displays options for setting the current configuration as the rescue configuration, and for viewing and deleting the rescue configuration. For more information, see “Setting, Viewing, or Deleting the Rescue Configuration” on page 20.

## CLI Configuration Commands

The CLI configuration commands allow you to perform the same configuration tasks you can perform using the J-Web interface. Instead of invoking the tools through a graphical interface, you enter configuration mode commands to perform the tasks.

Table 7 provides a summary of the top-level CLI configuration commands.

**Table 7: Top-Level CLI Configuration Commands**

Command	Function
<b>Managing the Configuration and Configuration Files</b>	
<code>commit</code>	Commit the set of configuration changes in the candidate configuration to take operational effect.

**Table 7: Top-Level CLI Configuration Commands (continued)**

Command	Function
load	Load a configuration from an ASCII configuration file or from terminal input.
rollback	Return to a previously committed configuration.
save	Save the configuration to an ASCII file.
<b>Modifying the Configuration and Its Statements</b>	
activate	Activate a previously deactivated statement or identifier.
annotate	Add a comment to a statement.
copy	Copy and add a statement to the configuration.
deactivate	Deactivate a statement or identifier.
delete	Delete a statement or identifier from the configuration.
insert	Insert an identifier into an existing hierarchy.
rename	Rename an existing statement or identifier.
set	Create a statement hierarchy and set identifier values.
<b>Navigating the Configuration Hierarchy</b>	
edit	Move inside the specified statement hierarchy.
exit	Exit the current level of the statement hierarchy (same function as quit).
quit	Exit the current level of the statement hierarchy (same function as exit).
top	Return to the top level of configuration mode.
up	Move up one level in the statement hierarchy.
<b>Miscellaneous</b>	
help	Provide help about statements.
run	Issue an operational mode command without leaving configuration mode.
show	Display the current configuration.
status	Display the users currently editing the configuration.

For more information about CLI configuration mode commands, see the JUNOS software configuration guides.

## Filtering Configuration Command Output

Certain configuration commands, such as `show` commands, display output. You can filter or redirect the output to a file by including a vertical bar (`|`), called a *pipe*, when you enter the command. For more information, see the *J-series Services Router Administration Guide*.

## Before You Begin

To use the J-Web interface and CLI configuration tools, you must have the appropriate access privileges. For more information about configuring

access privilege levels, see the *J-series Services Router Administration Guide* and the *JUNOS System Basics Configuration Guide*.

## Using J-Web Quick Configuration

Use J-Web Quick Configuration to quickly and easily configure the Services Router for basic operation. To access Quick Configuration, select **Configuration > Quick Configuration**. You can select a Quick Configuration option from either the side pane or the main pane (see Figure 1). To configure the Services Router using Quick Configuration, see the configuration sections in this manual.

**Figure 1: J-Web Quick Configuration Options**

Juniper NETWORKS

ROUTER - J4300

Logged in as: **regress**

[Help](#) [About](#) [Logout](#)

**Monitor** **Configuration** **Diagnose** **Manage**

[Configuration > Quick Configuration > Summary](#)

### Quick Configuration

#### Summary

#### Router Configuration

The following pages help you to configure your router quickly and easily. They provide access to the most commonly configured parameters and are useful in generating the initial configuration of the router.

- ▶ **Set Up**  
Define network identification, default gateway, name and time servers, root user authentication, and basic local network access to the system.
- ▶ **SSL**  
Configure certificates and SSL access methods.
- ▶ **Interfaces**  
List all interfaces installed on system and configure logical interfaces and common interface parameters.
- ▶ **Users**  
Define users allowed to access the router and configure authentication servers. Pick authorization level for each user.

▶ **Quick Configuration**

- Set Up
- SSL
- Interfaces
- Users
- SNMP
- Routing
- Firewall/NAT
- IPSec Tunnels
- Realtime Performance Monitoring

▶ **View and Edit**

▶ **History**

▶ **Rescue**

Table 8 describes the functions of the buttons that appear in the J-Web Quick Configuration pages.

**Table 8: J-Web Quick Configuration Buttons**

Button	Function
Add	Adds statements or identifiers to the configuration.
Delete	Deletes statements or identifiers from the configuration.
OK	Commits your entries into the configuration, and returns you one level up in the configuration hierarchy.
Cancel	Clears the entries you have not yet applied to the configuration, and returns you one level up in the configuration hierarchy.
Apply	Commits your entries into the configuration, and stays at the same level in the configuration hierarchy.

## Using the J-Web Configuration Editor

You can use the J-Web configuration editor to perform the following tasks:

- Viewing the Configuration Text on page 8
- Editing and Committing the Clickable Configuration on page 9
- Editing and Committing the Configuration Text on page 13
- Uploading a Configuration File on page 14

### Viewing the Configuration Text

To view the entire configuration in text format, select **Configuration > View and Edit > View Configuration Text**. The main pane displays the configuration in text format (see Figure 2).

Each level in the hierarchy is indented to indicate each statement's relative position in the hierarchy. Each level is generally set off with braces, using an open brace ( { ) at the beginning of each hierarchy level and a closing brace ( } ) at the end. If the statement at a hierarchy level is empty, the braces are not displayed. Each leaf statement ends with a semicolon ( ; ), as does the last statement in the hierarchy.

This indented representation is used when the configuration is displayed or saved as an ASCII file. However, when you load an ASCII configuration file, the format of the file is not so strict. The braces and semicolons are required, but the indention and use of new lines are not required in ASCII configuration files.

**Figure 2: View Configuration Text Page**

Juniper NETWORKS **ROUTER - J4300** Logged in as: **regress**  
[Help](#) [About](#) [Logout](#)

**Monitor** **Configuration** **Diagnose** **Manage**

► Quick Configuration  
 ▼ View and Edit  
 View Configuration Text  
 Edit Configuration  
 Edit Configuration Text  
 Upload Configuration File  
 ► History  
 ► Rescue

**View and Edit**  
**View Configuration Text**  
 The current configuration running on the router

```
version "7.1I10 [builder]";
groups {
  re0 {
    system {
      host-name Router;
    }
    interfaces {
      fxp0 {
        unit 0 {
          family inet {
            address 192.168.124.65/24;
          }
        }
      }
    }
  }
}
global {
  system {
```

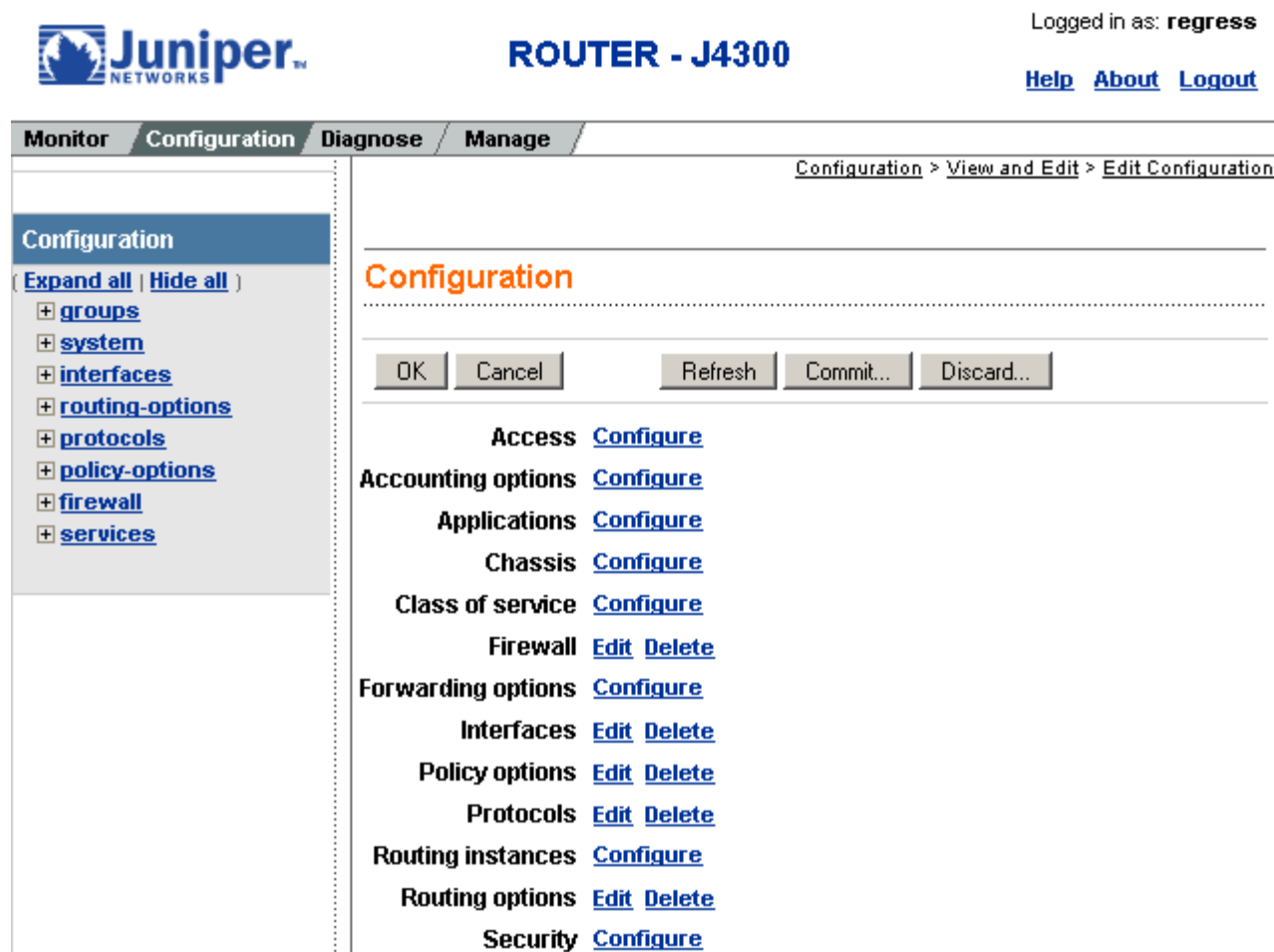
### **Editing and Committing the Clickable Configuration**

Use the J-Web configuration editor's clickable interface to perform the following configuration tasks on a Services Router:

- Editing the Clickable Configuration on page 9
- Discarding Parts of a Candidate Configuration on page 12
- Committing a Clickable Configuration on page 13

### **Editing the Clickable Configuration**

To edit the configuration on a series of pages of clickable options that steps you through the hierarchy, select **Configuration > View and Edit > Edit Configuration**. The side pane displays the top level of the configured hierarchy, and the main pane displays configured hierarchy options and the Icon Legend (see Figure 3).

**Figure 3: Edit Configuration Page (Clickable)**

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



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

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

To include, edit, or delete statements in the candidate configuration, click one of the links described in Table 9 in the main pane. Then specify configuration information by typing into a field, selecting a value from a list, or clicking a check box (toggle).



**Table 9: J-Web Edit Clickable Configuration Links**

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

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

The main pane includes icons that display information about statements and identifiers when you place your cursor over them. Table 10 describes the meaning of these icons.

**Table 10: J-Web Edit Clickable Configuration Icons**

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



**NOTE:** You can annotate statements with comments or make them inactive only through the CLI. For more information, see “Deactivating a Statement or Identifier” on page 28 and the *JUNOS System Basics Configuration Guide*.

After typing or selecting your configuration edits, click a button in the main pane (described in Table 11) to apply your changes or cancel them, refresh the display, or discard parts of the candidate configuration. An updated configuration does not take effect until you commit it.

**Table 11: J-Web Edit Clickable Configuration Buttons**

Button	Function
OK	Applies edits to the candidate configuration, and returns you one level up in the configuration hierarchy.
Cancel	Clears the entries you have not yet applied to the candidate configuration, and returns you one level up in the configuration hierarchy.
Refresh	Updates the display with any changes to the configuration made by other users.
Commit	Verifies edits and applies them to the current configuration file running on the Services Router. For details, see “Committing a Clickable Configuration” on page 13.
Discard	Removes edits applied to, or deletes existing statements or identifiers from, the candidate configuration. For details, see “Discarding Parts of a Candidate Configuration” on page 12.

## Discarding Parts of a Candidate Configuration

Before committing a candidate configuration, you can discard changes you applied or delete existing statements or identifiers.

To discard parts of a candidate configuration:

1. Navigate to the level of the hierarchy you want to edit and click **Discard**.  
  
The main pane displays a list of target statements based on the hierarchy level and the changes you have made.
2. Select a radio button to specify the appropriate discard operation or deletion. (Not all buttons appear in all situations.)
  - **Discard Changes Below This Point**—Discards changes made to the candidate configuration at the displayed hierarchy level and below. All subordinate statements and identifiers contained within a discarded statement are also discarded.
  - **Discard All Changes**—Discards all changes made to the candidate configuration.
  - **Delete Configuration Below This Point**—Deletes all changes and statements in the candidate configuration at the displayed hierarchy level and below. All subordinate statements and identifiers contained within a deleted statement are also deleted.
3. To confirm the discard operation or deletion, click **OK**.  
  
To cancel a discard operation or deletion, click **Cancel**.

The updated candidate configuration does not take effect on the Services Router until you commit it.

## Committing a Clickable Configuration

When you finish making changes to a candidate configuration with the J-Web configuration editor's clickable interface, you must commit the changes to use them in the current operational software running on the Services Router.

If another user is editing an exclusive candidate configuration with the CLI, you cannot commit a configuration until the user has committed the configuration. To display a list of users, see “Displaying Users Editing the Configuration” on page 18. For more information about editing an exclusive candidate configuration, see “Entering and Exiting Configuration Mode” on page 21.

To commit a candidate configuration:

1. In the J-Web configuration editor's clickable interface, click **Commit**.

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

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

To cancel a commit operation, click **Cancel**.

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

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

## Editing and Committing the Configuration Text

To edit the entire configuration in text format:



**CAUTION:** We recommend that you use this method to edit and commit the configuration only if you have experience editing configurations through the CLI.

---

1. Select **Configuration > View and Edit > Edit Configuration Text**. The main pane displays the configuration in a text editor (see Figure 4).

For more information about the format of an ASCII configuration file, see “Viewing the Configuration Text” on page 8.

2. Navigate to the hierarchy level you want to edit.

You can edit the candidate configuration using standard text editor operations—insert lines (by using the Enter key), delete lines, and modify, copy, and paste text.

3. Click **OK** to load and commit the configuration.

The Services Router checks the configuration for the correct syntax before committing it.

**Figure 4: Edit Configuration Text Page**

The screenshot displays the Juniper J-Web Configuration Editor interface. At the top, the Juniper Networks logo is on the left, 'ROUTER - J4300' is in the center, and 'Logged in as: regress' is on the right. Below the logo is a navigation bar with tabs: Monitor, Configuration (selected), Diagnose, and Manage. On the left side, there is a sidebar menu with options: Quick Configuration, View and Edit (selected), View Configuration Text, Edit Configuration Text, Upload Configuration File, History, and Rescue. The main content area is titled 'View and Edit' and 'Edit Configuration Text'. It includes a warning: 'Edit the configuration. When you click "Commit", the edited configuration replaces the current configuration. If any errors occur when the configuration is loading or committed, they are displayed and the configuration is restored.' Below this, a 'Configuration' section shows a text editor with the following configuration text:

```
version "7.1I0 [builder]";
groups {
  re0 {
    system {
      host-name Router;
    }
    interfaces {
      fxp0 {
        unit 0 {
          family inet {
            address 192.168.1.1;
          }
        }
      }
    }
  }
}
```

### Uploading a Configuration File

To upload a configuration file from your local system:

1. Select **Configuration > View and Edit > Upload Configuration File**.  
The main pane displays the File to Upload box (see Figure 5).
2. Specify the name of the file to upload using one of the following methods:
  - Type the absolute path and filename in the File to Upload box.

- Click **Browse** to navigate to the file.
- 3. Click **OK** to upload and commit the configuration.

The Services Router checks the configuration for the correct syntax before committing it.

**Figure 5: J-Web Upload Configuration File Page**

Juniper NETWORKS

ROUTER - J4300

Logged in as: **regress**

[Help](#) [About](#) [Logout](#)

**Monitor** **Configuration** **Diagnose** **Manage**

[Configuration](#) > [View and Edit](#) > [Upload Configuration File](#)

**View and Edit**

**Upload Configuration File**

Type the name of a configuration file on the local hard drive. When you click "Upload and Commit", the configuration in the file replaces the existing configuration and takes effect. If any errors occur when the file is loading or committing, they are displayed and the previous configuration is restored.

\* **File to Upload**   

Copyright © 2004-2005, Juniper Networks, Inc. All Rights Reserved. [Trademark Notice.](#)

## Managing Configuration Files with the J-Web Interface

The J-Web interface provides configuration database and history information that allows you to manage configuration files. This section contains the following topics:

- Configuration Database and History Overview on page 16
- Displaying Users Editing the Configuration on page 18
- Comparing Configuration Files on page 18
- Downloading a Configuration File on page 19
- Loading a Previous Configuration File on page 20
- Setting, Viewing, or Deleting the Rescue Configuration on page 20

## Configuration Database and History Overview

When you commit a configuration, the Services Router saves the current operational version and the previous 49 versions of committed configurations. To manage these configuration files with the J-Web interface, select **Configuration > History**. The main pane displays Database Information and Configuration History (see Figure 6).

Table 12 and Table 13 summarize the contents of the display.

**Figure 6: Configuration Database and History Page**

### History

---

#### Database Information

The following users are editing the configuration:

User Name	Start Time	Idle Time	Terminal	PID	Edit Flags	Edit Path
root	2005-01-18 14:57:05 PST	00:02:02	d0	2540	None	[edit groups]

---

#### Configuration History

The following table shows the router's commit history.

To view a configuration, click the revision number.

To compare configurations, select two and click "Compare".

Compare

	Number	Date/Time	User	Client	Comment	Log Message	Action
<input type="checkbox"/>	<a href="#">Current</a>	2005-01-18 16:12:46 PST	root	cli			<a href="#">Download</a>
<input type="checkbox"/>	<a href="#">1</a>	2005-01-18 15:01:13 PST	root	cli			<a href="#">Download</a> <a href="#">Rollback</a>

**Table 12: J-Web Configuration Database Information Summary**

Field	Description
User Name	Name of user editing the configuration.
Start Time	Time of day the user logged in to the Services Router.
Idle Time	Elapsed time since the user issued a configuration command from the CLI.
Terminal	Terminal on which the user is logged in.

**Table 12: J-Web Configuration Database Information Summary (continued)**

Field	Description
PID	Process identifier assigned to the user by the Services Router.
Edit Flags	Designates a private or exclusive edit.
Edit Path	Level of the configuration hierarchy that the user is editing.

**Table 13: J-Web Configuration History Summary**

Field	Description
Number	Version of the configuration file.
Date/Time	Date and time the configuration was committed.
User	Name of the user who committed the configuration.
Client	Method by which the configuration was committed: <ul style="list-style-type: none"> <li>■ cli—A user entered a JUNOS command-line interface command.</li> <li>■ junoscript—A JUNOScript client performed the operation. Commit operations performed by users through the J-Web interface are identified in this way.</li> <li>■ snmp—An SNMP <b>set</b> request started the operation.</li> <li>■ button—The CONFIG button on the router was pressed to commit the rescue configuration (if set) or to clear all configurations except the factory configuration.</li> <li>■ autoinstall—Autoinstallation was performed.</li> <li>■ other—Another method was used to commit the configuration.</li> </ul>
Comment	Comment.
Log Message	Method used to edit the configuration: <ul style="list-style-type: none"> <li>■ Imported via paste—Configuration was edited and loaded with the <b>Configuration &gt; View and Edit &gt; Edit Configuration Text</b> option. For more information, see “Editing and Committing the Configuration Text” on page 13.</li> <li>■ Imported upload [<i>filename</i>] —Configuration was uploaded with the <b>Configuration &gt; View and Edit &gt; Upload Configuration File</b> option. For more information, see “Uploading a Configuration File” on page 14.</li> <li>■ Modified via <i>quick-configuration</i>—Configuration was modified using the J-Web Quick Configuration tool specified by <i>quick-configuration</i>. For more information, see “Using J-Web Quick Configuration” on page 7.</li> <li>■ Rolled back via <i>user-interface</i>—Configuration was rolled back to a previous version through the user interface specified by <i>user-interface</i>, which can be <b>Web Interface</b> or <b>CLI</b>. For more information, see “Loading a Previous Configuration File” on page 20.</li> </ul>
Action	Action to perform with the configuration file. The action can be <b>Download</b> or <b>Rollback</b> . For more information, see “Downloading a Configuration File” on page 19 and “Loading a Previous Configuration File” on page 20.

The configuration history display allows you to perform the following operations:

- View a configuration.
- Compare two configurations.
- Download a configuration file to your local system.
- Roll back the configuration to any of the previous versions stored on the Services Router.

For more information about saved versions of configuration files, see “Editing and Committing a Configuration” on page 4.

### ***Displaying Users Editing the Configuration***

To display a list of users editing the Services Router configuration, select **Configuration > History**. The list is displayed as Database Information in the main pane (see Figure 6). Table 12 summarizes the Database Information display.

### ***Comparing Configuration Files***

To compare any two of the past 50 committed configuration files:

1. Select **Configuration > History**.

A list of the current and previous 49 configurations is displayed as Configuration History in the main pane (see Figure 6). Table 13 summarizes the Configuration History display.

2. Click two of the check boxes to the left of the configuration versions you want to compare.
3. Click **Compare**.

The main pane displays the differences between the two configuration files at each hierarchy level as follows (see Figure 7):

- Lines that have changed are highlighted side by side in green.
- Lines that exist only in the more recent configuration file are displayed in red on the left.
- Lines that exist only in the least recent configuration file are displayed in blue on the right.



**Figure 7: J-Web Configuration File Comparison Results**

<b>[edit system]</b>	<b>[edit system]</b>
	autoinstallation; radius-server { 10.10.10.10; }
<b>[edit system tacplus-server]</b>	<b>[edit system tacplus-server]</b>
	192.17.8.2;
<b>[edit system tacplus-server]</b>	<b>[edit system tacplus-server]</b>
10.7.7.9 secret "\$9\$l.le87-ds4JDbSz6A0hcbs2goG"; ## SECRET-DATA	
<b>[edit]</b>	<b>[edit]</b>
	chassis { alarm { ethernet { link-down yellow; } } }
<b>[edit interfaces fe-0/0/0 unit 0 family inet]</b>	<b>[edit interfaces fe-0/0/0 unit 0 family inet]</b>
service { input { service-set jweb-wan-sfw-service-set; } output { service-set jweb-wan-sfw-service-set; } }	
<b>[edit interfaces fe-0/0/0 unit 0 family inet]</b>	<b>[edit interfaces fe-0/0/0 unit 0 family inet]</b>
	address 192.168.124.75/24

### Downloading a Configuration File

To download a configuration file from the Services Router to your local system:

1. Select **Configuration > History**.

A list of the current and previous 49 configurations is displayed as Configuration History in the main pane (see Figure 6). Table 13 summarizes the Configuration History display.

2. In the Action column, click **Download** for the version of the configuration you want to download.

3. Select the options your Web browser provides that allow you to save the configuration file to a target directory on your local system.

The file is saved as an ASCII file.

## Loading a Previous Configuration File

To download a configuration file from the Services Router to your local system:

To load (roll back) and commit a previous configuration file stored on the Services Router:

1. Select **Configuration > History**.

A list of the current and previous 49 configurations is displayed as Configuration History in the main pane (see Figure 6). Table 13 summarizes the Configuration History display.

2. In the Action column, click **Rollback** for the version of the configuration you want to load.

The main pane displays the results of the rollback operation.



**NOTE:** When you click **Rollback**, the Services Router loads and commits the selected configuration. This behavior is different from entering the **rollback** configuration mode command from the CLI, where the configuration is loaded, but not committed.

---

## Setting, Viewing, or Deleting the Rescue Configuration

If someone inadvertently commits a configuration that denies management access to a Services Router, you can delete the invalid configuration and replace it with a rescue configuration by pressing the **CONFIG** button on the router. You must have previously set the rescue configuration through the J-Web interface or the CLI. The rescue configuration is a previously committed, valid configuration.



**CAUTION:** Pressing and holding the **CONFIG** button for 15 seconds or more—until the configuration LED blinks red—deletes *all* configurations on the router, including the backup configurations and rescue configuration, and loads and commits the factory configuration.

---

You can change the default behavior of the **CONFIG** button. For more information, see “Disabling the CONFIG Button” on page 32.

To view, set, or delete the rescue configuration, select **Configuration > Rescue**. On the Rescue page, you can perform the following tasks:

- View the current rescue configuration—Click **View rescue configuration**.
- Set the current running configuration as the rescue configuration—Click **Set rescue configuration**.
- Delete the current rescue configuration—Click **Delete rescue configuration**.

## Using the CLI Configuration Editor

---

You can use the CLI configuration editor to perform the following tasks:

- Entering and Exiting Configuration Mode on page 21
- Navigating the Configuration Hierarchy on page 23
- Modifying the Configuration on page 24
- Committing a Configuration with the CLI on page 29
- Disabling the CONFIG Button on page 32
- Entering Operational Mode Commands During Configuration on page 33

### Entering and Exiting Configuration Mode

You must have access privileges to edit the configuration. For more information, see “Before You Begin” on page 6.

To enter and exit configuration mode:

1. At the CLI prompt, enter the **configure** operational mode command.

Select the form of the **configure** command (see Table 14) that is appropriate for the way you want to edit and commit the candidate configuration. For example:

```
user@host> configure
user@host#
```

2. To display the users currently editing the configuration, enter the **status** command:

```
user@host# status
Users currently editing the configuration:
  user1 terminal p1 (pid 66847) on since 2004-04-19 12:32:56 PDT
    [edit]
  user2 terminal p2 (pid 85743) on since 2004-04-19 11:44:06 PDT
    [edit interfaces]
```

For each user, the CLI displays the username, terminal, process identifier, login date and time, and hierarchy level being edited. You can specify the terminal and process identifier in the `request system logout` command.

3. To exit configuration mode and return to operational mode:

- For the top level, enter the following command:

```
user@host# exit
```

- From any level, enter the following command:

```
user@host# exit configuration-mode
```

For more information about the `configure` command, including restrictions on entering and exiting the various configuration modes, see the *JUNOS System Basics Configuration Guide*.

**Table 14: Forms of the configure Command**

Command	Edit Access	Commit Access
configure	<ul style="list-style-type: none"> <li>■ No one can lock the configuration. All users can make configuration changes.</li> <li>■ When you enter configuration mode, the CLI displays the following information: <ul style="list-style-type: none"> <li>■ A list of the other users editing the configuration.</li> <li>■ Hierarchy levels the users are viewing or editing.</li> <li>■ Whether the configuration has been changed, but not committed.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>■ No one can lock the configuration. All users can commit all changes to the candidate configuration.</li> <li>■ If you and another user make changes and the other user commits changes, your changes are committed as well.</li> </ul>
configure exclusive	<ul style="list-style-type: none"> <li>■ One user locks the configuration and makes changes without interference from other users.</li> <li>■ Other users can enter and exit configuration mode, but they cannot change the configuration.</li> <li>■ If you enter configuration mode while another user has locked the configuration, the CLI displays the user and the hierarchy level the user is viewing or editing.</li> <li>■ If you enter configuration mode while another user has locked the configuration, you can forcibly log out that user with the <code>request system logout user</code> operational mode command. (For details, see the <i>JUNOS System Basics and Services Command Reference</i>.)</li> </ul>	
configure private	<ul style="list-style-type: none"> <li>■ Multiple users can edit the configuration at the same time.</li> <li>■ Each user has a private candidate configuration to edit independently of other users.</li> </ul>	<ul style="list-style-type: none"> <li>■ When you commit the configuration, the Services Router verifies that the operational (running) configuration has not been modified by another user before accepting your private candidate configuration as the new operational configuration.</li> <li>■ If the configuration has been modified by another user, you can merge the modifications into your private candidate configuration and attempt to commit again.</li> </ul>

## Navigating the Configuration Hierarchy

When you first enter configuration mode, you are at the top level of the configuration command hierarchy, which is indicated by the `[edit]` banner. To move down through an existing configuration command hierarchy, or to create a hierarchy and move down to that level, use the `edit` command, specifying the hierarchy level at which you want to be:

```
user@host# edit <statement-path> <identifier>
```

Replace *statement-path* with the hierarchy level and *identifier* with a string that identifies an instance of a statement. (Not all statements require identifiers.) If the identifier contains a space, you must enclose the identifier in quotation marks (" ").

After you enter an `edit` command, the banner changes to indicate your current level in the hierarchy:

```
[edit]
user@host# edit protocols ospf
```

```
[edit protocols ospf]
user@host#
```

To move back up to the previous hierarchy level, enter the `exit` command. This command is, in effect, the opposite of the `edit` command. For example:

```
[edit]
user@host# edit protocols ospf
```

```
[edit protocols ospf]
user@host# edit area 0.0.0.0
```

```
[edit protocols ospf area 0.0.0.0]
user@host# exit
```

```
[edit protocols ospf]
user@host# exit
```

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

To move up one level, enter the `up` command. For example:

```
[edit]
user@host# edit protocols ospf area 0.0.0.0
```

```
[edit protocols ospf area 0.0.0.0]
user@host# up
```

```
[edit protocols ospf]
user@host# up
```

```
[edit protocols]
user@host# up
```

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

To move directly to the top level of the hierarchy, enter the **top** command. For example:

```
[edit protocols ospf area 0.0.0.0]
user@host# top
```

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

To display the configuration, enter the **show** command:

**show** <*statement-path*>

The configuration at the current hierarchy level, or at the level specified by *statement-path*, is displayed. For example, entering the **show** command in each of the following cases displays the same level of the configuration:

```
[edit]
user@host# show interfaces fe-0/0/0
unit 0 {
  family inet {
    address 192.168.4.1/30;
  }
}
```

```
[edit]
user@host# edit interfaces fe-0/0/0
[edit interfaces fe-0/0/0]
user@host# show
unit 0 {
  family inet {
    address 192.168.4.1/30;
  }
}
```

## Modifying the Configuration

You can modify the configuration by performing the following operations:

- Adding or Modifying a Statement or Identifier on page 25
- Deleting a Statement or Identifier on page 25
- Copying a Statement on page 26
- Renaming an Identifier on page 26
- Inserting an Identifier on page 27
- Deactivating a Statement or Identifier on page 28

## Adding or Modifying a Statement or Identifier

To add or modify statements in a configuration, use the **set** command:

```
set <statement-path> statement <identifier>
```

Replace *statement-path* with the path to the statement from the current hierarchy level, and *statement* with the statement itself. Replace *identifier* with a string that identifies an instance of a statement. (Not all statements require identifiers.) If the identifier contains a space, you must enclose the identifier in quotation marks (" ").

If the statement or identifier does not exist in the configuration hierarchy, it is added. If the statement or identifier already exists, it is modified (unless multiple occurrences of the same statement or identifier are allowed in the configuration, in which case another instance is added to the configuration). After you enter the **set** command, you remain at the same level in the hierarchy.

You can enter a single **set** command from the top level of the hierarchy. Alternatively, you can enter the **edit** command to move to the target hierarchy level, from which you can enter the **set** command. In either case, the CLI creates the hierarchy level if it does not exist. For example, to set the OSPF hello interval from the top level of the hierarchy, enter the **set** command as follows:

```
[edit]
user@host# set protocols ospf area 0.0.0.0 interface t1-0/0/0 hello-interval 5
```

Alternatively, use the **edit** command to create and move to the [edit protocols ospf area 0.0.0.0 interface t1-0/0/0] hierarchy level, then enter a **set** command to set the value of the hello-interval statement:

```
[edit]
user@host# edit protocols ospf area 0.0.0.0 interface t1-0/0/0
```

```
[edit protocols ospf area 0.0.0.0 interface t1-0/0/0]
user@host# set hello-interval 5
```

## Deleting a Statement or Identifier

To delete a statement or identifier from the configuration, enter the **delete** command:

```
delete <statement-path> <identifier>
```

When you delete a statement, the statement and all its subordinate statements and identifiers are removed from the configuration and revert to their default values. To delete the entire hierarchy starting at the current level, enter the **delete** command without specifying a statement or an identifier. You are prompted to confirm the deletion.

As with the **set** command, you can enter a single **delete** command from the top level of the hierarchy, or you can use the **edit** command to move to the target hierarchy level, from which you can enter the **delete** command.

## Copying a Statement

To make a copy of an existing statement in the configuration, use the **copy** command:

**copy** *existing-statement* **to** *new-statement*

The existing statement and all its subordinate statements are copied and added to the configuration. After you enter the **copy** command, the configuration might not be valid. If necessary, modify the existing statement or the new statement to ensure the configuration is valid.

The following example shows how to copy a unit configured at the [edit interfaces fe-0/0/0] hierarchy level:

```
[edit interfaces fe-0/0/0]
user@host# show
unit 0 {
  family inet {
    address 10.14.1.1/24;
  }
}

[edit interfaces fe-0/0/0]
user@host# copy unit 0 to unit 1

[edit interfaces fe-0/0/0]
user@host# show
unit 0 {
  family inet {
    address 10.14.1.1/24;
  }
}
unit 1 {
  family inet {
    address 10.14.1.1/24;
  }
}
```

In this example, after you enter the **copy** command, unit 0 and unit 1 have the same IP address in the candidate configuration. To modify the IP address of unit 1 before committing the configuration, use the **rename** command as described in “Renaming an Identifier” on page 26.

## Renaming an Identifier

There are two ways to rename an identifier that already exists in a configuration:

- Delete the identifier with the **delete** command, then add it back into the configuration with the **set** command.
- Rename the identifier with the **rename** command:

**rename** *<statement-path>* *identifier1* **to** *identifier2*



In the example provided in “Copying a Statement” on page 26, to rename the IP address of unit 1 from 10.14.1.1/24 to 10.14.2.1/24, enter the rename command as follows:

```
user@host# rename interfaces fe-0/0/0 unit 1 family inet address 10.14.1.1/24 to address 10.14.2.1/24
```

## Inserting an Identifier

To insert an identifier into a specific location within the configuration, use the insert command:

```
insert <statement-path> identifier1 (before | after) identifier2
```

Generally, you can add most identifiers into the configuration in any order. However, when you are inserting identifiers that must be analyzed in order—such as terms in a routing policy or firewall filter—you must specify **before** or **after**. If you do not specify where to insert an identifier with the insert command, the identifier is placed at the end of the list of similar identifiers.

In the following example, the firewall filter terms were added to the configuration in the following order: term1, term3, term2. The insert command is used to insert term2 before term3.

```
[edit]
user@host# show firewall
family inet {
  filter filter1 {
    term term1 {
      from {
        address {
          192.168.0.0/16;
        }
      }
      then {
        reject;
      }
    }
    term term3 {
      then {
        reject;
      }
    }
    term term2 {
      from {
        destination-port ssh;
      }
      then accept;
    }
  }
}
```

```
[edit]
user@host# insert firewall family inet filter filter1 term term2 before term term3
```

```
[edit]
user@host# show firewall
family inet {
  filter filter1 {
    term term1 {
      from {
        address {
          192.168.0.0/16;
        }
      }
      then {
        reject;
      }
    }
    term term2 {
      from {
        destination-port ssh;
      }
      then accept;
    }
    term term3 {
      then {
        reject;
      }
    }
  }
}
```

## Deactivating a Statement or Identifier

You can deactivate a statement or identifier so that it does not take effect when you enter the `commit` command. Any deactivated statements and identifiers are marked with the `inactive:` tag and remain in the configuration.

To deactivate a statement or identifier, use the `deactivate` command:

**deactivate** (*statement* | *identifier*)

To reactivate a statement or identifier, use the `reactivate` command:

**reactivate** (*statement* | *identifier*)

Reactivate removes the `inactive:` tag so that a statement or identifier takes effect when you commit the configuration.

In both commands, *statement* or *identifier* must be at the current hierarchy level.

The following example shows how to deactivate interface `fe-0/0/0` at the `[edit interfaces]` hierarchy level:

```
[edit interfaces]
user@host# deactivate fe-0/0/0
```

```
[edit interfaces]
user@host# show
inactive: fe-0/0/0 {
  unit 0 {
    family inet {
      address 10.14.1.1/24;
    }
  }
}
```

## Committing a Configuration with the CLI

To save candidate configuration changes to the configuration database and activate the configuration on the Services Router, enter the **commit** command from any hierarchy level:

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

If more than one user is modifying the configuration, committing it saves and activates the changes made by all the users.

The Services Router checks the configuration for syntax errors. If the syntax is correct, the configuration is activated and becomes the current, operational configuration running on the Services Router. If the configuration contains syntax errors, the router sends a message indicating the location of the error and does not activate the configuration. The error message has the following format:

```
[edit edit-path]
offending-statement;
error-message
```

You can specify one or more options within the **commit** command—or use it with the **rollback** command—to perform the following operations:

- Verifying a Configuration on page 29
- Committing a Configuration and Exiting Configuration Mode on page 30
- Committing a Configuration That Requires Confirmation on page 30
- Scheduling and Canceling a Commit on page 30
- Loading a Previous Configuration File with the CLI on page 31
- Setting or Deleting the Rescue Configuration with the CLI on page 32

## Verifying a Configuration

To verify that the syntax of a configuration is correct, enter the **commit check** command:

```
[edit]
user@host# commit check
configuration check succeeds
```

If the configuration contains syntax errors, a message indicates the location of the error.

## Committing a Configuration and Exiting Configuration Mode

To save candidate configuration changes, activate the configuration on the Services Router, and exit configuration mode, enter the `commit and-quit` command:

```
[edit]
user@host# commit and-quit
commit complete
exiting configuration mode
user@host>
```

If the configuration contains syntax errors, a message indicates the location of the error.

## Committing a Configuration That Requires Confirmation

You can commit the current candidate configuration but require an explicit confirmation for the committed configuration to become permanent. This commit process is useful for verifying that a configuration change works correctly and does not prevent management access to the Services Router. If the change prevents access or causes other errors, an automatic rollback to the previous configuration restores access after the rollback confirmation timeout expires.

To commit the current candidate configuration, but require an explicit confirmation for the commit to become permanent, use the `commit confirmed` command:

```
commit confirmed <minutes>
```

Replace *minutes* with the number of minutes to allow for the timeout period. The default value is 10 minutes.

To make the new configuration permanent, enter the `commit` or `commit check` command within the timeout period specified in the `commit confirmed` command. If the commit is not confirmed within the timeout period, the Services Router automatically rolls back to the previous configuration.

If the configuration contains syntax errors, a message indicates the location of the error.

## Scheduling and Canceling a Commit

To schedule a candidate configuration for a commit operation at a future time or the next time the Services Router is rebooted, use the `commit at` command:

```
commit at string
```

Replace *string* with **reboot** or the time at which the configuration is to be committed, in one of the following formats:

- *hh:mm[:ss]* —Hours, minutes, and seconds (optional), in 24-hour format. For example, 20:30 is 8:30 PM.
- *yyyy-mm-dd hh:mm[:ss]* —Year, month, date, hours, minutes, and seconds (optional), in 24-hour format. For example, 2004-09-05 08:00 is September 5, 2004 at 8:00 AM.

The Services Router checks the configuration. If the result of the check is successful, the current user is logged out of configuration mode, and the configuration data is left in a read-only state. No other commit operation can be performed until the scheduled one is completed. If the configuration contains syntax errors, a message indicates the location of the error.

To cancel a pending commit operation, use the **clear system commit** operational mode command. For more information, see the *JUNOS System Basics and Services Command Reference*.

## Loading a Previous Configuration File with the CLI

To load, or *roll back*, a previous configuration file stored on the Services Router without activating it, use the **rollback** command:

**rollback** <*string*>

Replace *string* with a value from 0 through 49, or **rescue** (if a rescue configuration exists). The default value is 0.

When you commit a configuration, the Services Router saves the current operational version and the previous 49 versions of committed configurations. The most recently committed configuration is version 0 (the current operational version), and the oldest saved configuration is version 49.

If you have defined a rescue configuration, you can roll back to this configuration by entering **rollback rescue**. (You can also roll back to the rescue configuration or the default factory configuration by pressing the **CONFIG** button on the Services Router. For more information, see the *J-series Services Router Getting Started Guide*.)

To set the rescue configuration, see “Setting or Deleting the Rescue Configuration with the CLI” on page 32.

For more information about saved versions of configuration files, see “Editing and Committing a Configuration” on page 4.

To activate the configuration you loaded, you must commit it:

```
[edit]
user@host# rollback 2
load complete
[edit]
user@host# commit
```

To display previous configurations, including the rollback number, date, time, name of the user who committed changes, and commit method, use the `rollback ?` command:

```
user@host# rollback ?
Possible completions:
<[Enter]>          Execute this command
0                  2004-05-27 14:50:05 PDT by root via junoscript
1                  2004-05-27 14:00:14 PDT by root via cli
2                  2004-05-27 13:16:19 PDT by snmpset via snmp
...
28                 2004-05-21 16:56:25 PDT by root via cli
rescue             2004-05-27 14:30:23 PDT by root via cli
|                 Pipe through a command
```

The access privilege level for using the `rollback` command is controlled by the `rollback` permission bit. Users for whom this permission bit is not set can return only to the most recently committed configuration. Users for whom this bit is set can return to any prior committed configuration. For more information, see the *JUNOS System Basics Configuration Guide*.

## Setting or Deleting the Rescue Configuration with the CLI

If someone inadvertently commits a configuration that denies management access to the Services Router, you can delete the invalid configuration and replace it with a rescue configuration by pressing the **CONFIG** button on the router. You must have previously set the rescue configuration through the J-Web interface or the CLI. The rescue configuration is a previously committed, valid configuration.



**CAUTION:** Pressing and holding the **CONFIG** button for 15 seconds or more—until the configuration LED blinks red—deletes *all* configurations on the router, including the backup configurations and rescue configuration, and loads and commits the factory configuration.

---

To set the current running configuration as the rescue configuration, use the following command:

```
user@host > request system configuration rescue save
```

To delete the current rescue configuration, use the following command:

```
user@host > request system configuration rescue delete
```

## Disabling the CONFIG Button

You can change the default behavior of the **CONFIG** button by including the `config-button` statement at the `[edit chassis]` hierarchy level:

```
config-button <no-rescue> <no-clear>
```

The `no-rescue` option prevents the CONFIG button from loading the rescue configuration. The `no-clear` option prevents the CONFIG button from deleting all configurations on the router.

To return the function of the CONFIG button to its default behavior, do not include the `config-button` statement in the router configuration.

## Entering Operational Mode Commands During Configuration

While in configuration mode, you might need to enter an operational mode command, such as `show` or `request`. To enter a single operational mode command, first enter the `run` command and then specify the operational mode command as follows:

```
user@host# run operational-mode-command
```

For example, to display a pending system reboot while in configuration mode, enter the `show system reboot` operational mode command as follows:

```
[edit]
user@host# run show system reboot
No shutdown/reboot scheduled.
```

If you are in operational mode, the `show cli history` command displays the history of the operational mode commands issued. To display the history of the configuration mode commands issued, enter the `show cli history` command from configuration mode as follows:

```
[edit]
user@host# run show cli history
15:32:51 - exit
15:52:02 - load merge terminal
17:07:57 - run show ospf statistics
17:09:12 - exit
17:18:49 - run show cli history
```

## Managing Configuration Files with the CLI

---

This section contains the following topics:

- Loading a New Configuration File on page 33
- Saving a Configuration File on page 36

### Loading a New Configuration File

You can create a configuration file, copy the file to the Services Router, and then load the file into the CLI. After you load the file, you can commit it to activate the configuration on the router, or you can edit the configuration interactively with the CLI and commit it at a later time.

You can also create a configuration while typing at the terminal and then load it. Loading a configuration from the terminal is generally useful when you are cutting existing portions of the configuration and pasting them elsewhere in the configuration.

To load an existing configuration file that is located on the router, use the following version of the **load** command:

**load (merge | override | patch | replace | update) filename <relative>**

To load a configuration from the terminal, use the following version of the **load** command:

**load (merge | override | patch | replace | update) terminal <relative>**

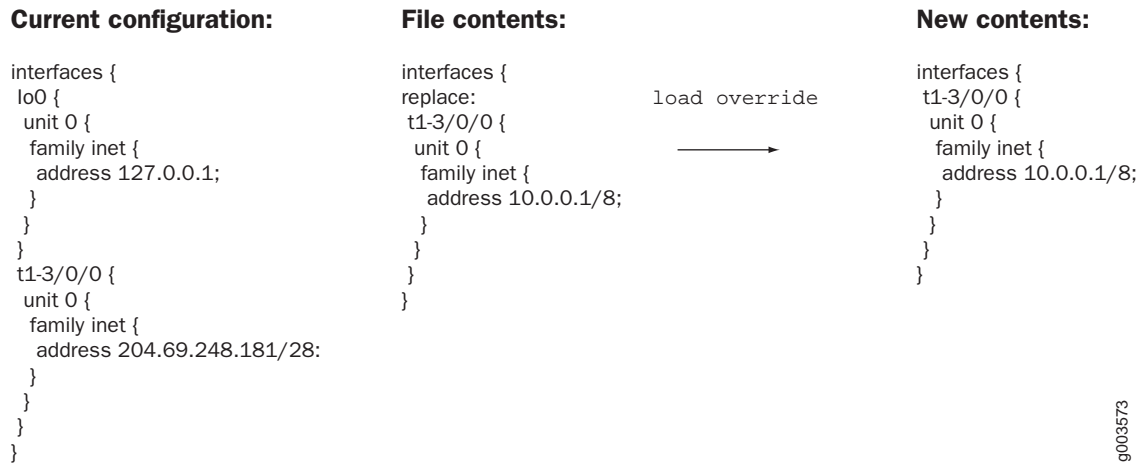
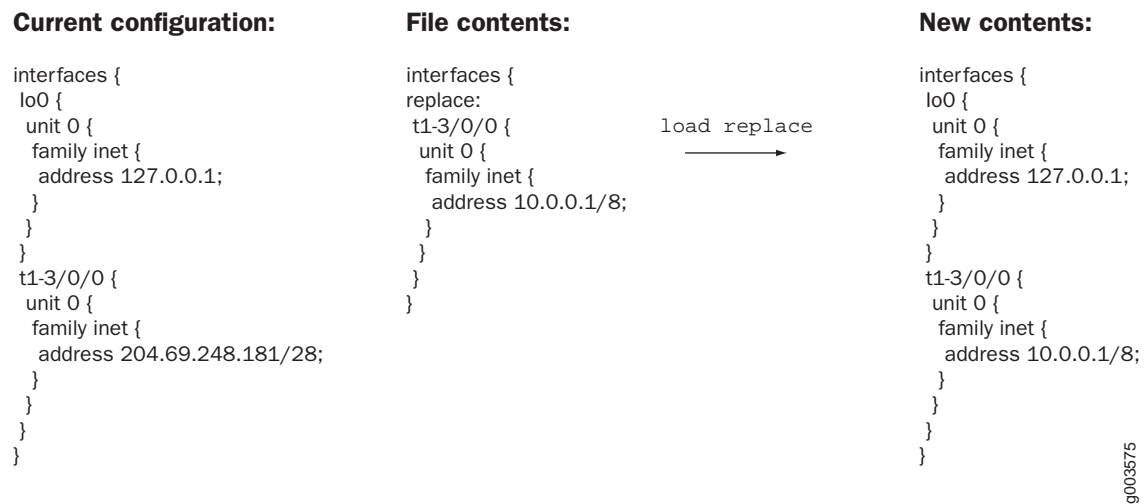
Use the load command options provided in Table 15. (The *incoming configuration* is the configuration in *filename* or the one that you type at the terminal). For more information about loading a configuration, see the *JUNOS System Basics Configuration Guide*.

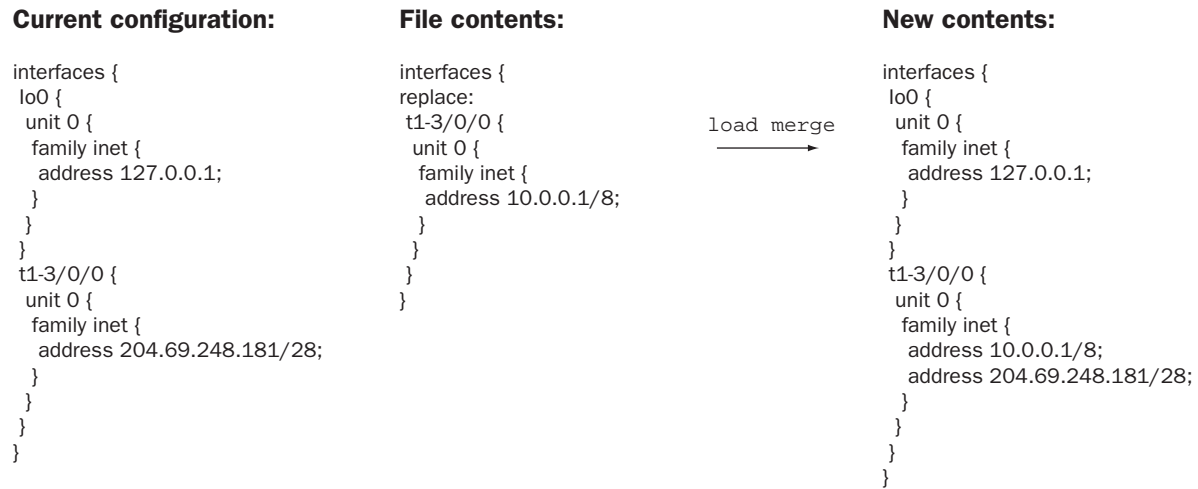
**Table 15: Load Configuration File Options**

Option	Function
merge	Combines the current configuration and the incoming configuration. A merge operation is useful when you are adding a new section to an existing configuration. If the existing configuration and the incoming configuration contain conflicting statements, the statements in the incoming configuration override those in the existing configuration.
override	Discards the current candidate configuration and loads the incoming configuration.
patch	Changes part of the configuration with the incoming configuration and marks only those parts as changed.
relative	Allows you to use the <b>merge</b> , <b>replace</b> , and <b>update</b> options without specifying the full hierarchy level.
replace	<p>Replaces portions of the configuration based on the <b>replace:</b> tags in the incoming configuration. The Services Router searches for the <b>replace:</b> tags, deletes the existing statements of the same name (if any), and replaces them with the incoming configuration. If no statement of the same name exists in the configuration, the replace operation adds it to the configuration.</p> <p>If you are performing a replace operation and the incoming configuration does not contain any <b>replace:</b> tags, the replace operation is equivalent to a merge operation. If you are running automated scripts and cannot know in advance whether the scripts need to perform a replace or a merge operation, the scripts can use the replace operation to cover either case.</p> <p>If you are performing an override or merge operation and the incoming configuration contains <b>replace:</b> tags, the tags are ignored and the override or merge operation is performed.</p>
update	Replaces only the configuration that has changed. An update operation compares the current configuration to the current candidate configuration, and loads only the changes between these configurations in the incoming configuration.

Figure 8 through Figure 10 show the results of override, replace, and merge operations.



**Figure 8: Loading a Configuration with the Override Operation****Figure 9: Loading a Configuration with the Replace Operation**

**Figure 10: Loading a Configuration with the Merge Operation**

g003574

## Saving a Configuration File

To save your current configuration to an ASCII file, including any uncommitted changes made by you and all users, issue the **save** command:

**save** *filename*

By default, the configuration is saved to a file in your home directory. For information about specifying filenames, see the *JUNOS System Basics Configuration Guide*.

## **Part 2**

# **Configuring Router Interfaces**

- Interfaces Overview on page 39
- Configuring Network Interfaces on page 99
- Configuring Digital Subscriber Line Interfaces on page 131
- Configuring Point-to-Point Protocol over Ethernet on page 165
- Configuring ISDN on page 187



## Chapter 2

# Interfaces Overview

J-series Services Routers support network interfaces for E1, E3, T1, T3, Fast Ethernet, serial, Point-to-Point Protocol over Ethernet (PPPoE), and ISDN media. In addition, the router supports a set of special interfaces for such tasks as router identification and security services. Each type of interface has particular physical and logical characteristics.

To configure and monitor Services Router 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.

This chapter contains the following topics. For more information about interfaces, see the *JUNOS Network Interfaces Configuration Guide*, the *JUNOS Services Interfaces Configuration Guide*, and the *JUNOS Interfaces Command Reference*.

- Interfaces Terms on page 40
- Network Interfaces on page 43
- Data Link Layer Overview on page 48
- Ethernet Interface Overview on page 50
- T1 and E1 Interfaces Overview on page 54
- T3 and E3 Interfaces Overview on page 58
- Serial Interface Overview on page 63
- ADSL Interface Overview on page 69
- SHDSL Interface Overview on page 72
- ISDN Interface Overview on page 72
- Interface Physical Properties on page 75
- Physical Encapsulation on an Interface on page 79
- Interface Logical Properties on page 86
- Special Interfaces on page 93

## Interfaces Terms

To understand interfaces, become familiar with the terms defined in Table 16 .

**Table 16: Network Interfaces Terms**

Term	Definition
alternate mark inversion (AMI)	Original method of formatting T1 and E1 data streams.
asymmetric digital subscriber line (ADSL) interface	Physical WAN interface for connecting a Services Router 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.
ADSL2 interface	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.
ADSL2 + interface	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.
Annex A	ITU-T Standard G.992.1 that defines how ADSL works over plain old telephone service (POTS) lines.
Annex B	ITU-T Standard G.992.1 that defines how ADSL works over Integrated Services Digital Network (ISDN) lines.
binary 8-zero substitution (B8ZS)	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.
Challenge Handshake Authentication Protocol (CHAP)	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.
checksum	See <i>frame checksum sequence</i> .
channel service unit (CSU)	Unit that connects a digital telephone line to a multiplexer or other signal service.
Cisco HDLC	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.
clock source	Source of the consistent, periodic signal used by a router to synchronize data communication and processing tasks.
CSU compatibility mode	Subrate on an E3 or T3 interface that allows a Services Router 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).
data-link connection identifier (DLCI)	Identifier for a Frame Relay virtual connection, also called a logical interface.
data service unit (DSU)	Unit that connects a data terminal equipment (DTE) device—in this case, a Services Router—to a digital telephone line.
data terminal equipment (DTE)	RS-232 interface that a Services Router uses to exchange information with a serial device.
DS1	Digital signal 1, another name for a T1 interface.

**Table 16: Network Interfaces Terms (continued)**

<b>Term</b>	<b>Definition</b>
<b>DS3 interface</b>	Digital signal 3, another name for a T3 interface.
<b>data inversion</b>	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.
<b>E1 interface</b>	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.
<b>E3 interface</b>	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.
<b>encapsulation type</b>	Type of protocol header in which data is wrapped for transmission.
<b>Fast Ethernet interface</b>	Physical LAN interface for transmitting data at 100 Mbps. Fast Ethernet, also called 100Base-T, additionally supports standard 10Base-T Ethernet transmission.
<b>FPC</b>	Logical identifier for a Physical Interface Module (PIM) installed on a Services Router. 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.
<b>frame check sequence (FCS)</b>	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.
<b>Frame Relay</b>	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.
<b>fractional E1</b>	Service also called channelized E1, in which a 2.048-Mbps E1 link is subdivided into 32 DS0 time slots (channels) in which time slot 0 is reserved. The individual channels or groups of channels connect to different destinations, and customers pay for only the channels used and not for the entire line.
<b>fractional T1</b>	Service also called channelized T1, in which a 1.544-Mbps T1 link is subdivided into 24 DS0 time slots (channels) in which time slot 0 is reserved. The individual channels or groups of channels connect to different destinations, and customers pay for only the channels used and not for the entire line.
<b>High-Level Data Link Control (HDLC)</b>	International Telecommunication Union (ITU) standard for a bit-oriented data link layer protocol on which most other bit-oriented protocols are based.
<b>hostname</b>	Name assigned to the Services Router during initial configuration.
<b>ITU-T G.991.2</b>	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.
<b>ITU-T G.992.1</b>	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.
<b>ITU-T G.994.1</b>	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.

**Table 16: Network Interfaces Terms (continued)**

<b>Term</b>	<b>Definition</b>
ITU-T G.997.1	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.
logical interface	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.
maximum transmission unit (MTU)	Maximum or largest segment size that a network can transmit.
Multilink Frame Relay (MLFR)	Protocol that allows multiple Frame Relay links to be aggregated by inverse multiplexing. MLFR is often used in conjunction with Multilink Point-to-Point Protocol (MLPPP).
Multilink Point-to-Point Protocol (MLPPP)	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.
Physical Interface Module (PIM)	<p>Network interface card that is fixed or can be interchangeably installed on a Services Router to provide the physical connections to a LAN or WAN, receiving incoming packets and transmitting outgoing packets. A PIM contains <i>one</i> of the following interfaces or sets of interfaces:</p> <ul style="list-style-type: none"> <li>■ Two Fast Ethernet LAN interfaces</li> <li>■ Two T1 or two E1 WAN interfaces</li> <li>■ Single E3 or T3 (DS3) WAN interface (J6300 model only)</li> <li>■ 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 (J4300 and J6300 models)</li> <li>■ Single ISDN S/T or U interface (J2300 model) or four ISDN S/T or U interfaces (J4300 and J6300 models)</li> <li>■ Two serial interfaces</li> <li>■ Symmetric high-speed digital subscriber line (SHDSL) WAN interface—Annex A or Annex B to support ATM-over-SHDSL connections</li> </ul>
Point-to-Point Protocol (PPP)	Link-layer protocol that provides multiprotocol encapsulation. PPP is used for link-layer and network-layer configuration.



**Table 16: Network Interfaces Terms (continued)**

Term	Definition
serial interface	<p>Physical LAN interface for transmitting data between computing devices. A Services Router has two types of serial interfaces:</p> <ul style="list-style-type: none"> <li>■ 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.</li> <li>■ 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. Services Router 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 66.</li> </ul> <p>For cable details, see the <i>J-series Services Router Getting Started Guide</i>.</p>
symmetric high-speed digital subscriber line (G.SHDSL)	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.
symmetric high-speed digital subscriber line (SHDSL) transceiver unit–remote (STU–R)	Equipment that provides symmetric high-speed digital subscriber line (SHDSL) connections to remote user terminals such as data terminals or telecommunications equipment.
T1 interface	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.
T3 interface	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.

## Network Interfaces

Services Routers 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 router. Each Services Router interface has a unique name that follows a naming convention.

This section contains the following topics:

- Media Types on page 44
- Network Interface Naming on page 44

## Media Types

Each type of interface on a Services Router uses a particular medium to transmit data. The physical wires and data link layer protocols used by a medium determine how traffic is sent. Services Routers support the following media types:

- Asynchronous Transfer Mode over asymmetric digital subscriber line (ATM-over-ADSL) interface (J4300 and J6300 models only)



**NOTE:** Services Routers with ADSL PIMs can use PPP over Ethernet (PPPoE) and PPP over ATM (PPPoA) to connect through ADSL lines only, not for direct ATM connections.

---

- Asynchronous Transfer Mode over symmetrical high-speed digital subscriber line (ATM-over-SHDSL) interface



**NOTE:** Services Routers with SHDSL PIMs can connect through SHDSL lines only, not for direct ATM connections.

---

- E1 WAN interface
- E3 WAN interface (J6300 models only)
- Fast Ethernet LAN interface
- Integrated Services Digital Network (ISDN) BRI WAN interface
- Serial interface (EIA-530, RS-449/422, RS-232, V.35, and X.21 line protocols)
- T1 WAN interface
- T3 WAN interface (also called DS3) (J6300 models only)

You must configure each network interface before it can operate on the router. 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 a Services Router 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 Services Router interface names are similar to but not identical with the interface names on the larger routing platforms.

This section contains the following topics:

- J-series Interface Naming Conventions on page 45

- Understanding CLI Output for J-series Interfaces on page 47

## J-series Interface Naming Conventions

The unique name of each Services Router 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 interface on the router has the following format, to identify the physical device that corresponds to a single physical network connector:

*type-pim /0/ port*

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

*type-pim /0/ port : channel*

- Each logical interface has an additional logical unit identifier, preceded by a period (.):

*type-pim /0/ port : < channel > . unit*

The parts of an interface name are summarized in Table 17.

**Table 17: J-series Services Router Interface Names**

<b>Name Part</b>	<b>Meaning</b>	<b>Possible Values</b>
<i>type</i>	Type of network medium that can connect to this interface.	<p>Network interface identifiers:</p> <ul style="list-style-type: none"> <li>■ <i>at</i>—ATM-over-ADSL or ATM-over-SHDSL WAN interface</li> <li>■ <i>bc</i>—Bearer channel on an ISDN BRI</li> <li>■ <i>br</i>—Basic Rate Interface for establishing ISDN connections</li> <li>■ <i>dc</i>—Delta channel on an ISDN BRI</li> <li>■ <i>dl</i>—Dialer interface for initiating ISDN connections</li> <li>■ <i>e1</i>—E1 WAN interface</li> <li>■ <i>e3</i>—E3 WAN interface</li> <li>■ <i>fe</i>—Fast Ethernet LAN interface</li> <li>■ <i>se</i>—Serial interface (either RS-232, RS-422/499, RS-530, V.35, or X.21)</li> <li>■ <i>t1</i>—T1 (also called DS1) WAN interface</li> <li>■ <i>t3</i>—T3 (also called DS3) WAN interface</li> </ul> <p>Special interface identifiers: (See “Special Interfaces” on page 93.)</p> <ul style="list-style-type: none"> <li>■ <i>dsc</i></li> <li>■ <i>gr, gre</i></li> <li>■ <i>ip, ipip</i></li> <li>■ <i>lo</i></li> <li>■ <i>ls</i></li> <li>■ <i>lsi</i></li> <li>■ <i>mtun</i></li> <li>■ <i>pd, pimd</i></li> <li>■ <i>pe, pime</i></li> <li>■ <i>sp</i></li> <li>■ <i>tap</i></li> </ul>
<i>pim</i>	Number of the chassis slot in which a PIM is installed.	<ul style="list-style-type: none"> <li>■ On a J2300 router, always 0.</li> <li>■ On a J4300 or J6300 router, this number begins at 1 and increases from left to right, bottom to top to a maximum of 6.</li> </ul> <p>The PIM number 0 is reserved for the out-of-band management ports. (See “Management Interface” on page 96.)</p>
0	Number of the PIM installed in a chassis slot.	<p>Always 0.</p> <p>Only one PIM can be installed in a slot.</p>

**Table 17: J-series Services Router Interface Names (continued)**

Name Part	Meaning	Possible Values
<i>port</i>	Number of the port on a PIM on which the physical interface is located.	<ul style="list-style-type: none"> <li>■ On a single-port PIM, always 0.</li> <li>■ On a multiple-port PIM, this number begins at 0 and increases from left to right, bottom to top, to a maximum of 3.</li> </ul>
Port numbers appear on the PIM faceplate.		
<i>channel</i>	Number of the channel (time slot) on a fractional T1 or E1 interface.	<ul style="list-style-type: none"> <li>■ On an E1 interface, a value from 0 through 32. The 0 and 1 time slots are reserved.</li> <li>■ On a T1 interface, a value from 0 through 24. The 0 time slot is reserved.</li> </ul>
<i>unit</i>	Number of the logical interface created on a physical interface.	<p>A value from 0 through 16384.</p> <p>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 86.</p>

For example, the interface name `e1-5/0/0:15.0` 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 J-series Interfaces

The JUNOS Internet software that operates J-series Services Routers was originally developed for Juniper Networks M-series and T-series routing platforms that support many ports, on interface cards called Physical Interface Cards (PICs). On these larger platforms, PICs are installed into slots on FPCs, and FPCs are installed into slots in the router chassis.

Because Services Routers have the same hardware and software architectures as the M-series and T-series routing platforms, PIM slots are detected internally by the JUNOS software as FPC slots, and the PIM 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:
Item          Version  Part number  Serial number  Description
Chassis              REV 02.04  710-010001  JN000192AB    J4300
Midplane

```

System IO	REV 02.03	710-010003	CORE100885	System IO board
Routing Engine	RevX2.6	750-010005	IWGS40735451	RE-J.2
FPC 0				FPC
PIC 0				2x FE
FPC 2	RevX2.1	750-010355	CORE100458	FPC
PIC 0				2x T1
FPC 5	REV 04	750-010353	AF04451744	FPC
PIC 0				2x FE

## 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 Services Routers.

### **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 router, 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 Services Routers 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 50
- Collisions and Detection on page 51
- Collision Domains and LAN Segments on page 52
- Broadcast Domains on page 53
- Ethernet Frames on page 53

### ***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 18 shows collision rounds up to round 10.

**Table 18: Collision Backoff Algorithm Rounds**

Round	Size of Set	Elements in the Set
1	2	{0,1}
2	4	{0,1,2,3}
3	8	{0,1,2,3,...,7}
4	16	{0,1,2,3,4,...,15}
5	32	{0,1,2,3,4,5,...,31}
6	64	{0,1,2,3,4,5,6,...,63}
7	128	{0,1,2,3,4,5,6,7,...,127}
8	256	{0,1,2,3,4,5,6,7,8,...,255}

**Table 18: Collision Backoff Algorithm Rounds (continued)**

Round	Size of Set	Elements in the Set
9	512	{0,1,2,3,4,5,6,7,8,9,...,511}
10	1024	{0,1,2,3,4,5,6,7,8,9,10,...,1023}

## 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.

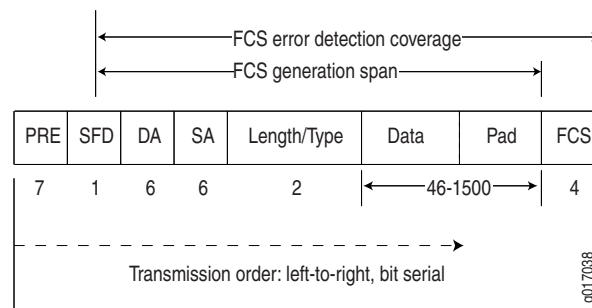
## Broadcast Domains

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 11 shows the Ethernet frame format.

**Figure 11: 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 54
- E1 Overview on page 55
- T1 and E1 Signals on page 55
- Encoding on page 55
- T1 and E1 Framing on page 56
- T1 and E1 Loopback Signals on page 57

### 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 ( $8,000 \times 193 = 1.544$  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:

Chan. 1	Chan. 2	Chan. 3	Chan. 4
---------	---------	---------	---------

```

Frame 1  [10001100][00110001][11111000][10101010]
Frame 2  [11100101][01110110][10001000][11001010]
Frame 3  [00010100][00101111][11000001][00000001]

```

## 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 55.

## 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

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]
[xxxxxxxx][1]
[xxxxxxxx][0]
[xxxxxxxx][0]
[xxxxxxxx][0]
[xxxxxxxx][1]
[xxxxxxxx][1]
[xxxxxxxx][0]
[xxxxxxxx][1]
[xxxxxxxx][1]
[xxxxxxxx][1]
[xxxxxxxx][1]
[xxxxxxxx][1]
```

```
[xxxxxxxx][0]
[xxxxxxxx][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:

```
....100001000010000100...
```

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

```
....100100100100100100....
```

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

## 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.

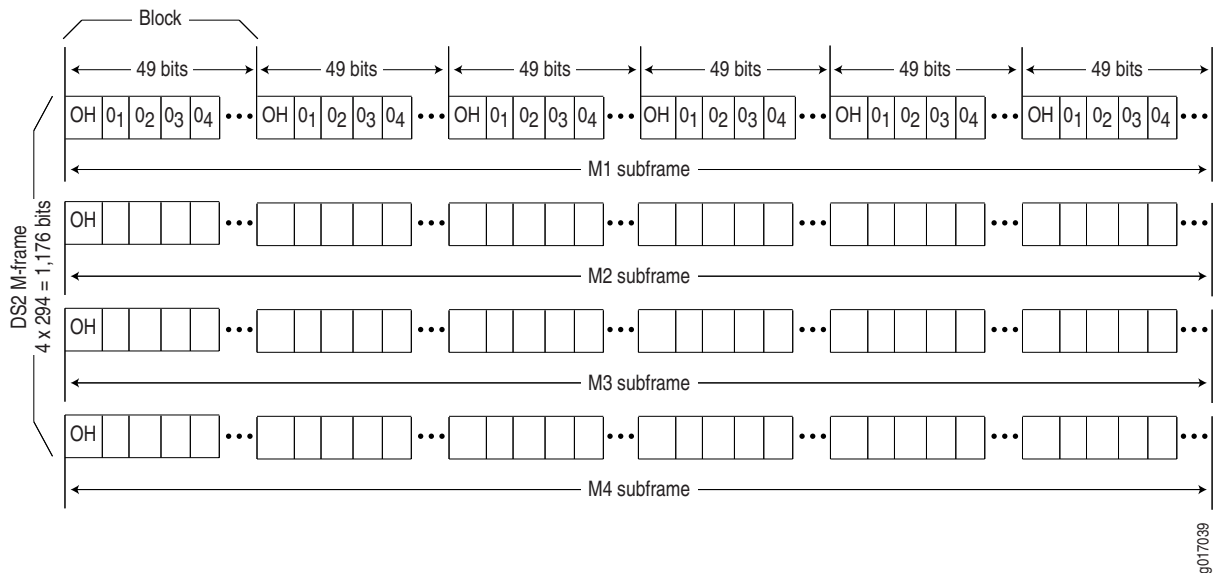
E3 is the equivalent European transmission format. E3 links are similar to T3 (DS3) links, but carry signals at 34.368 Mbps. Each signal has 16 E1 channels, and each channel transmits at 2.048 Mbps. E3 links use all 8 bits of a channel, whereas T3 links use 1 bit in each channel for overhead.

### 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 12 shows the DS2 M-frame format.

**Figure 12: 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  $0_n$  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.

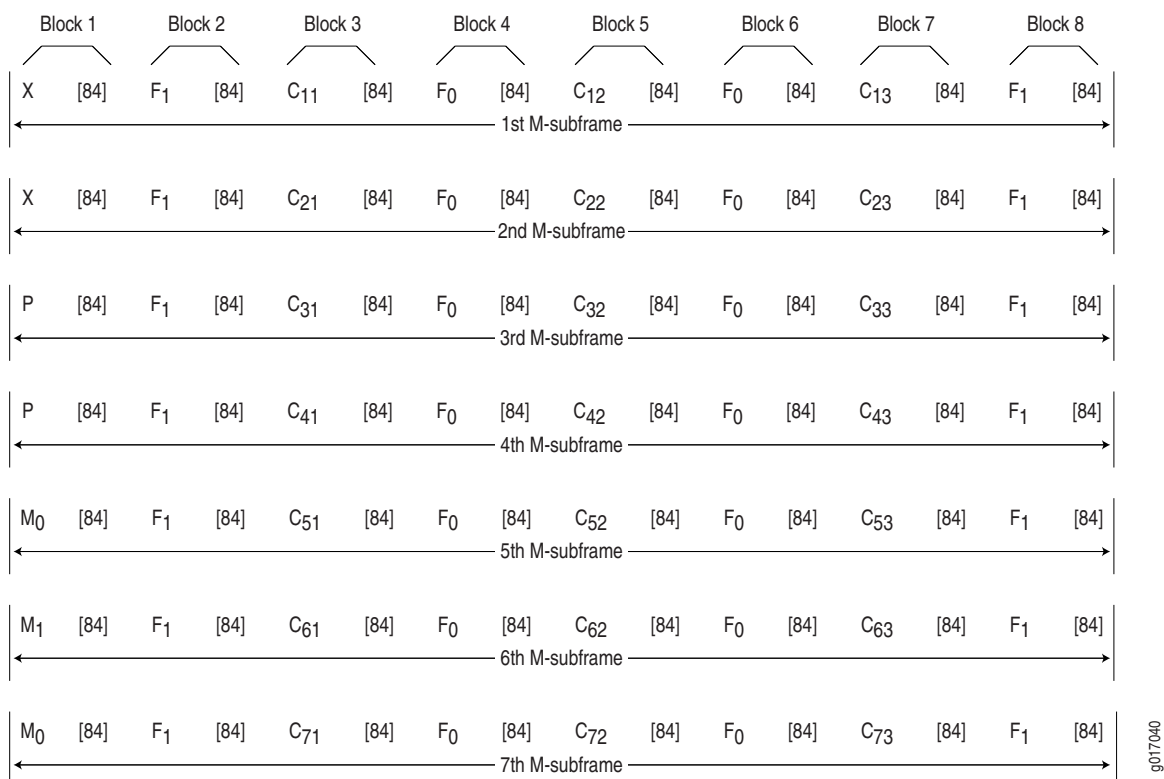
A DS2 connection requires a nominal transmit rate of 6.304 Mbps. However, because multiplexers increase the overall output rate to the intermediate rate of 6.312 Mbps, the output rate is higher than individual input rates on DS1 signals. The extra bandwidth is used to stuff the incoming DS1 signals with 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 13 and Figure 14.

#### **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 13.

**Figure 13: DS3 M13 Frame Format**

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.
- Multiframe 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<sub>11</sub>, C<sub>12</sub>, and C<sub>13</sub> 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.

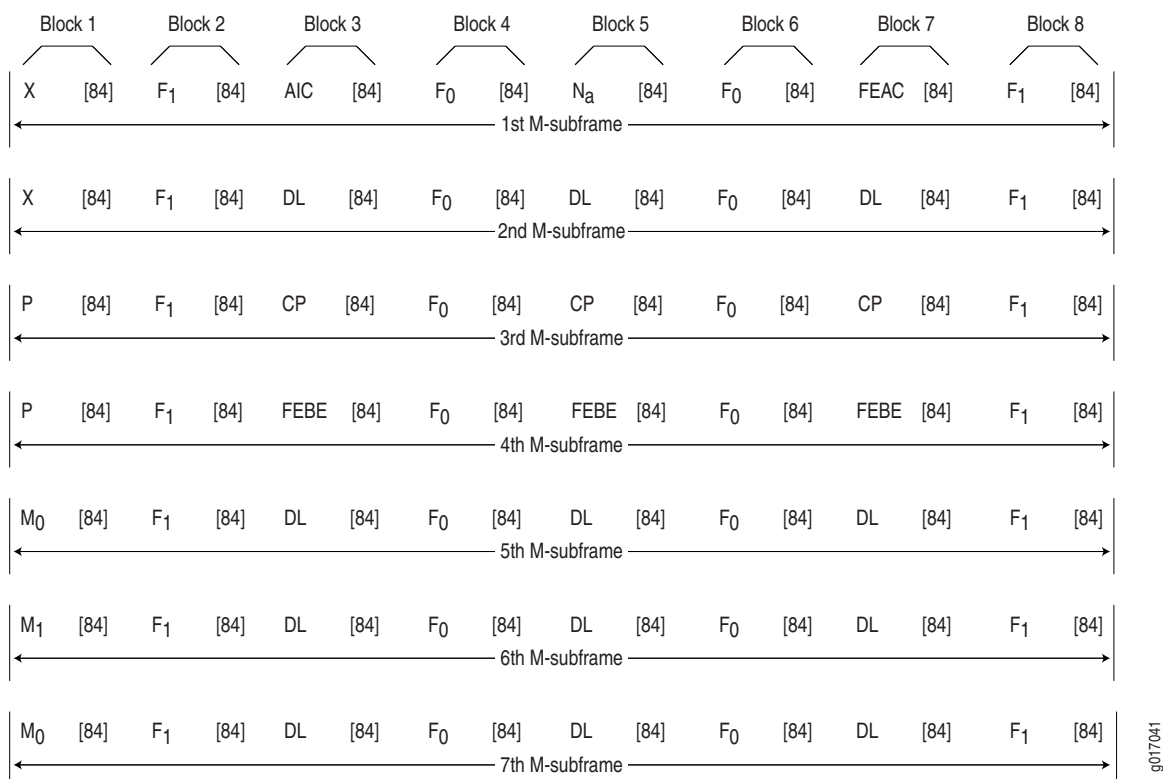
- Parity bits (P-bits)—Compute parity over all but 1 bit of the M-frame. (The first X-bit is not included.) Each DS3 frame contains 2 P-bits, which are located at the beginning of subframes 3 and 4. Both P-bits must be identical.

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 14.

**Figure 14: DS3 C-Bit Parity Framing**

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<sub>a</sub>—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 0xxxxxx 1111111, in which x can be either 1 or 0. Bits are transmitted from right to left.

Table 19 lists some C-bit code words and the alarm or status condition indicated.

**Table 19: FEAC C-Bit Condition Indicators**

<b>Alarm or Status Condition</b>	<b>C-Bit Code Word</b>
DS3 equipment failure requires immediate attention.	00110010 11111111
DS3 equipment failure occurred—such as suspended, not activated, or unavailable service—that is non-service-affecting.	00011110 11111111
DS3 loss of signal.	00011100 11111111
DS3 out of frame.	00000000 11111111
DS3 alarm indication signal (AIS) received.	00101100 11111111
DS3 idle received.	00110100 11111111
Common equipment failure occurred that is non-service-affecting.	00011101 11111111
Multiple DS1 loss of signal.	00101010 11111111
DS1 equipment failure occurred that requires immediate attention.	00001010 11111111
DS1 equipment failure occurred that is non-service-affecting.	00000110 11111111
Single DS1 loss of signal.	00111100 11111111

- 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 20 lists and defines serial signals and their sources.

**Table 20: Serial Transmission Signals**

Signal Name	Definition	Signal Source
TD	Transmitted data	DTE
RD	Received data	DCE
RTS	Request to send	DTE
CTS	Clear to send	DCE
DSR	Data set ready	DCE
Signal Ground	Grounding signal	–
CD	Carrier detect	–
DTR	Data terminal ready	DTE
RI	Ring indicator	–

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.

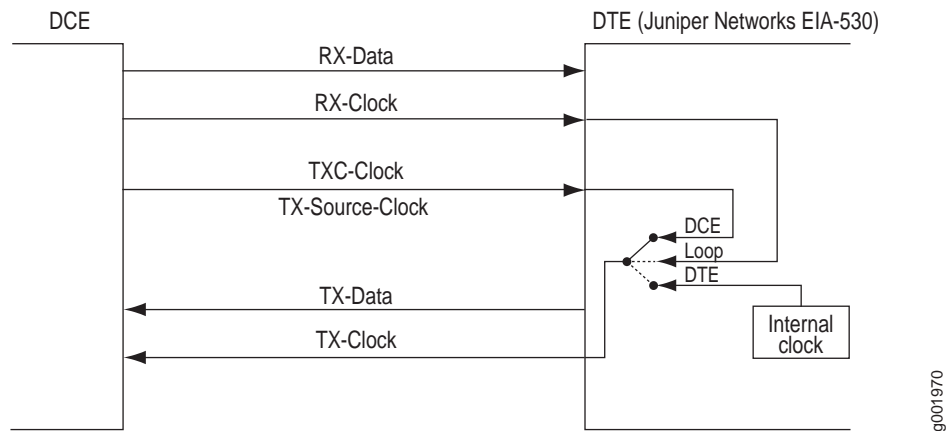
## Serial Clocking Modes

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.
- DTE clocking mode—Uses an internally generated clock. The speed of this clock is configured locally. DTE clocking mode is also known as line timing.

Both loop clocking mode and DCE clocking mode use external clocks generated by the DCE.

Figure 15 shows the clock sources for loop, DCE, and DTE clocking modes.

**Figure 15: 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 67



- RS-232 on page 67
- RS-422/449 on page 68
- V.35 on page 68
- X.21 on page 69

## 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  $-12\text{V}$  and  $+12\text{V}$ . Within this range, voltages between  $-3\text{V}$  and  $+3\text{V}$  are considered inoperative and are used to absorb line noise. Control signals are considered operative when the voltage ranges from  $+3$  to  $+25\text{V}$ .

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).

## 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. A typical ADSL circuit uses bandwidths of 1.5 Mbps to 2.0 Mbps downstream and 16 Kbps upstream. Depending on the length of the copper wire, an ADSL link can have up to 6.1 Mbps downstream and 64 Kbps upstream.

J4300 and J6300 Services Routers support ADSL, ADSL2, and ADSL2 + , which comply with the following standards:

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



**NOTE:** Services Routers with ADSL PIMs can use PPP over Ethernet (PPPoE) and PPP over ATM (PPPoA) to connect through ADSL lines only, not for direct ATM connections.

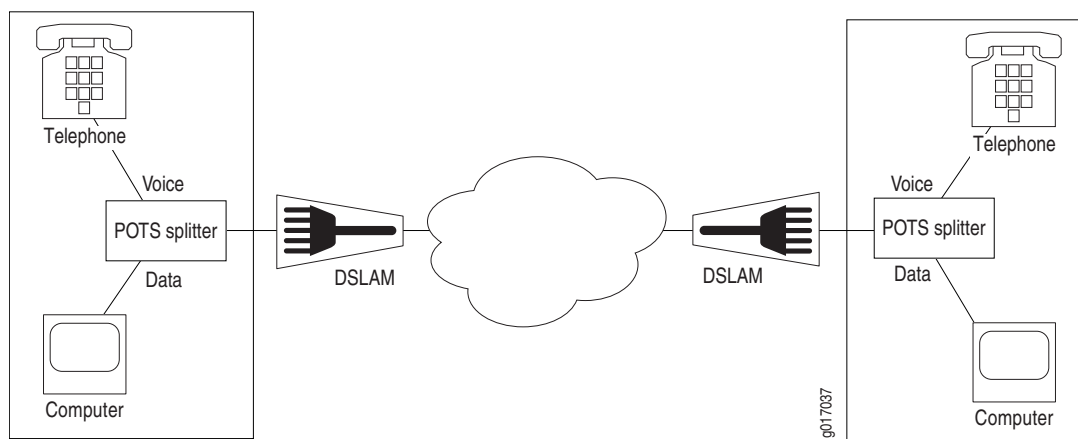
---

## 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 16.

**Figure 16: Typical ADSL Topology****ADSL2 and ADSL2+**

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).

First-generation ADSL standards require fixed 32-bit overhead framing on all ADSL packets. On long lines with low rates of 128 Kbps, the overhead represents 25 percent of the available bandwidth. ADSL2 standards allow the overhead per frame to be a programmable value between 4 Kbps and 32 Kbps, to provide up to 28 Kbps more bandwidth for payload data.

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 multicarrier 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.

**Asynchronous Transfer Mode**

On a J-series Services Router, the ADSL link is employed over an Asynchronous Transfer Mode (ATM)-over-ADSL interface. Although the interface type is *at*, the physical interface is ADSL. ATM-over-ADSL and ATM-over-SHDSL interfaces can be configured with the properties associated with traditional ATM interfaces, including virtual circuit and path information and ATM encapsulation.

## SHDSL Interface Overview

---

SHDSL interfaces on J-series Service Routers 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.

## 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

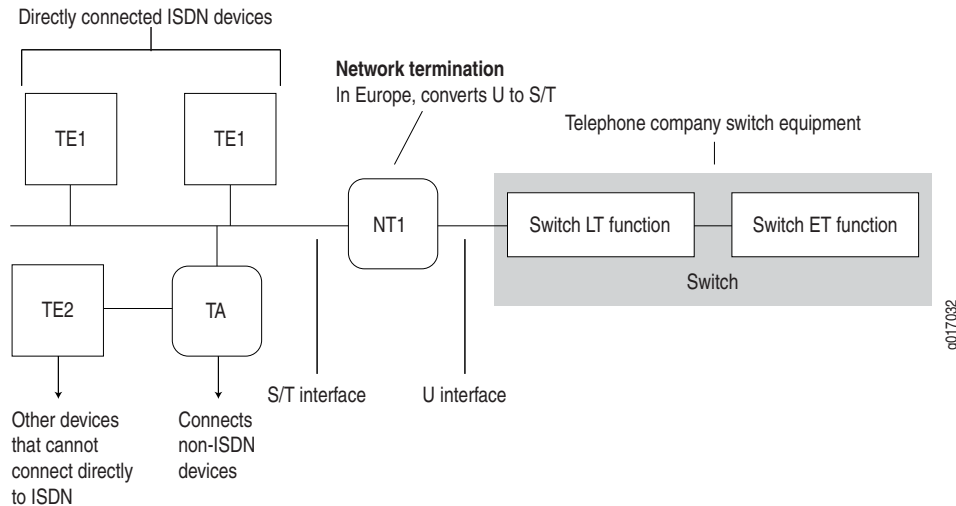
ISDN provides two basic types of service, Basic Rate Interface (BRI) and Primary Rate Interface (PRI). Services Routers support ISDN BRI only.

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.

## Typical ISDN Network

Figure 17 shows a typical ISDN network.

**Figure 17: ISDN Network**



In Figure 17, 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 17. 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 21 summarizes some key physical properties of J-series Services Router interfaces.

**Table 21: Interface Physical Properties**

Physical Property	Description
bert-error-rate	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 76.
bert-period	Bit error rate test (BERT) time period over which bit errors are sampled. See “Bit Error Rate Testing” on page 76.
chap	Challenge Handshake Authentication Protocol (CHAP). Specifying <b>chap</b> enables CHAP authentication on the interface. See “CHAP Authentication” on page 82.
clocking	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 76.
description	A user-defined text description of the interface, often used to describe the interface’s purpose.
disable	Administratively disables the interface.

**Table 21: Interface Physical Properties (continued)**

Physical Property	Description
encapsulation	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 79.
fcs	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 78.
mtu	Maximum transmission unit (MTU) size. The MTU is the largest size packet or frame, specified in 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.
no-keepalives	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.
payload-scrambler	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.

## 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 Services Router 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 router 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, Services Routers generate their own clock signals to send and receive traffic.

The system clock allows the router to sample (or detect) and transmit data being received and transmitted through its interfaces. Clocking enables the router 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	1	0	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.

## 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 J-series Services Router physical interfaces:

- Frame Relay on page 79
- Point-to-Point Protocol on page 81
- Point-to-Point Protocol over Ethernet on page 83
- High-Level Data Link Control on page 85

### 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 18 shows a typical Frame Relay network.

**Figure 18: Frame Relay Network**

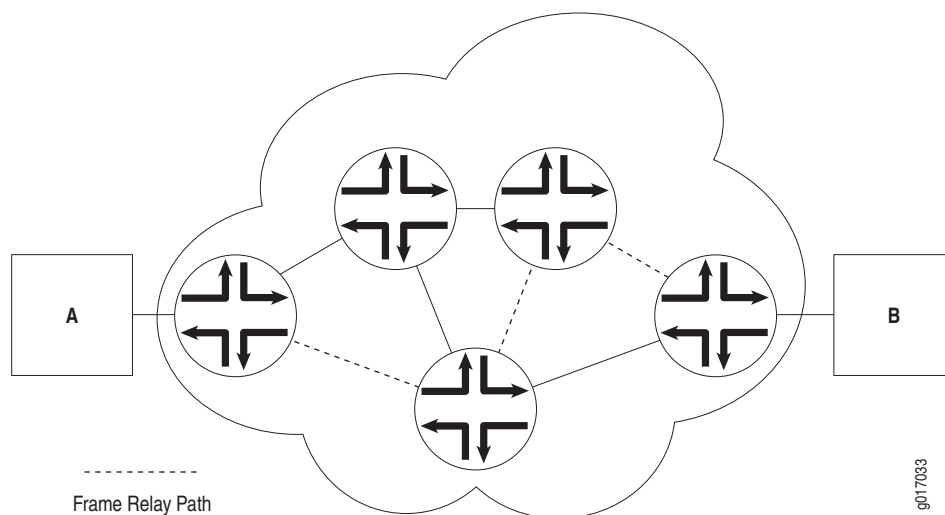


Figure 18 shows multiple paths from host A to host B. In a typical routed network, traffic is sent from device to device with each device making routing decisions based on its own routing table. In a packet-switched network, the

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 routers can switch packets to the appropriate next-hop address in the circuit. Multiple paths that pass through the same transit routers 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 router. When the queues reach a predefined level of saturation, traffic is determined to be congested. When traffic congestion occurs in a virtual circuit, the router 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.

## CHAP 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.

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.

## 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 Services Routers.

- 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 Services Router) 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. Routers must have a unique IP address for every interface.

This section contains the following topics:

- Protocol Families on page 86
- IPv4 Addressing on page 87
- IPv6 Addressing on page 90
- Virtual LANs on page 92

### 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).

## 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 router's packet forwarding components. The JUNOS software automatically configures this protocol family on the router's internal interfaces only.
- vpls—Virtual private LAN service (VPLS).

## 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 (Web servers, for example) must have a globally unique IP address. Devices that are visible only within the network (routers, 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 19 shows two subnets in a network.

**Figure 19: Subnets in a Network**

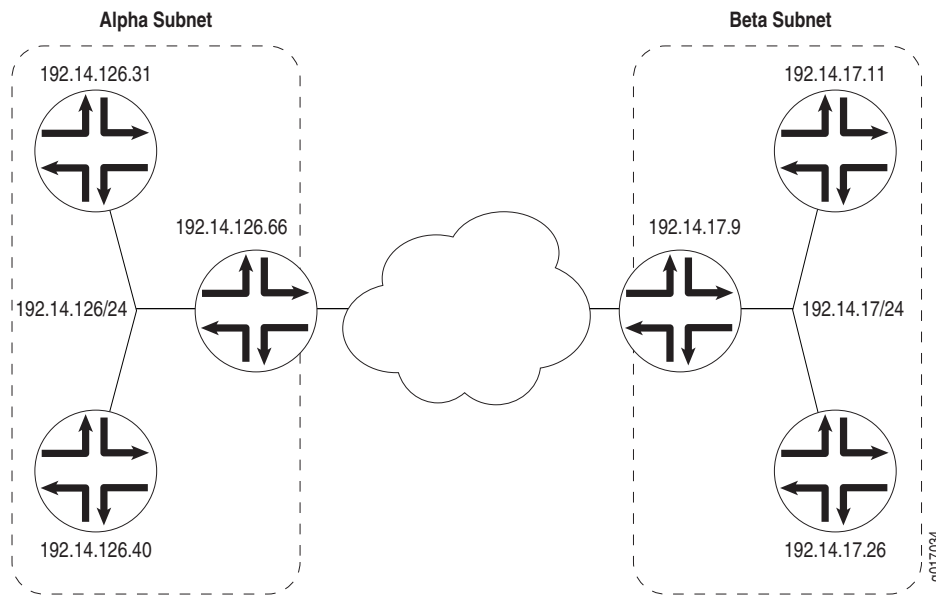


Figure 19 shows three devices connected to one subnet and three more devices connected to a second subnet. Collectively, the six devices and two subnets make up the larger network. In this example, the network is assigned the network prefix **192.14.0.0**, a class B address. Each device has an IP address 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 . xxxxxxxx
```

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

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

```
aaaa:aaaa:aaaa:aaaa:aaaa:aaaa:aaaa:aaaa
```

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:0:0:1:200: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
```

## 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 feature called address scoping that 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 | flgs | scop | 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.

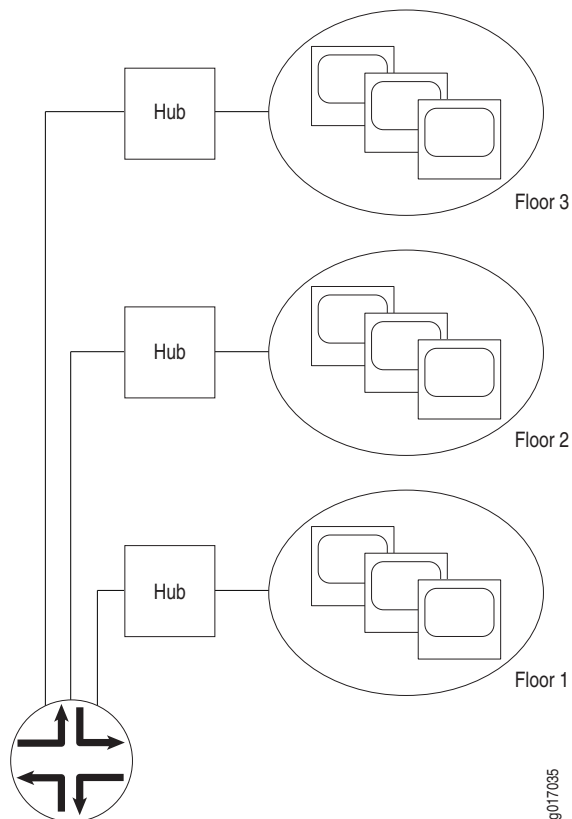
Similar to multicast addresses, anycast addresses identify a set of interfaces. However, packets are sent to only one of the interfaces, not to all interfaces. Anycast addresses are allocated from the normal unicast address space and cannot be distinguished from a unicast address in format. Therefore,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

## 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 20 shows a typical LAN topology.

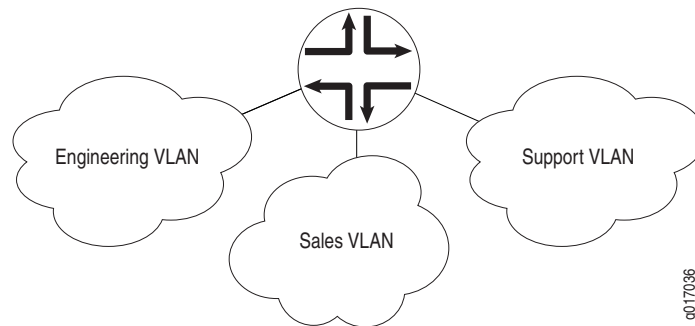
### Figure 20: Typical LAN



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 21 shows a typical VLAN topology.

**Figure 21: Typical VLAN**



## Special Interfaces

In addition to the configured network interfaces associated with the physical ports and wires that make up much of the network, J-series Services Routers have special interfaces. Table 22 lists each special interface and briefly describes its use.

**Table 22: Special Interfaces on a Services Router**

Interface Name	Description
dsc	Discard interface. See “Discard Interface” on page 95.
fxp0	This interface is not supported on a J-series Services Router. (On an M-series or T-series router, <code>fxp0</code> is used for out-of-band management.) For more information about the J-series Services Router management port interface, see “Management Interface” on page 96.
gr-0/0/0	Configurable generic routing encapsulation (GRE) interface. GRE allows the encapsulation of one routing protocol over another routing protocol.  Within a Services Router, 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.
gre	Internally generated GRE interface. This interface is generated by the JUNOS software to handle GRE. It is not a configurable interface.

**Table 22: Special Interfaces on a Services Router (continued)**

Interface Name	Description
ip-0/0/0	<p>Configurable IP-over-IP encapsulation (also called IP tunneling) interface. IP tunneling allows the encapsulation of one IP packet over another IP packet.</p> <p>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.</p> <p>Within a Services Router, 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.</p>
ipip	Internally generated IP-over-IP interface. This interface is generated by the JUNOS software to handle IP-over-IP encapsulation. It is not a configurable interface.
lo0	Loopback address. The loopback address has several uses, depending on the particular JUNOS feature being configured. See "Loopback Interface" on page 96.
lo0.16385	Internal loopback address. The internal loopback address is a particular instance of the loopback address with the logical unit number 16385. It is created by the JUNOS software as the loopback interface for the internal routing instance. This interface prevents any filter on lo0.0 from disrupting internal traffic.
ls-0/0/0	<p>Configurable link services interface. Link services include the multilink services MLPPP, MLFR, and Compressed Real-Time Transport Protocol (CRTP).</p> <p>Within a Services Router, 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.</p> <p>For more information about multilink services, see "Services Interfaces" on page 97.</p>
lsi	Internally generated link services interface. This interface is generated by the JUNOS software to handle multilink services like MLPPP, MLFR, and CRTP. It is not a configurable interface.
lt-0/0/0	<p>Configurable logical tunnel interface. The tunnel interface is used to provide services such as Layer 3 MPLS VPNs over GRE, IPsec over GRE, GRE over IPsec, PIM sparse mode multicast, multicast over Layer 3 VPNs, virtual private LAN service (VPLS), VPLS or Layer 2 VPNs terminated into Layer 3 VPNs, IPv6-over-IPv4 encapsulation, and logical routers.</p> <p>Within a Services Router, packets are routed to this internal interface for tunnel services. The logical tunnel 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 tunnel services.</p>
mt-0/0/0	<p>Configurable multicast tunnel interface. Multicast tunnels filter all unicast packets; if an incoming packet is not destined for a 224/8-or-greater prefix, the packet is dropped and a counter is incremented.</p> <p>Within a Services Router, packets are routed to this internal interface for multicast filtering. The multicast tunnel 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 multicast tunneling.</p>
mtun	Internally generated multicast tunnel interface. This interface is generated by the JUNOS software to handle multicast tunnel services. It is not a configurable interface.

**Table 22: Special Interfaces on a Services Router (continued)**

Interface Name	Description
pd-0/0/0	<p>Configurable Protocol Independent Multicast (PIM) de-encapsulation interface. In PIM sparse mode, the first-hop routing platform encapsulates packets destined for the rendezvous point router. 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.</p> <p>Within a Services Router, 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 medium or Physical Interface Module (PIM). You must configure the interface for it to perform PIM de-encapsulation.</p>
pe-0/0/0	<p>Configurable Protocol Independent Multicast (PIM) encapsulation interface. In PIM sparse mode, the first-hop routing platform encapsulates packets destined for the rendezvous point router. 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.</p> <p>Within a Services Router, 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 medium or Physical Interface Module (PIM). You must configure the interface for it to perform PIM encapsulation.</p>
pimd	Internally generated Protocol Independent Multicast (PIM) de-encapsulation interface. This interface is generated by the JUNOS software to handle PIM de-encapsulation. It is not a configurable interface.
pime	Internally generated Protocol Independent Multicast (PIM) encapsulation interface. This interface is generated by the JUNOS software to handle PIM encapsulation. It is not a configurable interface.
pp0	<p>Configurable PPPoE encapsulation interface. PPP packets being routed in an Ethernet network use PPPoE encapsulation.</p> <p>Within a Services Router, 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 165.</p>
sp-0/0/0	<p>Configurable services interface. The services interface is used to enable a number of routing services such as stateful firewall filters, IPSec, and Network Address Translation (NAT).</p> <p>Within a Services Router, packets are routed to this internal interface for encapsulation or processing, depending on the services configured. The configurable 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 enable service sets.</p>
tap	Internally generated interface. This interface is generated by the 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.

## 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:

- Router identification—The loopback interface is used to identify the router. While any interface address can be used to determine if the router 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 router. 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 router is online provides a misleading result. An interface might be unavailable because of a problem unrelated to the router's configuration or operation.

- Routing information—The loopback address is used by protocols such as OSPF to determine protocol-specific properties for the router 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

The management interface (also called the out-of-band management interface) on a J-series Services Router can either be `fe-0/0/0` or `fe-0/0/1`. The management interface is a Fast Ethernet interface with a permanent port on the front of the router chassis.

The management interface is the primary interface for accessing the router remotely. Typically, the management interface is not connected to the in-band network, but is connected instead to the router's internal network. Through the management interface you can access the router over the network and configure it from anywhere, regardless of its physical location.

As a security feature, users cannot log in as *root* through the management interface. To access the router 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 Services Router, these same features are implemented by the general-purpose CPU on the main circuit board.

Although the same JUNOS Internet software image supports the services features across all routing platforms, on a Services Router no Physical Interface Module (PIM) is associated with services features.

To configure services on a Services Router, you must configure one or more internal interfaces by specifying PIM slot 0 and port 0—for example, `sp-0/0/0` for stateful firewall filters and NAT or `gr-0/0/0` for GRE.

Services Routers support multilink protocol services on the `ls-0/0/0` interface. At the logical level, the `ls-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).

### 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

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 `ls-0/0/0` interface.

MLFR FRF.16 is supported on the `ls-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.

### 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 Services Router, CRTP can operate on a T1 or E1 interface with PPP encapsulation.



## Chapter 3

# Configuring Network Interfaces

Each Services Router can support types of interfaces that perform different functions. The router uses network 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.

This chapter includes the following topics. For more information about interfaces, see “Interfaces Overview” on page 39 and the *JUNOS Network Interfaces Configuration Guide*. To configure DSL interfaces, see “Configuring Digital Subscriber Line Interfaces” on page 131. To configure PPPoE interfaces, see “Configuring Point-to-Point Protocol over Ethernet” on page 165. To configure ISDN interfaces, see “Configuring ISDN” on page 187.

- Before You Begin on page 99
- Configuring Network Interfaces with Quick Configuration on page 100
- Configuring Network Interfaces with a Configuration Editor on page 122
- Verifying Interface Configuration on page 127

### Before You Begin

---

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

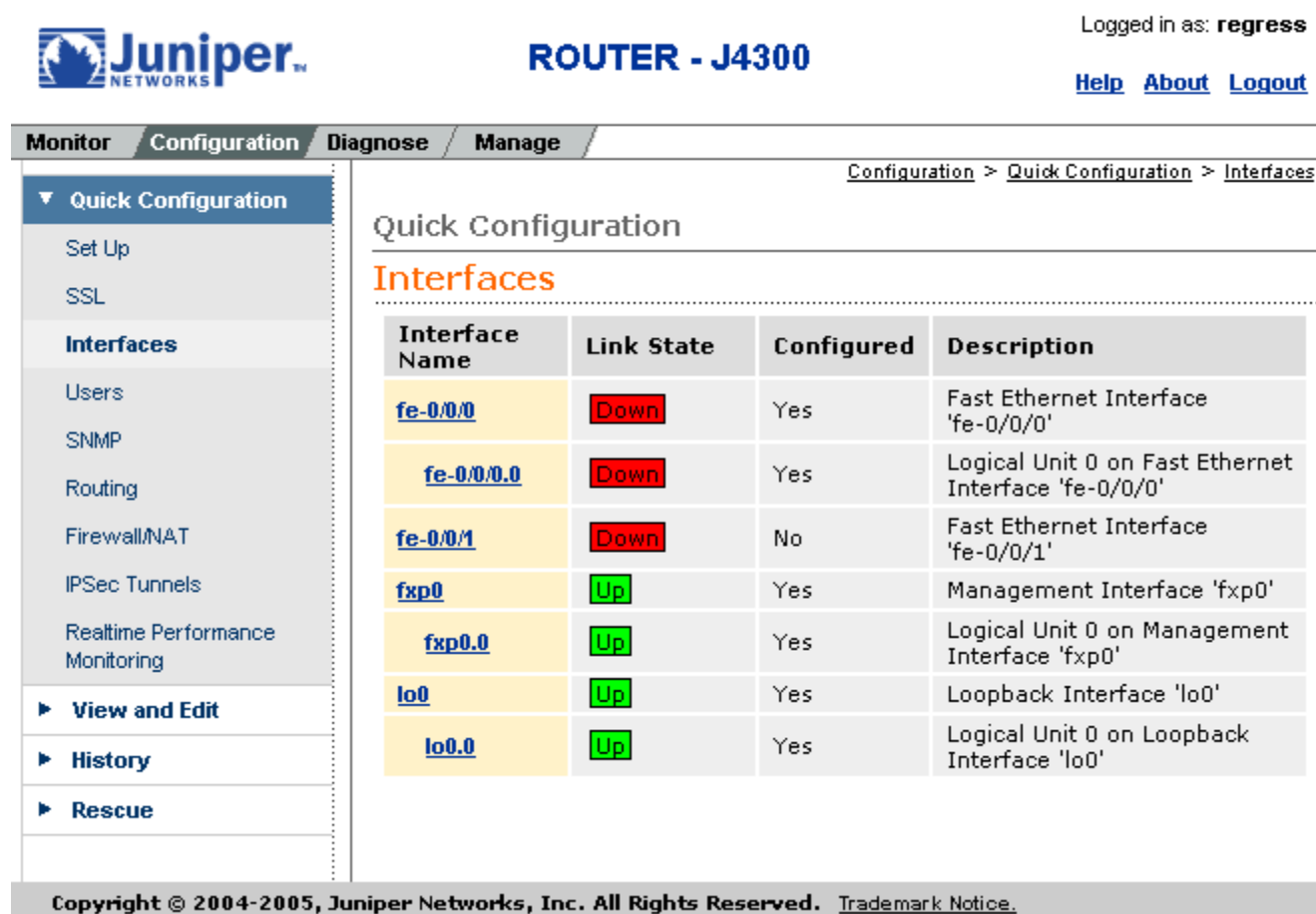
- Install Services Router hardware. For more information, see the *J-series Services Router Getting Started Guide*.
- Establish basic connectivity. For more information, see the *J-series Services Router Getting Started Guide*.
- If you do not already have a basic understanding of physical and logical interfaces and Juniper Networks interface conventions, read “Interfaces Overview” on page 39.

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 J-series Services Router by displaying the Quick Configuration page, as shown in Figure 22.

## Configuring Network Interfaces with Quick Configuration

The Quick Configuration page allows you to configure network interfaces on a Services Router, as shown in Figure 22.

**Figure 22: Quick Configuration Interfaces Page**



Juniper NETWORKS ROUTER - J4300

Logged in as: regress

[Help](#) [About](#) [Logout](#)

Monitor Configuration Diagnose Manage

Configuration > Quick Configuration > Interfaces

**Quick Configuration**

**Interfaces**

Interface Name	Link State	Configured	Description
<a href="#">fe-0/0/0</a>	Down	Yes	Fast Ethernet Interface 'fe-0/0/0'
<a href="#">fe-0/0/0.0</a>	Down	Yes	Logical Unit 0 on Fast Ethernet Interface 'fe-0/0/0'
<a href="#">fe-0/0/1</a>	Down	No	Fast Ethernet Interface 'fe-0/0/1'
<a href="#">fxp0</a>	Up	Yes	Management Interface 'fxp0'
<a href="#">fxp0.0</a>	Up	Yes	Logical Unit 0 on Management Interface 'fxp0'
<a href="#">lo0</a>	Up	Yes	Loopback Interface 'lo0'
<a href="#">lo0.0</a>	Up	Yes	Logical Unit 0 on Loopback Interface 'lo0'

Copyright © 2004-2005, Juniper Networks, Inc. All Rights Reserved. Trademark Notice.

To configure a network interface with Quick Configuration:

1. In the J-Web user interface, select **Configuration > Quick Configuration > Interfaces**. You can select **Interfaces** in the list under Router Configuration or from the left pane.

A list of the network interfaces present on the Services Router is displayed, as shown in Figure 22. The third column indicates whether the interface has been configured.

2. To configure properties for a network interface, select the interface name and proceed with configuration as described in one of the following topics:

- Configuring an E1 Interface with Quick Configuration on page 101
- Configuring an E3 Interface with Quick Configuration on page 104
- Configuring a Fast Ethernet Interface with Quick Configuration on page 109
- Configuring a T1 Interface with Quick Configuration on page 111
- Configuring a T3 Interface with Quick Configuration on page 115
- Configuring a Serial Interface with Quick Configuration on page 118

### ***Configuring an E1 Interface with Quick Configuration***

To configure properties on an E1 interface:

1. From the Quick Configuration page, as shown in Figure 22, select the E1 interface you want to configure.

The properties you can configure on an E1 interface are displayed, as shown in Figure 23.

**Figure 23: E1 Interfaces Quick Configuration Page**

The screenshot shows the Juniper J6300 Router web interface. The top navigation bar includes the Juniper logo, the router model "ROUTER - J6300", and the user "regress" is logged in. There are links for "Help", "About", and "Logout". Below the navigation bar, the "Configuration" tab is selected, and the breadcrumb trail is "Configuration > Quick Configuration > Interfaces".

The left sidebar contains a menu with the following items: "Quick Configuration" (expanded), "Set Up", "SSL", "Interfaces" (selected), "Users", "SNMP", "Routing", "Firewall/NAT", "IPSec Tunnels", "Realtime Performance Monitoring", "View and Edit", "History", and "Rescue".

The main content area is titled "Quick Configuration" and "Interfaces". It shows the "Physical Interface: 'e1-1/0/0'". Under the "Logical Interfaces" section, it states "No logical interfaces configured." and has an "Add..." button. The "Physical Interface Description" field is empty. The "Encapsulation" section has a dropdown menu and an "Enable CHAP" checkbox. The "CHAP Local Identity" section has a "Use System Host Name" checkbox and fields for "Local Name", "CHAP Peer Identity", and "CHAP Secret".

2. Enter information into the Quick Configuration page, as described in Table 23.
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 127.

**Table 23: E1 Quick Configuration Summary**

Field	Function	Your Action
<b>Logical Interfaces</b>		
Add logical interfaces	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.	Click <b>Add</b> .
Logical Interface Description	(Optional) Describes the logical interface.	Type a text description of the logical interface to more clearly identify it in monitoring displays.
IPv4 Addresses and Prefixes	Specifies one or more IPv4 addresses for the interface.	<ol style="list-style-type: none"> <li>1. Type one or more IPv4 addresses and prefixes. For example:  10.10.10.10/24</li> <li>2. Click <b>Add</b>.</li> <li>3. Click <b>OK</b>.</li> </ol>
Physical Interface Description	(Optional) Adds supplementary information about the physical E1 interface.	Type a text description of the E1 interface to more clearly identify it in monitoring displays.
MTU (bytes)	Specifies the maximum transmission unit size for the E1 interface.	Type a value between <b>256</b> and <b>9192</b> bytes. The default MTU for E1 interfaces is 1504.
Clocking	Specifies the transmit clock source for the E1 line.	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>internal</b>—Services Router's own system clock (the default)</li> <li>■ <b>external</b>—Clock received from the E1 interface</li> </ul>
<b>Encapsulation</b>		
Encapsulation	Specifies the encapsulation type for traffic on the interface.	<p>From the list, select the encapsulation for this E1 interface:</p> <ul style="list-style-type: none"> <li>■ <b>PPP</b></li> <li>■ <b>Frame Relay</b></li> <li>■ <b>Cisco HDLC</b></li> </ul>
Enable CHAP	Enables or disables CHAP authentication on an E1 interface with PPP encapsulation only.	<ul style="list-style-type: none"> <li>■ To enable CHAP, select the check box.</li> <li>■ To disable CHAP, clear the check box.</li> </ul>
<b>CHAP Local Identity (available if CHAP is enabled)</b>		
Use System Host Name	Specifies that the E1 interface uses the Services Router's system hostname in CHAP challenge and response packets.	<ul style="list-style-type: none"> <li>■ To enable, select the check box (the default).</li> <li>■ To disable, clear the check box.</li> </ul>

**Table 23: E1 Quick Configuration Summary (continued)**

Field	Function	Your Action
Local Name	If Use System Host Name is disabled, specifies the local name for CHAP to use.	Type a local name for this E1 interface.
CHAP Peer Identity	Identifies the client or peer with which the Services Router communicates on this E1 interface.	Type the CHAP client name.
CHAP Secret	Specifies the secret password for CHAP authentication, known to both sides of the connection.	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.
<b>E1 Options</b>		
Framing Mode	Specifies the framing mode for the E1 line.	From the list, select one of the following: <ul style="list-style-type: none"> <li>■ <b>g704</b>—The default</li> <li>■ <b>g704-no-crc4</b>—G704 without cyclic redundancy check 4 (CRC4)</li> <li>■ <b>unframed</b>—Unframed transmission format</li> </ul>
Invert Data	Enables or disables data inversion. Data inversion is normally used only in alternate mark inversion (AMI) mode.	<ul style="list-style-type: none"> <li>■ To enable, select the check box.</li> <li>■ To disable, clear the check box.</li> </ul>
Timeslots	Specifies the number of time slots allocated to a fractional E1 interface. By default, an E1 interface uses all the time slots.	Type numeric values from 2 through 32. Separate discontinuous entries with commas, and use hyphens to indicate ranges. For example:  2,4,7–9
Frame Checksum	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.	Select <b>16</b> or <b>32</b> . The default checksum is 16.

## Configuring an E3 Interface with Quick Configuration

To configure properties on an E3 interface:

1. From the Quick Configuration page, as shown in Figure 22, select the interface you want to configure.

The properties you can configure on an E3 interface are displayed, as shown in Figure 24.

Figure 24: E3 Interfaces Quick Configuration Page

Juniper NETWORKS

ROUTER - J6300

Logged in as: regress

[Help](#) [About](#) [Logout](#)

**Monitor** **Configuration** **Diagnose** **Manage** **Alarms**

**Quick Configuration**

Set Up

Secure Access

**Interfaces**

Users

SNMP

Routing

Firewall/NAT

DHCP

IPSec Tunnels

Realtime Performance Monitoring

► **View and Edit**

► **History**

► **Rescue**

[Configuration](#) > [Quick Configuration](#) > [Interfaces](#)

**Quick Configuration**

**Interfaces** **Physical Interface: 'e3-3/0/0'**

**Logical Interfaces**

	Logical Interface Name	Link State	Configured	Description
<input type="checkbox"/>	<a href="#">e3-3/0/0.0</a>	Up	Yes	Logical Unit 0 on E3 Interface 'e3-3/0/0'

**Physical Interface Description**

**MTU (bytes)**  ?

**Clocking**  (internal) ?

**Encapsulation**

**Encapsulation**

**Enable CHAP** ☐

- Enter information into the Quick Configuration page, as described in Table 24.
- 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**.
- To verify that the E3 interface is configured correctly, see “Verifying Interface Configuration” on page 127.

**Table 24: E3 Quick Configuration Summary**

Field	Function	Your Action
<b>Logical Interfaces</b>		
Add logical interfaces	Defines one or more logical units that you connect to this physical E3 interface. You must define at least one logical unit for an E3 interface. You can define multiple units if the encapsulation type is Frame Relay.	Click <b>Add</b> .
Logical Interface Description	(Optional) Describes the logical interface.	Type a text description of the logical interface to more clearly identify it in monitoring displays.
IPv4 Addresses and Prefixes	Specifies one or more IPv4 addresses for the interface.	<ol style="list-style-type: none"> <li>1. Type one or more IPv4 addresses and prefixes. For example:  10.10.10.10/24</li> <li>2. Click <b>Add</b>.</li> <li>3. Click <b>OK</b>.</li> </ol>
Physical Interface Description	(Optional) Adds supplementary information about the physical E3 interface.	Type a text description of the E3 interface to more clearly identify it in monitoring displays.
MTU (bytes)	Specifies the maximum transmission unit size for the E3 interface.	Type a value between <b>256</b> and <b>9192</b> bytes. The default MTU for E3 interfaces is <b>4474</b> .
Clocking	Specifies the transmit clock source for the E3 line.	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>internal</b>—Services Router's own system clock (the default)</li> <li>■ <b>external</b>—Clock received from the E3 interface</li> </ul>
<b>Encapsulation</b>		
Encapsulation	Specifies the encapsulation type for traffic on the interface.	<p>From the list, select the encapsulation for this E3 interface:</p> <ul style="list-style-type: none"> <li>■ <b>PPP</b></li> <li>■ <b>Frame Relay</b></li> <li>■ <b>Cisco HDLC</b></li> </ul>
Enable CHAP	Enables or disables CHAP authentication on an E3 interface with PPP encapsulation only.	<ul style="list-style-type: none"> <li>■ To enable CHAP, select the check box.</li> <li>■ To disable CHAP, clear the check box.</li> </ul>
<b>CHAP Local Identity (available if CHAP is enabled)</b>		
Use System Host Name	Specifies that the E3 interface uses the Services Router's system hostname in CHAP challenge and response packets.	<ul style="list-style-type: none"> <li>■ To enable, select the check box (the default).</li> <li>■ To disable, clear the check box.</li> </ul>



**Table 24: E3 Quick Configuration Summary (continued)**

Field	Function	Your Action
Local Name	If Use System Host Name is disabled, specifies the local name for CHAP to use.	Type a local name for this E3 interface.
CHAP Peer Identity	Identifies the client or peer with which the Services Router communicates on this E3 interface.	Type the CHAP client name.
CHAP Secret	Specifies the secret password for CHAP authentication, known to both sides of the connection.	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.
<b>E3 Options</b>		
Bert Algorithm	<p>Specifies the bit error rate test (BERT) algorithm to use during a BERT.</p> <p>BERT is supported only when transmission is unframed. (See the Unframed option.)</p>	<p>From the Bert Algorithm list, select the algorithm to use:</p> <ul style="list-style-type: none"> <li>■ <b>all-ones-repeating</b></li> <li>■ <b>alternating-ones-zeros</b></li> <li>■ <b>all-zeros-repeating</b></li> <li>■ <b>pseudo-2e11-o152</b></li> <li>■ <b>pseudo-2e15-o151</b></li> <li>■ <b>pseudo-2e20-o151</b></li> <li>■ <b>pseudo-2e20-o153</b></li> <li>■ <b>pseudo-2e23-o151</b></li> <li>■ <b>pseudo-2e29</b></li> <li>■ <b>pseudo-2e31</b></li> <li>■ <b>pseudo-2e9-o153</b></li> </ul> <p>The default is <b>pseudo-2e15-o151</b>.</p>
Bert Error Rate	Specifies the exponent $n$ in the bit error rate $10^{-n}$ .	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).
Bert Period	Specifies the length of time—in seconds—of the BERT.	Type a value between 1 and 240. The default is 10.

**Table 24: E3 Quick Configuration Summary (continued)**

Field	Function	Your Action
Compatibility Mode	<p>Defines the transmission mode and subrating to use on the E3 interface. 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.</p> <p>CSU compatibility mode and subrating are supported only when transmission is unframed. (See the Unframed option.)</p>	<p>Select one of the following check boxes:</p> <ul style="list-style-type: none"> <li>■ <b>Off</b>—CSU compatibility is disabled.</li> <li>■ <b>Digital-Link</b>—Compatible with a Digital Link CSU.</li> <li>■ <b>Kentrox</b>—Compatible with a Kentrox CSU.</li> </ul> <p>If you select <b>Digital-Link</b>, you can optionally specify a substrate by selecting a value from the Subrate list.</p> <p>If you select <b>Kentrox</b>, you can optionally specify a substrate by typing a value from 1 through 48 in the Subrate box.</p> <p>If you do not specify a substrate, the full E3 rate is used.</p>
Frame Checksum	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.	From the Frame Checksum list, select <b>16</b> or <b>32</b> . The default value is <b>16</b> .
Idle Cycle Flag	Specifies the value to transmit during idle cycles.	<p>From the Idle Cycle Flag list, select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>flags</b>—Transmits the value 0x7E during idle cycles. This is the default.</li> <li>■ <b>ones</b>—Transmits the value 0xFF during idle cycles.</li> </ul>
Loopback	<p>Configures the E3 interface as a loopback interface for testing purposes.</p> <p>When E3 is configured as a local loopback interface, the router transmits test traffic simultaneously to the CSU and to the receiver at the E3 interface.</p> <p>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.</p>	<p>From the Loopback list, select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>local</b>—Traffic loops from the transmitter to the receiver at the E3 interface during tests.</li> <li>■ <b>remote</b>—Traffic loops from the receiver to the transmitter at the E3 interface during tests.</li> </ul>

**Table 24: E3 Quick Configuration Summary (continued)**

<b>Field</b>	<b>Function</b>	<b>Your Action</b>
Payload Scrambler	<p>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.</p> <p>The payload scrambler is supported only when CSU compatibility is enabled and transmission is framed. (See the Compatibility Mode and Unframed options).</p>	<p>Select one of the following check boxes:</p> <ul style="list-style-type: none"> <li>■ <b>Yes</b>—Transmission is scrambled.</li> <li>■ <b>No</b>—Transmission is not scrambled.</li> </ul>
Start End Flag	Specifies whether the end and start flags are separated.	<p>From the Start End Flag list, select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>filler</b>—Flags are separated by idle cycles.</li> <li>■ <b>shared</b>—Flags overlap (no separation).</li> </ul>
Unframed	Specifies whether the transmission is framed (G.751 framing) or unframed.	<p>Select one of the following check boxes:</p> <ul style="list-style-type: none"> <li>■ <b>Yes</b>—Unframed transmission.</li> <li>■ <b>No</b>—Framed transmission.</li> </ul>

### **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 22, select the interface you want to configure.

The properties you can configure on a Fast Ethernet interface are displayed, as shown in Figure 25.

**Figure 25: Fast Ethernet Interfaces Quick Configuration Page**

The screenshot shows the Juniper J4300 Router web interface. The top navigation bar includes 'Monitor', 'Configuration', 'Diagnose', and 'Manage'. The 'Configuration' tab is active, and the breadcrumb trail is 'Configuration > Quick Configuration > Interfaces'. The left sidebar shows a tree view with 'Quick Configuration' expanded, containing 'Set Up', 'SSL', 'Interfaces' (selected), 'Users', 'SNMP', 'Routing', 'Firewall/NAT', 'IPSec Tunnels', and 'Realtime Performance Monitoring'. Below this are 'View and Edit', 'History', and 'Rescue' buttons.

The main content area is titled 'Quick Configuration' and 'Interfaces'. It shows the 'Physical Interface: fe-0/0/0'. Below this is a table for 'Logical Interfaces':

	Logical Interface Name	Link State	Configured	Description
<input type="checkbox"/>	<a href="#">fe-0/0/0.0</a>	Down	Yes	Logical Unit 0 on Fast Ethernet Interface 'fe-0/0/0'

Below the table are 'Add...' and 'Delete' buttons. A 'Physical Interface Description' text box is also present. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Copyright © 2004-2005, Juniper Networks, Inc. All Rights Reserved. [Trademark Notice.](#)

2. Enter information into the Quick Configuration page, as described in Table 25.
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 127.

**Table 25: Fast Ethernet Quick Configuration Summary**

Field	Function	Your Action
<b>Logical Interfaces</b>		
Add logical interfaces	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.	Click <b>Add</b> .
Logical Interface Description	(Optional) Describes the logical interface.	Type a text description of the logical interface to more clearly identify it in monitoring displays.
IPv4 Addresses and Prefixes	Specifies one or more IPv4 addresses for the interface.	<ol style="list-style-type: none"> <li>1. Type one or more IPv4 addresses and prefixes. For example:  10.10.10.10/24</li> <li>2. Click <b>Add</b>.</li> <li>3. Click <b>OK</b>.</li> </ol>
Physical Interface Description	(Optional) Adds supplementary information about the physical Fast Ethernet interface.	Type a text description of the Fast Ethernet interface to more clearly identify it in monitoring displays.
MTU (bytes)	Specifies the maximum transmission unit size for the Fast Ethernet interface.	Type a value between <b>256</b> and <b>9192</b> bytes. The default MTU for Fast Ethernet interfaces is <b>1504</b> .

### Configuring a T1 Interface with Quick Configuration

To configure properties on a T1 interface:

1. From the Quick Configuration page, as shown in Figure 22, select the interface you want to configure.

The properties you can configure on a T1 interface are displayed, as shown in Figure 26.

**Figure 26: T1 Interfaces Quick Configuration Page**

Juniper NETWORKS **ROUTER - J6300** Logged in as: **regress**  
[Help](#) [About](#) [Logout](#)

**Monitor** **Configuration** **Diagnose** **Manage**

[Configuration](#) > [Quick Configuration](#) > [Interfaces](#)

**Quick Configuration**

Set Up  
SSL  
**Interfaces**  
Users  
SNMP  
Routing  
Firewall/NAT  
IPSec Tunnels  
Realtime Performance Monitoring

► **View and Edit**  
► **History**  
► **Rescue**

**Quick Configuration**

**Interfaces** **Physical Interface: 't1-6/0/1'**

**Logical Interfaces**

No logical interfaces configured.

**Physical Interface Description**

**Encapsulation**

**Encapsulation**   
**Enable CHAP** ☐

**CHAP Local Identity**

**Use System Host Name** ☒  
**Local Name**   
**\* CHAP Peer Identity**   
**\* CHAP Secret**

2. Enter information into the Quick Configuration page, as described in Table 26.
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 127.

**Table 26: T1 Quick Configuration Summary**

Field	Function	Your Action
<b>Logical Interfaces</b>		
Add logical interfaces	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.	Click <b>Add</b> .
Logical Interface Description	(Optional) Describes the logical interface.	Type a text description of the logical interface to more clearly identify it in monitoring displays.
IPv4 Addresses and Prefixes	Specifies one or more IPv4 addresses for the interface.	<ol style="list-style-type: none"> <li>1. Type one or more IPv4 addresses and prefixes. For example:  10.10.10.10/24</li> <li>2. Click <b>Add</b>.</li> <li>3. Click <b>OK</b>.</li> </ol>
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 <b>256</b> and <b>9192</b> bytes. The default MTU for T1 interfaces is <b>1504</b> .
Clocking	Specifies the transmit clock source for the T1 line.	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>internal</b>—Services Router's own system clock (the default)</li> <li>■ <b>external</b>—Clock received from the T1 interface</li> </ul>
<b>Encapsulation</b>		
Encapsulation	Specifies the encapsulation type for traffic on the interface.	<p>From the list, select the encapsulation for this T1 interface:</p> <ul style="list-style-type: none"> <li>■ <b>PPP</b></li> <li>■ <b>Frame Relay</b></li> <li>■ <b>Cisco HDLC</b></li> </ul>
Enable CHAP	Enables or disables CHAP authentication on a T1 interface with PPP encapsulation only.	<ul style="list-style-type: none"> <li>■ To enable CHAP, select the check box.</li> <li>■ To disable CHAP, clear the check box.</li> </ul>
<b>CHAP Local Identity (available if CHAP is enabled)</b>		
Use System Host Name	Specifies that the T1 interface uses the Services Router's system hostname in CHAP challenge and response packets.	<ul style="list-style-type: none"> <li>■ To enable, select the check box (the default).</li> <li>■ To disable, clear the check box.</li> </ul>

**Table 26: T1 Quick Configuration Summary (continued)**

Field	Function	Your Action
Local Name	If Use System Host Name is disabled, specifies the local name for CHAP to use.	Type a local name for this T1 interface.
CHAP Peer Identity	Identifies the client or peer with which the Services Router communicates on this T1 interface.	Type the CHAP client name.
CHAP Secret	Specifies the secret password for CHAP authentication, known to both sides of the connection.	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.
<b>T1 Options</b>		
Framing Mode	Specifies the framing mode for the T1 line.	From the list, select one of the following: <ul style="list-style-type: none"> <li>■ <b>esf</b>—Extended superframe (the default)</li> <li>■ <b>sf</b>—Superframe</li> </ul>
Line Encoding	Specifies the line encoding method.	From the list, select one of the following: <ul style="list-style-type: none"> <li>■ <b>ami</b>—Alternate mark inversion</li> <li>■ <b>b8zs</b>—Binary 8 zero substitution (the default)</li> </ul>
Byte Encoding	Specifies the byte encoding method.	From the list, select one of the following: <ul style="list-style-type: none"> <li>■ <b>nx56</b>—7 bits per byte</li> <li>■ <b>nx64</b>—8 bits per byte (the default)</li> </ul>
Invert Data	Enables or disables data inversion. Data inversion is normally used only in alternate mark inversion (AMI) mode.	<ul style="list-style-type: none"> <li>■ To enable, select the check box.</li> <li>■ To disable, clear the check box.</li> </ul>
Timeslots	Specifies the number of time slots allocated to a fractional T1 interface. By default, a T1 interface uses all the time slots.	Type numeric values from <b>1</b> through <b>24</b> . You can use any combination of time slots. To configure ranges, use hyphens. To configure discontinuous slots, use commas. For example:  <b>1-5,10,24</b>



**Table 26: T1 Quick Configuration Summary (continued)**

Field	Function	Your Action
Frame Checksum	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.	Select <b>16</b> or <b>32</b> . The default value is <b>16</b> .
Line Buildout	<p>Specifies the T1 line buildout in feet for cables 655 feet (200 m) or shorter, or in decibels for longer cables.</p> <p>Line buildout compensates for the loss in decibels based on the distance from the device to the first repeater in the circuit.</p>	<p>From the list, select one of the following line buildouts:</p> <ul style="list-style-type: none"> <li>■ <b>0–132</b> (0 m–40 m) (the default)</li> <li>■ <b>133–265</b> (40 m–81 m)</li> <li>■ <b>266–398</b> (81 m–121 m)</li> <li>■ <b>399–531</b> (121 m–162 m)</li> <li>■ <b>532–655</b> (162 m–200 m)</li> <li>■ <b>long-0db</b></li> <li>■ <b>long-7.5db</b></li> <li>■ <b>long-15db</b></li> <li>■ <b>long-22.5db</b></li> </ul>

### Configuring a T3 Interface with Quick Configuration

To configure properties on a T3 (DS3) interface:

1. From the Quick Configuration page, as shown in Figure 22, select the interface you want to configure.

The properties you can configure on a T3 interface are displayed, as shown in Figure 27.

**Figure 27: T3 Interfaces Quick Configuration Page**

Juniper NETWORKS **ROUTER - J6300** Logged in as: **regress**  
[Help](#) [About](#) [Logout](#)

**Monitor Configuration Diagnose Manage**

**Quick Configuration**  
 Set Up  
 SSL  
**Interfaces**  
 Users  
 SNMP  
 Routing  
 Firewall/NAT  
 IPSec Tunnels  
 Realtime Performance Monitoring

**View and Edit**  
**History**  
**Rescue**

**Configuration > Quick Configuration > Interfaces**

**Quick Configuration**  
**Interfaces Physical Interface: 't3-4/0/0'**

**Logical Interfaces**  
 No logical interfaces configured.  
 Add...

**Physical Interface Description**

**Encapsulation**  
 Encapsulation  
 Enable CHAP

**CHAP Local Identity**  
 Use System Host Name  
 Local Name  
 \* CHAP Peer Identity  
 \* CHAP Secret

2. Enter information into the Quick Configuration page, as described in Table 27.
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 127.

**Table 27: T3 Quick Configuration Summary**

Field	Function	Your Action
<b>Logical Interfaces</b>		
Add logical interfaces	Defines one or more logical units that you connect to this physical T3 interface. You must define at least one logical unit for a T3 interface. You can define multiple units if the encapsulation type is Frame Relay.	Click <b>Add</b> .
Logical Interface Description	(Optional) Describes the logical interface.	Type a text description of the logical interface to more clearly identify it in monitoring displays.
IPv4 Addresses and Prefixes	Specifies one or more IPv4 addresses for the interface.	<ol style="list-style-type: none"> <li>1. Type one or more IPv4 addresses and prefixes. For example:  10.10.10.10/24</li> <li>2. Click <b>Add</b>.</li> <li>3. Click <b>OK</b>.</li> </ol>
Physical Interface Description	(Optional) Adds supplementary information about the physical T3 interface.	Type a text description of the T3 interface to more clearly identify it in monitoring displays.
MTU (bytes)	Specifies the maximum transmission unit size for the T3 interface.	Type a value between <b>256</b> and <b>9192</b> bytes. The default MTU for T3 interfaces is <b>4474</b> .
Clocking	Specifies the transmit clock source for the T3 line.	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>internal</b>—Services Router's own system clock (the default)</li> <li>■ <b>external</b>—Clock received from the T3 interface</li> </ul>
<b>Encapsulation</b>		
Encapsulation	Specifies the encapsulation type for traffic on the interface.	<p>From the list, select the encapsulation for this T3 interface:</p> <ul style="list-style-type: none"> <li>■ <b>PPP</b></li> <li>■ <b>Frame Relay</b></li> <li>■ <b>Cisco HDLC</b></li> </ul>
Enable CHAP	Enables or disables CHAP authentication on a T3 interface with PPP encapsulation only.	<ul style="list-style-type: none"> <li>■ To enable CHAP, select the check box.</li> <li>■ To disable CHAP, clear the check box.</li> </ul>
<b>CHAP Local Identity (available if CHAP is enabled)</b>		
Use System Host Name	Specifies that the T3 interface uses the Services Router's system hostname in CHAP challenge and response packets.	<ul style="list-style-type: none"> <li>■ To enable, select the check box (the default).</li> <li>■ To disable, clear the check box.</li> </ul>

**Table 27: T3 Quick Configuration Summary (continued)**

Field	Function	Your Action
Local Name	If Use System Host Name is disabled, specifies the local name for CHAP to use.	Type a local name for this T3 interface.
CHAP Peer Identity	Identifies the client or peer with which the Services Router communicates on this T3 interface.	Type the CHAP client name.
CHAP Secret	Specifies the secret password for CHAP authentication, known to both sides of the connection.	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.
<b>T3 Options</b>		
Frame Checksum	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.	Select <b>16</b> or <b>32</b> . The default value is <b>16</b> .
Enable Long Buildout	Specifies a short or long cable length for copper-cable-based T3 interfaces. A long cable is longer than 225 feet (68.6m).	<div> <input type="checkbox"/> To enable long buildout, select the check box.         </div> <div> <input type="checkbox"/> To disable long buildout, clear the check box.         </div>
Disable C-Bit Parity Mode	Enables or disables C-bit parity mode, which controls the type of framing that is present on the transmitted T3 signal.	<div> <input type="checkbox"/> To disable, select the check box.         </div> <div> <input type="checkbox"/> To enable, clear the check box.         </div>

## Configuring a Serial Interface 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 a Services Router 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 22, select the interface you want to configure.

The properties you can configure on a serial interface are displayed, as shown in Figure 28.

**Figure 28: Serial Interfaces Quick Configuration Page**

The screenshot shows the Juniper J6300 Router configuration interface. At the top, the Juniper logo and 'ROUTER - J6300' are displayed. The user is logged in as 'regress'. Navigation links for 'Help', 'About', and 'Logout' are present. The main menu includes 'Monitor', 'Configuration', 'Diagnose', and 'Manage'. The 'Configuration' tab is active, and the breadcrumb trail is 'Configuration > Quick Configuration > Interfaces'. The left sidebar shows a tree view with 'Quick Configuration' expanded, containing 'Set Up', 'SSL', 'Interfaces' (selected), 'Users', 'SNMP', 'Routing', 'Firewall/NAT', 'IPSec Tunnels', and 'Realtime Performance Monitoring'. Below this are 'View and Edit', 'History', and 'Rescue' buttons. The main content area is titled 'Quick Configuration' and 'Interfaces'. It shows 'Physical Interface: 'se-5/0/0''. Under 'Logical Interfaces', it states 'No logical interfaces configured.' with an 'Add...' button. The 'Physical Interface Description' field is empty. The 'Encapsulation' section has a dropdown menu. The 'Enable CHAP' checkbox is unchecked. The 'CHAP Local Identity' section has 'Use System Host Name' checked. The 'Local Name' field is empty. The 'CHAP Peer Identity' and 'CHAP Secret' fields are marked with red asterisks and are empty.

2. Enter information into the Quick Configuration page, as described in Table 28.
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 127.

**Table 28: Serial Quick Configuration Summary**

Field	Function	Your Action
<b>Logical Interfaces</b>		
Add logical interfaces	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.	Click <b>Add</b> .
Logical Interface Description	(Optional) Describes the logical interface.	Type a text description of the logical interface to more clearly identify it in monitoring displays.
IPv4 Addresses and Prefixes	Specifies one or more IPv4 addresses for the interface.	<ol style="list-style-type: none"> <li>Type one or more IPv4 addresses and prefixes. For example:  10.10.10.10/24</li> <li>Click <b>Add</b>.</li> <li>Click <b>OK</b>.</li> </ol>
Physical Interface Description	(Optional) Adds supplementary information about the physical serial interface.	Type a text description of the serial interface to more clearly identify it in monitoring displays.
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.
<b>Encapsulation</b>		
Encapsulation	Specifies the encapsulation type for traffic on the interface.	<p>From the list, select the encapsulation for this serial interface:</p> <ul style="list-style-type: none"> <li>■ <b>PPP</b></li> <li>■ <b>Frame Relay</b></li> <li>■ <b>Cisco HDLC</b></li> </ul>
Enable CHAP	Enables or disables CHAP authentication on a serial interface with PPP encapsulation only.	<ul style="list-style-type: none"> <li>■ To enable CHAP, select the check box.</li> <li>■ To disable CHAP, clear the check box.</li> </ul>
<b>CHAP Local Identity (available if CHAP is enabled)</b>		
Use System Host Name	Specifies that the serial interface use the Services Router's system hostname in CHAP challenge and response packets.	<ul style="list-style-type: none"> <li>■ To enable, select the check box (the default).</li> <li>■ To disable, clear the check box.</li> </ul>
Local Name	If Use System Host Name is disabled, specifies the local name for CHAP to use.	Type a local name for this serial interface.
CHAP Peer Identity	Identifies the client or peer with which the Services Router communicates on this serial interface.	Type the CHAP client name.
CHAP Secret	Specifies the secret password for CHAP authentication, known to both sides of the connection.	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.
<b>Serial Options</b>		

**Table 28: Serial Quick Configuration Summary (continued)**

Field	Function	Your Action
Clocking Mode	<p>Specifies the clock source to determine the timing on serial interfaces.</p> <p>If you use an externally timed clocking mode—<b>dce</b> or <b>loop</b>—long cables might introduce a phase shift of DTE-transmitted clock and data. At high speeds, this phase shift might cause errors.</p> <p>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:</p> <ul style="list-style-type: none"> <li>■ In the J-Web configuration editor, set the Transmit clock value to <b>invert</b> on the <b>Interfaces &gt; interface-name &gt; Serial options</b> page.</li> <li>■ In the CLI configuration editor, include the <b>transmit-clock invert</b> statement at the <b>[edit interfaces se-pim / 0 / port serial-options]</b> hierarchy level.</li> </ul>	<p>From the list, select one of the following timing sources:</p> <ul style="list-style-type: none"> <li>■ <b>dce</b>—Uses a transmit clock generated by the data circuit-terminating equipment (DCE) for the Services Router's DTE.</li> <li>■ <b>internal</b>—Uses the Services Router's internal clock.</li> <li>■ <b>loop</b>—Uses the DCE's or DTE's receive clock (the default).</li> </ul> <p>For X.21 serial interfaces, you must use the <b>loop</b> clocking mode.</p> <p>When the Services Router is functioning as DTE, you must use the <b>dce</b> clocking mode for all interfaces except X.21 serial interfaces.</p> <p>When the Services Router is functioning as DCE, we recommend using the <b>internal</b> clocking mode for all interfaces.</p>
Clock Rate	<p>Specifies the line speed in kilohertz or megahertz for serial interfaces that use the DTE clocking mode.</p>	<p>From the list, select one of the following clock rates:</p> <ul style="list-style-type: none"> <li>■ 1.2 KHz</li> <li>■ 2.4 KHz</li> <li>■ 9.6 KHz</li> <li>■ 19.2 KHz</li> <li>■ 38.4 KHz</li> <li>■ 56.0 KHz</li> <li>■ 64.0 KHz</li> <li>■ 72.0 KHz</li> <li>■ 125.0 KHz</li> <li>■ 148.0 KHz</li> <li>■ 250.0 KHz</li> <li>■ 500.0 KHz</li> <li>■ 800.0 KHz</li> <li>■ 1.0 MHz</li> <li>■ 1.3 MHz</li> <li>■ 2.0 MHz</li> <li>■ 4.0 MHz</li> <li>■ 8.0 MHz</li> </ul>

## Configuring Network Interfaces with a Configuration Editor

---

To enable the interfaces installed on your Services Router 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 Network Interfaces with Quick Configuration” on page 100. 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 122
- Configuring Compressed Real-Time Transport Protocol (CRTP) on page 124
- Deleting a Network Interface with a Configuration Editor on page 126

For information about using the J-Web and CLI configuration editors, see “Using J-Web Configuration Tools” on page 3.

### ***Adding a Network Interface with a Configuration Editor***

To configure network interfaces for the Services Router:

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 29.
3. When you are finished configuring the router, commit the configuration.
4. To verify that the network interface is configured correctly, see “Verifying Interface Configuration” on page 127.



**Table 29: Adding an Interface**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
Navigate to the <b>Interfaces</b> level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to Interfaces, click <b>Configure</b> or <b>Edit</b>.</li> </ol>	<p>From the top of the configuration hierarchy, create and name the interface:</p> <pre>edit interfaces interface-name</pre>
Create the new interface.	<ol style="list-style-type: none"> <li>1. Next to Interface, click <b>Add new entry</b>.</li> <li>2. Enter the name of the new interface in the Interface name box.  Make sure the name conforms to the interface naming rules. For more information, see “Network Interface Naming” on page 44.</li> <li>3. Click <b>OK</b>.</li> </ol>	
Create the basic configuration for the new interface.	<ol style="list-style-type: none"> <li>1. Under Interface Name in the table, click the name of the new interface.</li> <li>2. Enter values in the other fields on this page if warranted.  All these entries are optional, but you need to set values for Clocking and Encapsulation in particular if the default values are not suitable.</li> </ol>	<p>Enter values for physical interface properties as needed. Examples include changes to the default values for physical encapsulation or MTU. For example:</p> <pre>set interface-name encapsulation ppp</pre>

**Table 29: Adding an Interface (continued)**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
Add values for interface-specific options.  Most interface types have optional parameters that are specific to the interface type.	<ol style="list-style-type: none"> <li>Under Nested configuration, click <b>Configure</b> for the appropriate interface type.</li> <li>In the interface-specific page that appears, enter the values you need to supply or change the default values.</li> <li>When you are finished, click <b>OK</b> to confirm your changes or <b>Cancel</b> to cancel them and return to the previous page.</li> </ol>	<ol style="list-style-type: none"> <li>From the [edit interfaces <i>interface-name</i>] hierarchy level, type  <b>edit interface-options</b></li> <li>Enter the statement for each interface-specific property for which you need to change the default value.</li> </ol>
Add logical interfaces.	<ol style="list-style-type: none"> <li>In the main Interface page for this interface, next to Unit, click <b>Add new entry</b>.</li> <li>On the Unit page for logical interfaces that appears, type a number from 0 through 16384 in the Interface unit number box.</li> <li>Enter values in other fields as required for your network.</li> <li>To configure protocol family values if needed, under Family, click <b>Configure</b> next to the appropriate protocol.</li> <li>To access additional subordinate hierarchies under Nested configuration, click <b>Configure</b> next to any parameter you want to configure.</li> <li>When you are finished, click <b>OK</b>.</li> </ol>	<ol style="list-style-type: none"> <li>From the [edit interfaces <i>interface-name</i>] hierarchy level, type  <b>set unit logical-unit-number</b>  Replace <i>logical-unit-number</i> with a value from 0 through 16384.</li> <li>Enter additional values for properties you need to configure on the logical interface, such as logical encapsulation or protocol family.</li> </ol>

## Configuring Compressed Real-Time Transport Protocol (CRTP)

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 12-byte RTP header, the IP and UDP header, can be too large a payload on networks using low-speed lines such as dial-up modems. Compressed Real-Time Transport Protocol (CRTP) can be configured on a single link to reduce network overhead on low-speed links.

On the Services Router, CRTP can be configured on a T1 or E1 interface with PPP encapsulation and using the link services interface as a compression device.

To configure CRTP on the Services Router:

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 30.
3. If you are finished configuring the router, commit the configuration.

**Table 30: Adding CRTP to an E1 or T1 Interface**

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the <b>Interfaces</b> level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to Interfaces, click <b>Edit</b>.</li> </ol>	<p>From the top of the configuration hierarchy, create and name the interface:</p> <pre>edit interfaces interface-name</pre>
Select an E1 or T1 interface—for example, <b>t1-1/0/0</b> .	<ol style="list-style-type: none"> <li>1. Next to a T1 or E1 interface, click <b>Edit</b>.</li> </ol>	<ol style="list-style-type: none"> <li>1. Enter <pre>set encapsulation ppp</pre> </li> </ol>
Set PPP as the type of encapsulation for the physical interface.	<ol style="list-style-type: none"> <li>2. From the Encapsulation list, select <b>ppp</b> as the encapsulation type.</li> <li>3. Under Unit, click <b>Edit</b>.</li> </ol>	<ol style="list-style-type: none"> <li>2. Enter <pre>edit unit 0</pre> </li> </ol>
Add the link services interface, <b>ls-0/0/0.0</b> to the physical interface.	<ol style="list-style-type: none"> <li>1. In the Compression device box, enter <b>ls-0/0/0.0</b></li> <li>2. Click <b>OK</b> until you return to the Interfaces page.</li> </ol>	<ol style="list-style-type: none"> <li>1. Enter <pre>set compression-device ls-0/0/0.0</pre> </li> <li>2. Enter <pre>exit</pre> <p>until you return to the <b>edit interfaces</b> hierarchy.</p> </li> </ol>

**Table 30: Adding CRTP to an E1 or T1 Interface (continued)**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
Add the link services interface, ls-0/0/0, to the Services Router.	<ol style="list-style-type: none"> <li>Next to Interface, click <b>Add new entry</b>.</li> <li>In the Interface name box, type ls-0/0/0.</li> <li>Click <b>OK</b> to return to the Interfaces page.</li> <li>On the main Interface page, next to ls-0/0/0, click <b>Edit</b>.</li> <li>Next to Unit, click <b>Add new entry</b>.</li> <li>In the Interface unit number box, type 0.</li> </ol>	<p>From the [edit interfaces] hierarchy level, enter</p> <p>edit interfaces ls-0/0/0 unit 0</p>
<p>Configure the link services interface, ls-0/0/0, properties.</p> <p><b>F-max period</b> —Maximum number of compressed packets allowed between transmission of full headers. It has a range from 1 to 65535.</p> <p><b>Maximum</b> and <b>Minimum</b>—UDP port values from 1 to 65536 to reserve these ports for RTP compression. CRTP is applied to network traffic on ports within this range. This is only applicable to voice services interfaces.</p>	<ol style="list-style-type: none"> <li>Next to Compression, select <b>yes</b>, and then click <b>Configure</b>.</li> <li>Select <b>RTP</b>, and then click <b>Configure</b>.</li> <li>In the F-Max period box, type 2500.</li> <li>Select Port, then click <b>Configure</b>.</li> <li>In the Minimum value box, type 2000.</li> <li>In the Maximum value box, type 64009.</li> <li>Click <b>OK</b>.</li> </ol>	<p>Enter</p> <p>set compression rtp f-max-period 2500 port maximum 64009 minimum 2000</p>

For more information about configuring CRTP on a single link, see the *JUNOS Network Interfaces Configuration Guide* and the *JUNOS Services Interfaces Configuration Guide*.

### Deleting a Network Interface with a Configuration Editor

To delete an interface on a Services Router:

- Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
- Perform the configuration tasks described in Table 31.



**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 31: Deleting an Interface**

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the <b>Interfaces</b> level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>Next to Interfaces, click <b>Edit</b>.</li> </ol>	From the top of the configuration hierarchy, enter  edit interfaces
Select the interface you want to delete.	In the Interface table, under Interface name, select the name of the interface you want to delete.	Enter  delete <i>interface-name</i>
Execute the selection.	<ol style="list-style-type: none"> <li>Click <b>Discard</b>.</li> <li>In the page that appears, select the appropriate radio button.  If you have not made any previous changes, the only selection available is <b>Delete Configuration Below This Point</b>.</li> </ol>	Commit the configuration change:  commit

## Verifying Interface Configuration

To verify an interface configuration, perform these tasks:

- Verifying the Link State of All Interfaces on page 127
- Verifying Interface Properties on page 128

### 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 Services Router are operational.

**Action** For each interface on the Services Router:

- In the J-Web interface, select **Diagnose > Ping Host**.
- In the Remote Host box, type the address of the interface for which you want to verify the link state.
- 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
```

**What It Means** 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 *J-series Services Router Administration Guide*.

For more information about using the J-Web interface to ping a host, see the *J-series Services Router Administration Guide*.

For information about the ping command, see the *J-series Services Router Administration Guide* or the *JUNOS Protocols, Class of Service, and System Basics 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: fe-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
```

**What It Means**

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.

For more information about **show interfaces detail**, see the *JUNOS Interfaces Command Reference*.





## Chapter 4

# Configuring Digital Subscriber Line Interfaces

The Services Router supports 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.

This chapter contains the following topics.

- DSL Terms on page 131
- Before You Begin on page 132
- Configuring ATM-over-ADSL Interfaces on page 133
- Configuring ATM-over-SHDSL Interfaces on page 143
- Configuring CHAP on DSL Interfaces (Optional) on page 154
- Verifying DSL Interface Configuration on page 156

## DSL Terms

Before configuring DSL on a Services Router, become familiar with the terms defined in Table 32.

**Table 32: DSL Terms**

Term	Definition
asymmetric digital subscriber line (ADSL) interface	Physical WAN interface for connecting a Services Router 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.
ADSL2 interface	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.

**Table 32: DSL Terms (continued)**

<b>Term</b>	<b>Definition</b>
<b>ADSL2+ interface</b>	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.
<b>Annex A</b>	ITU-T Standard G.992.1 that defines how ADSL works over plain old telephone service (POTS) lines.
<b>Annex B</b>	ITU-T Standard G.992.1 that defines how ADSL works over Integrated Services Digital Network (ISDN) lines.
<b>ITU-T G.991.2</b>	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.
<b>ITU-T G.992.1</b>	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.
<b>ITU-T G.994.1</b>	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.
<b>ITU-T G.997.1</b>	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.
<b>symmetric high-speed digital subscriber line (G.SHDSL)</b>	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.
<b>symmetric high-speed digital subscriber line (SHDSL) transceiver unit-remote (STU-R)</b>	Equipment that provides symmetric high-speed digital subscriber line (SHDSL) connections to remote user terminals such as data terminals or telecommunications equipment.

## Before You Begin

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

- Establish basic connectivity. See the *J-series 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 39.
- Configure network interfaces as necessary. See “Configuring Network Interfaces” on page 99.

## Configuring ATM-over-ADSL Interfaces

J4300 and J6300 Services Routers 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). ADSL is currently not supported on the J2300 Services Router.



**NOTE:** You can configure Services Routers 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/O/port`. 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 133
- Adding an ATM-over-ADSL Network Interface with a Configuration Editor on page 138

### Configuring an ATM-over-ADSL Interface with Quick Configuration

The Quick Configuration pages allow you to configure ATM-over-ADSL interfaces on a Services Router.

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

1. In the J-Web user interface, select **Configuration > Quick Configuration > Interfaces**.

A list of the network interfaces present on the Services Router is displayed.

2. Select the `at-pim/O/port` interface name for the ADSL port you want to configure.

The ATM-over-ADSL Quick Configuration page is displayed, as shown in Figure 29.

**Figure 29: ATM-over-ADSL Interface Quick Configuration Page**

The screenshot shows the Juniper J6300 Router configuration interface. The top navigation bar includes 'Monitor', 'Configuration', 'Diagnose', 'Manage', and 'Alarms'. The 'Configuration' tab is active, and the left sidebar shows a tree view with 'Quick Configuration' expanded, containing options like 'Set Up', 'Secure Access', 'Interfaces', 'Users', 'SNMP', 'Routing and Protocols', 'Class of Service', 'Firewall/NAT', 'DHCP', 'IPSec Tunnels', 'Realtime Performance Monitoring', and 'Firewall Filters'. The main content area is titled 'Quick Configuration' and 'Interfaces'. It displays 'DSL Physical Interface: 'at-4/0/0'' and 'Logical Interfaces' (No logical interfaces configured). Below this is the 'Physical Interface Description' section with fields for 'MTU (bytes)', 'Encapsulation', and 'VPI'. The 'ADSL Options' section includes an 'Operating Mode' dropdown. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Juniper NETWORKS

ROUTER - J6300

Logged in as: regress

[Help](#) [About](#) [Logout](#)

Monitor Configuration Diagnose Manage **Alarms**

Configuration > Quick Configuration > Interfaces

Quick Configuration

Interfaces DSL Physical Interface: 'at-4/0/0'

Logical Interfaces

No logical interfaces configured.

Add...

Physical Interface Description

MTU (bytes)

Encapsulation

VPI

ADSL Options

Operating Mode

OK Cancel Apply

3. Enter information into the ATM-over-ADSL Quick Configuration pages, as described in Table 33.
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 33: ATM-over-ADSL Interface Quick Configuration Pages Summary**

Field	Function	Your Action
<b>Configuring Logical Interfaces</b>		
Logical Interfaces	Lists the logical interfaces for this ATM-over-ADSL physical interface.	<ul style="list-style-type: none"> <li>■ To add a logical interface, click <b>Add</b>.</li> <li>■ To edit a logical interface, select the interface from the list.</li> <li>■ To delete a logical interface, select the check box next to the name and click <b>Delete</b>.</li> </ul>
<b>Adding or Editing a Logical Interface</b>		
Add Logical Interfaces	Defines one or more logical units that you connect to this physical ADSL interface.	Click <b>Add</b> .
Logical Interface Description	(Optional) Describes the logical interface.	Type a text description of the logical interface to more clearly identify it in monitoring displays.
IPv4 Addresses and Prefixes	Specifies one or more IPv4 addresses for the interface.	<ol style="list-style-type: none"> <li>1. Type one or more IPv4 addresses and prefixes. For example:  10.10.10.10/24</li> <li>2. Click <b>Add</b>.</li> <li>3. Click <b>OK</b>.</li> </ol>
Destination Address	Specifies the destination address.	Type an IPv4 address for the destination.

**Table 33: ATM-over-ADSL Interface Quick Configuration Pages Summary (continued)**

Field	Function	Your Action
Encapsulation	Specifies the type of encapsulation on the DSL logical interface.	<p>From the list, select one of the following types of encapsulations.</p> <p>For ATM-over-ADSL interfaces that use <b>inet</b> (IPv4) protocols only, select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>ATM VC multiplexing</b>—Use ATM virtual circuit multiplex encapsulation.</li> <li>■ <b>ATM NLPID</b>—Use ATM network layer protocol identifier (NLPID) encapsulation.</li> <li>■ <b>Cisco-compatible ATM NLPID</b>—Use Cisco NLPID encapsulation.</li> <li>■ <b>Ethernet over ATM (LLC/SNAP)</b>—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.</li> </ul> <p>For ATM-over-ADSL for PPP-over-ATM (PPPoA) interfaces only, select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>ATM PPP over AAL5/LLC</b>—Use AAL5 logical link control (LLC) encapsulation.</li> <li>■ <b>ATM PPP over Raw AAL5</b>—Use AAL5 multiplex encapsulation.</li> </ul> <p>For other encapsulation types on the ATM-over-ADSL interfaces, select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>PPPoE over ATM (LLC/SNAP)</b>—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.</li> <li>■ <b>Ethernet over ATM (LLC/SNAP)</b>—Use ATM subnetwork attachment point (SNAP) encapsulation.</li> </ul>
VCI	Configures the ATM virtual circuit identifier (VCI) for the interface.	In the VCI box, type the number for the VCI.
<b>Configuring Physical Interface Properties</b>		
Physical Interface Description	(Optional) Adds supplementary information about the physical ATM-over-ADSL interface.	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.

**Table 33: ATM-over-ADSL Interface Quick Configuration Pages Summary (continued)**

<b>Field</b>	<b>Function</b>	<b>Your Action</b>
MTU (bytes)	Specifies the maximum transmit size of a packet for the ATM-over-ADSL interface.	Type a value from 256 to 9192.
Encapsulation	Selects the type of encapsulation for traffic on this physical interface.	<p>From the list, select the type of encapsulation for this ATM-over-ADSL interface:</p> <ul style="list-style-type: none"> <li>■ <b>ATM permanent virtual circuits</b>—Use this type of encapsulation for PPP over ATM (PPPoA) over ADSL interfaces. This is the default encapsulation for ATM-over-ADSL interfaces.</li> <li>■ <b>Ethernet over ATM encapsulation</b>—Use this type of encapsulation for PPP over Ethernet (PPPoE) over ATM-over-ADSL interfaces that carry IPv4 traffic.</li> </ul>
VPI	Configures the ATM virtual path identifier for the interface.	Type a VPI value between 0 and 255.

**Table 33: ATM-over-ADSL Interface Quick Configuration Pages Summary (continued)**

Field	Function	Your Action
<b>Configuring ADSL Options</b>		
Operating Mode	Specifies the type of DSL operating mode for the ATM-over-ADSL interface.	<p>From the list, select one of the following types of DSL operating modes—for example <b>auto</b>.</p> <p>For Annex A or Annex B, select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>auto</b>—Configure 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.</li> <li>■ <b>itu-dmt</b>—Configure the ADSL interface to train in ITU G.992.1 mode.</li> </ul> <p>For Annex A only, select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>adsl2plus</b>—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.</li> <li>■ <b>itu-dmt-bis</b>—Configure the ADSL interface to train in ITU G.992.3 mode. You can configure this mode only when it is supported on the DSLAM.</li> <li>■ <b>ansi-dmt</b>—Configure the ADSL interface to train in the ANSI T1.413 Issue II mode.</li> </ul> <p>For Annex B only, select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>etsi</b>—Configure the ADSL line to train in the ETSI TS 101 388 V1.3.1 mode.</li> <li>■ <b>itu-annexb-ur2</b>—Configure the ADSL line to train in the G.992.1 Deutsche Telekom UR-2 mode.</li> <li>■ <b>itu-annexb-non-ur2</b>—Configure the ADSL line to train in the G.992.1 Non-UR-2 mode.</li> </ul>

### **Adding an ATM-over-ADSL Network Interface with a Configuration Editor**

To configure ATM-over-ADSL network interfaces for the Services Router 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 34.
3. If you are finished configuring the router, 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 154.
  - 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 165.
5. To check the configuration, see “Verifying DSL Interface Configuration” on page 156.

**Table 34: Adding an ATM-over-ADSL Network Interface**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
Navigate to the <b>Interfaces</b> level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to Interfaces, click <b>Edit</b>.</li> </ol>	From the top of the configuration hierarchy, create and name the interface:  edit interfaces at-2/0/0
Create the new interface—for example, at-2/0/0.	<ol style="list-style-type: none"> <li>1. Next to Interface, click <b>Add new entry</b>.</li> <li>2. In the Interface name box, type at-2/0/0.</li> <li>3. Click <b>OK</b>.</li> </ol>	
<b>Configuring Physical Properties</b>		

**Table 34: Adding an ATM-over-ADSL Network Interface (continued)**

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure ATM virtual path identifier (VPI) options for the interface—for example, <b>at-2/0/0</b> .	1. In the Interface name box, select <b>at-2/0/0</b> .	1. To configure the VPI value, enter
<ul style="list-style-type: none"> <li>■ ATM VPI—A number between 0 and 255—for example, 25.</li> <li>■ 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. <ul style="list-style-type: none"> <li>■ Down count—Number of consecutive OAM loopback cells an ATM virtual circuit must lose to be identified as unavailable—for example, 200.</li> <li>■ Up count—Number of consecutive OAM loopback cells an ATM virtual interface must receive to be identified as operational—for example, 200.</li> </ul> </li> <li>■ 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.</li> </ul>	2. Next to Atm options, click <b>Configure</b> . 3. Next to Vpi, click <b>Add new entry</b> . 4. In the Vpi number box, type 25. 5. Click <b>OK</b> . 6. In the Actions box, click <b>Edit</b> . 7. Next to Oam liveness, click <b>Configure</b> . 8. In the Down count box, type 200. 9. In the Up count box, type 200. 10. Click <b>OK</b> . 11. Next to Oam period, click <b>Configure</b> . 12. From the Oam period choices list, select <b>Oam period</b> . 13. In the Oam period box, type 100. 14. Click <b>OK</b> until you return to the Interface page.	2. To configure OAM liveness values on a VPI, enter  <b>set atm-options vpi 25 oam-liveness up-count 200 down-count 200</b> 3. To configure the OAM period, enter  <b>set atm-options vpi 25 oam-period 100</b>

**Table 34: Adding an ATM-over-ADSL Network Interface (continued)**

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure the type of DSL operating mode for the ATM-over-ADSL interface—for example <b>auto</b> .	1. Next to Dsl options, click <b>Configure</b> .	Enter
Annex A and Annex B support the following operating modes:	2. From the Operating Mode list, select <b>auto</b> .	set dsl-options operating-mode auto
<ul style="list-style-type: none"> <li>■ <b>auto</b>—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.</li> <li>■ <b>itu-dmt</b>—Configures the ADSL interface to train in ITU G.992.1 mode.</li> </ul>	3. Click <b>OK</b> .	
Annex A supports the following operating modes:		
<ul style="list-style-type: none"> <li>■ <b>adsl2plus</b>—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.</li> <li>■ <b>itu-dmt-bis</b>—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.</li> <li>■ <b>ansi-dmt</b>—Configures the ADSL interface to train in the ANSI T1.413 Issue II mode.</li> </ul>		
Annex B supports the following operating modes:		
<ul style="list-style-type: none"> <li>■ <b>etsi</b>—Configures the ADSL line to train in the ETSI TS 101 388 V1.3.1 mode.</li> <li>■ <b>itu-annexb-ur2</b>—Configures the ADSL line to train in the G.992.1 Deutsche Telekom UR-2 mode.</li> <li>■ <b>itu-annexb-non-ur2</b>—Configures the ADSL line to train in the G.992.1 Non-UR-2 mode.</li> </ul>		
Configure the encapsulation type—for example, <b>ethernet-over-atm</b> .	From the Encapsulation list, select <b>ethernet-over-atm</b> .	Enter
<ul style="list-style-type: none"> <li>■ <b>atm-pvc</b>—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.</li> <li>■ <b>ethernet-over-atm</b>—Ethernet over ATM encapsulation.  For PPP over Ethernet (PPPoE) over ATM-over-ADSL interfaces that carry IPv4 traffic, use this type of encapsulation.</li> </ul>		set encapsulation ethernet-over-atm

**Table 34: Adding an ATM-over-ADSL Network Interface (continued)**

Task	J-Web Configuration Editor	CLI Configuration Editor
<b>Configuring Logical Properties</b>		
Add the logical interface.	1. Scroll down the page to Unit, and click <b>Add new entry</b> .	Enter
Set a value from 0 and 16385—for example, 3.		set unit 3
Add other values if required by your network.	2. In the Interface unit number box, type 3.  3. Enter other values in the fields required by your network.	
Configure encapsulation for the ATM-for-ADSL logical unit—for example, <b>atm-nlpid</b> .	From the Encapsulation list, select <b>atm-nlpid</b> .	Enter
The following encapsulations are supported on the ATM-over-ADSL interfaces that use <b>inet</b> (IP) protocols only:		set unit 3 encapsulation atm-nlpid
<ul style="list-style-type: none"> <li>■ <b>atm-vc-mux</b>—Use ATM virtual circuit multiplex encapsulation.</li> <li>■ <b>atm-nlpid</b>—Use ATM network layer protocol identifier (NLPID) encapsulation.</li> <li>■ <b>atm-cisco-nlpid</b>—Use Cisco NLPID encapsulation.</li> <li>■ <b>ether-over-atm-llc</b>—For interfaces that carry IPv4 traffic, use Ethernet over LLC encapsulation. You cannot configure multipoint interfaces if you use this type of encapsulation.</li> </ul>		
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 127.)		
<ul style="list-style-type: none"> <li>■ <b>atm-ppp-llc</b>— AAL5 logical link control (LLC) encapsulation.</li> <li>■ <b>atm-ppp-vc-mux</b>—Use AAL5 multiplex encapsulation.</li> </ul>		
Other encapsulation types supported on the ATM-over-ADSL interfaces:		
<ul style="list-style-type: none"> <li>■ <b>ppp-over-ether-over-atm-llc</b>—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.</li> <li>■ <b>atm-snap</b>—Use ATM subnetwork attachment point (SNAP) encapsulation.</li> </ul>		

**Table 34: Adding an ATM-over-ADSL Network Interface (continued)**

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure Operation, Maintenance, and Administration (OAM) options for ATM virtual circuits: <ul style="list-style-type: none"> <li>■ OAM F5 loopback cell thresholds (“liveness”) on ATM virtual circuits. The range is between 1 and 255, and the default is 5 cells.               <ul style="list-style-type: none"> <li>■ Down count—Number of consecutive OAM loopback cells an ATM virtual circuit must lose to be identified as unavailable—for example, 200.</li> <li>■ Up count—Number of consecutive OAM loopback cells an ATM virtual interface must receive to be identified as operational—for example, 200.</li> </ul> </li> <li>■ 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.</li> </ul>	<ol style="list-style-type: none"> <li>Next to Oam liveness, click <b>Configure</b>.</li> <li>In the Down count box, type 200.</li> <li>In the Up count box, type 200.</li> <li>Click <b>OK</b>.</li> <li>Next to Oam period, click <b>Configure</b>.</li> <li>From the Oam period choices list, select <b>Oam period</b>.</li> <li>In the Oam period box, type 100.</li> <li>Click <b>OK</b>.</li> </ol>	<ol style="list-style-type: none"> <li>To configure OAM liveness values for an ATM virtual circuit, enter   <pre>set unit 3 oam-liveness up-count 200 down-count 200</pre> </li> <li>To configure the OAM period, enter   <pre>set unit 3 oam-period 100</pre> </li> </ol>
Add the Family protocol type—for example, <code>inet</code> .	<ol style="list-style-type: none"> <li>In the Inet box, select <b>Yes</b> and click <b>Configure</b>.</li> <li>Enter the values in the fields required by your network.</li> <li>Click <b>OK</b>.</li> </ol>	Enter  <pre>set unit 3 family inet</pre> Commands vary depending on the protocol type.
Configure ATM virtual channel identifier (VCI) options for the interface. <ul style="list-style-type: none"> <li>■ ATM VCI type—<code>vci</code>.</li> <li>■ ATM VCI value—A number between 0 and 4089—for example, 35— with VCIs 0 through 31 reserved.</li> </ul>	<ol style="list-style-type: none"> <li>From the Vci Type list, select <b>vci</b>.</li> <li>In the Vci box, type 35.</li> <li>Click <b>OK</b> until you return to the Interfaces page.</li> </ol>	<ol style="list-style-type: none"> <li>To configure the VCI value, enter   <pre>set unit 3 vci 35</pre> </li> </ol>

## Configuring ATM-over-SHDSL Interfaces

Services Routers 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 Services Routers with a G.SHDSL interface for connections through SHDSL only, not for direct ATM connections.

J-series Services Routers 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`. 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 144
- Adding an ATM-over-SHDSL Interface with a Configuration Editor on page 149

### **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 **Configuration > Quick Configuration > Interfaces**.  
A list of the network interfaces installed on the Services Router is displayed.
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 30.

**Figure 30: ATM-over-SHDSL Interfaces Quick Configuration Main Page**

Juniper NETWORKS Router - J6300

Logged in as: regress Help About Logout

Monitor Configuration Diagnose Manage **Alarms**

Configuration > Quick Configuration > Interfaces

**Quick Configuration**

**Interfaces** DSL Physical Interface: 'at-5/0/0'

Logical Interfaces

No logical interfaces configured.

Physical Interface Description

MTU (bytes)  ?

Encapsulation

VPI  ?

SHDSL Options

PIC Mode  ?

Annex  ?

Line Rate  ?

Loopback  ?

Current SNR Margin

Disable ☐ ?

Value  ?

SNEXT SNR Margin

Disable ☐ ?

Value  ?

Copyright © 2004-2005, Juniper Networks, Inc. All Rights Reserved. Trademark Notice.

3. Enter information into the ATM-over-SHDSL Quick Configuration page, as described in Table 35.
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 35: ATM-over-SHDSL Interface Quick Configuration Pages Summary**

Field	Function	Your Action
<b>Configuring Logical Interfaces</b>		
Logical Interface Name	Lists the logical interfaces for the ATM-over-SHDSL physical interface.	<p>If you have not added an <b>at-pim /0/ port</b> interface, click <b>Add</b> and enter the information required in the Interfaces Quick Configuration fields.</p> <p>If you have already configured a logical interface, select the interface name from the <b>Logical Interface Name</b> list.</p> <p>To delete a logical interface, select the interface and click <b>Delete</b>.</p>
<b>Adding or Editing a Logical Interface</b>		
Add Logical Interfaces	Defines one or more logical units that you connect to this physical ADSL interface.	Click <b>Add</b> .
Logical Interface Description	(Optional) Describes the logical interface.	Type a text description of the logical interface to clearly identify it in monitoring displays.
IPv4 Addresses and Prefixes	Specifies one or more IPv4 addresses for the interface.	<ol style="list-style-type: none"> <li>Type one or more IPv4 addresses and prefixes. For example:  10.10.10.10/24</li> <li>Click <b>Add</b>.</li> <li>Click <b>OK</b>.</li> </ol>
Destination Address	Specifies the destination address.	Type an IPv4 address for the destination.



**Table 35: ATM-over-SHDSL Interface Quick Configuration Pages Summary (continued)**

Field	Function	Your Action
Encapsulation	Specifies the type of encapsulation on the SHDSL logical interface.	<p>From the list, select one of the following types of encapsulations.</p> <p>For ATM-over-SHDSL interfaces that use <b>inet</b> (IPv4) protocols only, select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>Cisco-compatible ATM NLPID</b>—Use Cisco NLPID encapsulation.</li> <li>■ <b>ATM NLPID</b>—Use ATM network layer protocol identifier (NLPID) encapsulation.</li> <li>■ <b>ATM PPP over AA5/LLC</b>—Use AAL5 logical link control (LLC) encapsulation.</li> <li>■ <b>ATM PPP over raw AAL5</b>—Use AAL5 multiplex encapsulation.</li> <li>■ <b>ATM LLC/SNAP</b>—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.</li> <li>■ <b>ATM VC multiplexing</b>—Use ATM virtual circuit multiplex encapsulation.</li> </ul> <p>For other encapsulation types on the ATM-over-SHDSL interfaces, select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>Ethernet over ATM (LLC/SNAP)</b>—Use ATM subnetwork attachment point (SNAP) encapsulation.</li> <li>■ <b>PPPoE over ATM (LLC/SNAP)</b>—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.</li> </ul>
VCI	Configures the ATM virtual circuit identifier (VCI) for the interface.	In the VCI box, type the number for the VCI.
<b>Configuring Physical Properties</b>		
Physical Interface Description	Describes the physical interface description information. (Optional)	Type a description of the interface.
MTU (bytes)	Specifies the maximum transmission unit (MTU) size, in bytes, of a packet on the ATM-over-SHDSL interface.	Type a value for the byte size—for example, <b>1500</b> .

**Table 35: ATM-over-SHDSL Interface Quick Configuration Pages Summary (continued)**

Field	Function	Your Action
Encapsulation	Selects the type of encapsulation for traffic on the physical interface.	<p>Select one of the following types of encapsulation:</p> <ul style="list-style-type: none"> <li>■ <b>ATM permanent virtual circuits</b>—Use this type of encapsulation for PPP over ATM (PPPoA) over SHDSL interfaces. This is the default encapsulation for ATM-over-SHDSL interfaces.</li> <li>■ <b>Ethernet over ATM encapsulation</b>—Use this type of encapsulation for PPP over Ethernet (PPPoE) over ATM-over-SHDSL interfaces that carry IPv4 traffic.</li> </ul>
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.
<b>Configuring SHDSL Options</b>		
PIC Mode	Specifies the mode on the ATM-over-SHDSL interface.	<p>Select either of the following:</p> <ul style="list-style-type: none"> <li>■ <b>1-port-atm</b>—1-port four-wire mode</li> <li>■ <b>2-port-atm</b>—2-port two-wire mode</li> </ul>
Annex	<p>Specifies the type of annex for the interface.</p> <p>Annex defines the System Reference Model for connecting DSL networks to the plain old telephone service (POTS).</p>	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>Annex A</b>—Used in North American network implementations.</li> <li>■ <b>Annex B</b>—Used in European network implementations.</li> </ul>
Line Rate	Specifies the available line rates, in kilobits per second, to use on an G.SHDSL interface.	<p>Select the appropriate value.</p> <p>For 2-port-atm mode only, you can select <b>auto</b>, which automatically selects a line rate.</p>
Loopback	<p>Specifies the type of loopback testing for the interface.</p> <p>Loopback testing is a diagnostic procedure in which a signal is transmitted and returned to the sending device after passing through all or a portion of a network or circuit. The returned signal is compared with the transmitted signal in order to evaluate the integrity of the equipment or transmission path.</p>	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>local</b>—Used for testing the SHDSL equipment with local network devices.</li> <li>■ <b>payload</b>—Used to command the remote configuration to send back the received payload.</li> <li>■ <b>remote</b>—Used to test SHDSL with a remote network configuration.</li> </ul>

**Table 35: ATM-over-SHDSL Interface Quick Configuration Pages Summary (continued)**

Field	Function	Your Action
Current SNR Margin	Specifies the signal-to-noise ratio (SNR) margin or disables SNR.	To disable Current SNR Margin, select <b>Disable</b> .
Disable		To configure a specific value, type a number from 0 to 10—for example, 5.
Value		The range is 0 dB to 10 dB with a default value of 0.
SNEXT SNR Margin	Sets a value, from –10 dB to 10 dB, for the self-near-crosstalk (SNEXT) SNR margin, or disables SNEXT.	To disable SNEXT SNR Margin, select <b>Disable</b> .
Disable		To configure a specific value, type a number from –10 to 10—for example, 5.
Value		

### ***Adding an ATM-over-SHDSL Interface with a Configuration Editor***

To configure ATM-over-SHDSL network interfaces for the Services Router 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.
3. If you are finished configuring the router, 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 154.
  - 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 165.
5. To check the configuration, see “Verifying DSL Interface Configuration” on page 156.

**Table 36: Adding an ATM-over-SHDSL Network Interface**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
Navigate to the <b>Chassis</b> level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to Chassis, click <b>Configure</b>.</li> </ol>	<p>From the top of the configuration hierarchy, add the interface to the chassis:</p> <pre>set chassis fpc 6 pic 0 shdsl pic-mode 1-port-atm</pre>
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.	<ol style="list-style-type: none"> <li>1. Next to Fpc, click <b>Add new entry</b>.</li> <li>2. In the Slot box, type 6.</li> <li>3. Next to Pic, click <b>Add new entry</b>.</li> <li>4. In the Slot box, type 0.</li> <li>5. Next to Shdsl, click <b>Configure</b>.</li> <li>6. From the Pic mode menu, select <b>1-port-atm</b>.</li> <li>7. Click <b>OK</b> until you return to the Configuration page.</li> </ol>	
Navigate to the <b>Interfaces</b> level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to Interfaces, click <b>Edit</b>.</li> </ol>	<p>From the top of the configuration hierarchy, create and name the interface:</p> <pre>edit interfaces at-2/0/0</pre>
Create the new interface—for example, at-2/0/0.	<ol style="list-style-type: none"> <li>1. Next to Interface, click <b>Add new entry</b>.</li> <li>2. In the Interface name box, type at-2/0/0.</li> <li>3. Click <b>OK</b>.</li> </ol>	
<b>Configuring Physical Properties</b>		

**Table 36: Adding an ATM-over-SHDSL Network Interface (continued)**

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure ATM virtual path identifier (VPI) options for the interface—for example, <b>at-2/0/0</b> .	1. In the Interface name box, select <b>at-2/0/0</b> .	1. To configure the VPI value, enter
<ul style="list-style-type: none"> <li>ATM VPI—A number between 0 and 255—for example, 25.</li> </ul>	2. Next to Atm options, click <b>Configure</b> .	<b>set atm-options vpi 25</b>
<ul style="list-style-type: none"> <li>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. <ul style="list-style-type: none"> <li>Down count—Number of consecutive OAM loopback cells an ATM virtual circuit must lose to be identified as unavailable—for example, 200.</li> <li>Up count—Number of consecutive OAM loopback cells an ATM virtual interface must receive to be identified as operational—for example, 200.</li> </ul> </li> </ul>	3. Next to Vpi, click <b>Add new entry</b> .	2. To configure OAM liveness values on a VPI, enter
	4. In the Vpi number box, type 25.	<b>set atm-options vpi 25</b>
	5. Click <b>OK</b> .	<b>oam-liveness up-count 200</b>
	6. In the Actions box, click <b>Edit</b> .	<b>200 down-count 200</b>
	7. Next to Oam liveness, click <b>Configure</b> .	3. To configure the OAM period, enter
	8. In the Down count box, type 200.	<b>set atm-options vpi 25</b>
	9. In the Up count box, type 200.	<b>oam-period 100</b>
	10. Click <b>OK</b> .	
	11. Next to Oam period, click <b>Configure</b> .	
	12. From the Oam period choices list, select <b>Oam period</b> .	
	13. In the Oam period box, type 100.	
	14. Click <b>OK</b> until you return to the Interface page.	
Configure the encapsulation type—for example, <b>ethernet-over-atm</b> .	From the Encapsulation list, select <b>ethernet-over-atm</b> .	Enter
<ul style="list-style-type: none"> <li><b>atm-pvc</b>—ATM permanent virtual circuits is the default encapsulation for ATM-over-SHDSL interfaces.</li> </ul> <p>For PPP over ATM (PPPoA) over SHDSL interfaces, use this type of encapsulation.</p>		<b>set encapsulation ethernet-over-atm</b>
<ul style="list-style-type: none"> <li><b>ethernet-over-atm</b>—Ethernet over ATM encapsulation.</li> </ul> <p>For PPP over Ethernet (PPPoE) over ATM-over-SHDSL interfaces that carry IPv4 traffic, use this type of encapsulation.</p>		

**Table 36: Adding an ATM-over-SHDSL Network Interface (continued)**

Task	J-Web Configuration Editor	CLI Configuration Editor
Set the annex type. <ul style="list-style-type: none"> <li>■ <b>Annex A</b>—Used in North American network implementations.</li> <li>■ <b>Annex B</b>—Used in European network implementations.</li> </ul>	1. Next to Shdsl options, click <b>Configure</b> . 2. From the Annex list, select <b>Annex-a</b> .	Enter  set shdsl-options annex annex-a
Configure the SHDSL line rate for the ATM-over-SHDSL interface—for example, automatic selection of the line rate.  The following values are available: <ul style="list-style-type: none"> <li>■ <b>auto</b>—Automatically selects a line rate. This option is available only in two-wire mode and is the default value.</li> <li>■ <b>192 Kbps or higher</b>—Speed of transmission of data on the SHDSL connection.</li> </ul> In the four-wire mode, the default line rate is 4608 Kbps.	From the Line Rate list, select <b>auto</b> .	Enter  set shdsl-options line-rate auto
Configure the loopback option for testing the SHDSL connection integrity—for example, local loopback.  The following values are available: <ul style="list-style-type: none"> <li>■ <b>local</b>—Used for testing the SHDSL equipment with local network devices.</li> <li>■ <b>payload</b>—Used to command the remote configuration to send back the received payload.</li> <li>■ <b>remote</b>—Used to test SHDSL with a remote network configuration.</li> </ul>	From the Loopback list, select <b>local</b> .	Enter  set shdsl-options loopback local
Configure the signal-to-noise ratio (SNR) margin—for example, 5 dB for either or both of the following thresholds: <ul style="list-style-type: none"> <li>■ <b>current</b>—Line trains at higher than current noise margin plus SNR threshold. The range is 0 to 10 dB. The default value is 0.</li> <li>■ <b>snext</b>—Line trains at higher than self-near-end crosstalk (SNEXT) threshold. The default value is disabled.</li> </ul> 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.	1. Next to Snr margin, select <b>Yes</b> , then click <b>Configure</b> . 2. From the Current list, select <b>Enter Specific Value</b> . 3. In the Value box, type 5. 4. From the Snext list, select <b>Enter Specific Value</b> . 5. In the Value box, type 5. 6. Click <b>OK</b> until you return to the Interface page.	1. Enter  set shdsl-options snr-margin current 5  2. Enter  set shdsl-options snr-margin snext 5
<b>Configuring Logical Properties</b>		

**Table 36: Adding an ATM-over-SHDSL Network Interface (continued)**

Task	J-Web Configuration Editor	CLI Configuration Editor
Add the logical interface.	1. Scroll down the page to Unit, and click <b>Add new entry</b> .	Enter
Set a value from 0 and 16385—for example, 3.		set unit 3
Add other values if required by your network.	2. In the Interface unit number box, type 3.  3. Enter other values in the fields required by your network.	
Configure encapsulation for the ATM-for-SHDSL logical unit—for example, <b>atm-nlpid</b> .	From the Encapsulation list, select <b>atm-nlpid</b> .	Enter
The following encapsulations are supported on the ATM-over-SHDSL interfaces that use <b>inet</b> (IP) protocols only:		set unit 3 encapsulation atm-nlpid
<ul style="list-style-type: none"> <li>■ <b>atm-vc-mux</b>—Use ATM virtual circuit multiplex encapsulation.</li> <li>■ <b>atm-nlpid</b>—Use ATM network layer protocol identifier (NLPID) encapsulation.</li> <li>■ <b>atm-cisco-nlpid</b>—Use Cisco NLPID encapsulation.</li> <li>■ <b>ether-over-atm-llc</b>—For interfaces that carry IPv4 traffic, use Ethernet over LLC encapsulation. You cannot configure multipoint interfaces if you use this type of encapsulation.</li> </ul>		
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 127.)		
<ul style="list-style-type: none"> <li>■ <b>atm-ppp-llc</b>—AAL5 logical link control (LLC) encapsulation.</li> <li>■ <b>atm-ppp-vc-mux</b>—Use AAL5 multiplex encapsulation.</li> </ul>		
Other encapsulation types supported on the ATM-over-SHDSL interfaces:		
<ul style="list-style-type: none"> <li>■ <b>ppp-over-ether-over-atm-llc</b>—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.</li> <li>■ <b>atm-snap</b>—Use ATM subnetwork attachment point (SNAP) encapsulation.</li> </ul>		

**Table 36: Adding an ATM-over-SHDSL Network Interface (continued)**

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure Operation, Maintenance, and Administration (OAM) options for ATM virtual circuits: <ul style="list-style-type: none"> <li>■ OAM F5 loopback cell thresholds (“liveness”) on ATM virtual circuits. The range is between 1 and 255, and the default is 5 cells.               <ul style="list-style-type: none"> <li>■ Down count—Number of consecutive OAM loopback cells an ATM virtual circuit must lose to be identified as unavailable—for example, 200.</li> <li>■ Up count—Number of consecutive OAM loopback cells an ATM virtual interface must receive to be identified as operational—for example, 200.</li> </ul> </li> <li>■ 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.</li> </ul>	1. Next to Oam liveness, click <b>Configure</b> . 2. In the Down count box, type 200. 3. In the Up count box, type 200. 4. Click <b>OK</b> . 5. Next to Oam period, click <b>Configure</b> . 6. From the Oam period choices list, select <b>Oam period</b> . 7. In the Oam period box, type 100. 8. Click <b>OK</b> .	1. To configure OAM liveness values for an ATM virtual circuit, enter  set unit 3 oam-liveness up-count 200 down-count 200  2. To configure the OAM period, enter  set unit 3 oam-period 100
Add the Family protocol type—for example, inet.	1. In the Inet box, select <b>Yes</b> and click <b>Configure</b> . 2. Enter the values in the fields required by your network. 3. Click <b>OK</b> .	Enter  set unit 3 family inet  Commands vary depending on the protocol type.
Configure ATM virtual channel identifier (VCI) options for the interface. <ul style="list-style-type: none"> <li>■ ATM VCI type—vci.</li> <li>■ ATM VCI value—A number between 0 and 4089—for example, 35—with VCIs 0 through 31 reserved.</li> </ul>	1. From the Vci type list, select <b>vci</b> . 2. In the Vci box, type 35. 3. Click <b>OK</b> until you return to the Interfaces page.	1. To configure the VCI value, enter  set unit 3 vci 35

## 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 37.
3. If you are finished configuring the router, commit the configuration.
4. To check the configuration, see “Verifying DSL Interface Configuration” on page 156.

**Table 37: Configuring CHAP**

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the Access level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>1. In the configuration hierarchy, select <b>Configuration &gt; Edit Configuration &gt; View and Edit</b>.</li> <li>2. Next to Access, click <b>Configure</b> or <b>Edit</b>.</li> </ol>	<p>From the top of the configuration hierarchy, enter</p> <pre>edit access</pre>
Define a CHAP access profile—for example, <b>A-ppp-client</b> —with a client named <b>client 1</b> and the secret (password) <b>my-secret</b> .	<ol style="list-style-type: none"> <li>1. Next to Profile, click <b>Add new entry</b>.</li> <li>2. In the Profile name box, type <b>A-ppp-client</b>.</li> <li>3. Next to Client, click <b>Add new entry</b>.</li> <li>4. In the Name box, type <b>client1</b>.</li> <li>5. In the Chap secret box, type <b>my-secret</b>.</li> <li>6. Click <b>OK</b> until you return to the Configuration page.</li> </ol>	<p>Enter</p> <pre>set profile A-ppp-client client client1 chap-secret my-secret</pre>
Navigate to the appropriate ATM interface level in the configuration hierarchy—for example, <b>at-3/0/0 unit 0</b> .	<ol style="list-style-type: none"> <li>1. In the configuration hierarchy, select <b>Interfaces</b>.</li> <li>2. In the Interface name box, click <b>at-3/0/0</b>.</li> <li>3. In the Interface unit number box, click <b>0</b>.</li> </ol>	<p>From the top of the configuration hierarchy, enter</p> <pre>edit interfaces at-3/0/0 unit 0</pre>
Configure CHAP on the ATM-over-ADSL or ATM-over-SHDSL interface and specify a unique profile name containing a client list and access parameters—for example, <b>A-ppp-client</b> .	<ol style="list-style-type: none"> <li>1. Next to Ppp options, click <b>Configure</b>.</li> <li>2. Next to Chap, click <b>Configure</b>.</li> <li>3. In the Access profile box, type <b>A-ppp-client</b>.</li> </ol>	<p>Enter</p> <pre>set ppp-options chap access-profile A-ppp-client</pre>

**Table 37: Configuring CHAP (continued)**

Task	J-Web Configuration Editor	CLI Configuration Editor
Specify a unique hostname to be used in CHAP challenge and response packets—for example, A-at-3/0/0.0.	In the Local name box, type, A-at-3/0/0.0	Enter  set ppp-options chap local-name A-at-3/0/0.0.
Set the <b>passive</b> option to handle incoming CHAP packets only.	1. In the Passive box, click <b>Yes</b> . 2. Click <b>OK</b> .	Enter  set ppp-options chap passive

## Verifying DSL Interface Configuration

To verify ATM-over-ADSL or ATM-over-SHDSL, perform these tasks:

- Verifying ADSL Interface Properties on page 156
- Displaying a PPPoA Configuration for an ATM-over-ADSL Interface on page 160
- Verifying an ATM-over-SHDSL Configuration on page 161

### 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**

```

user@host> show interfaces at-3/0/0 extensive

Physical interface: at-3/0/0, 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:           Queued packets  Transmitted packets      Dropped packets
0 best-effort             4              4              0
1 expedited-fo            0              0              0
2 assured-forw            0              0              0
3 network-cont            2340             2340             0

ADSL alarms   : LOS, LOM, LOCDNI, FAR_LOF, FAR_LOS, FAR_LOCDNI
ADSL defects  : LOF, LOS, LOCDNI, FAR_LOF, FAR_LOS, FAR_LOCDNI
ADSL media:
Seconds      Count  State
LOF          239206    2  OK
LOS          239208    1  OK
LOM           3         1  OK
LOP           0         0  OK
LOCDI         3         1  OK
LOCDNI        239205    1  OK

ADSL status:
Modem status  : Showtime
DSL mode      : Auto    Annex A
Last fail code: ATU-C not detected

ADSL Statistics:
Attenuation (dB)      : 0.5      ATU-R      ATU-C
Capacity used (%)     : 81        72
Noise margin (dB)     : 9.0      9.5
Output power (dBm)    : 7.5      8.5

Bit rate (kbps)      : Interleave Fast Interleave Fast
CRC                  : 0          8128    0          896
FEC                  : 0          3        0          0
HEC                  : 0          3        0          0
Received cells       : 0          287
Transmitted cells    : 0          4900
Bit error rate       : 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: 0,
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: 3
CoS transmit queue      Bandwidth      Buffer Priority Limit
                        %      bps      %      bytes
0 best-effort           95      7600000  95      0      low  none
3 network-control       5       400000   5      0      low  none

Logical interface at-3/0/0.0 (Index 66) (SNMP ifIndex 28) (Generation 23)
Flags: Point-To-Point SNMP-Traps 16384 Encapsulation: ATM-PPP-LLC
Traffic statistics:
Input bytes : 2432
Output bytes : 0
Input packets: 116
Output packets: 0
Local statistics:
Input bytes : 1810
Output bytes : 0
Input packets: 78
Output packets: 0

```

```

Transit statistics:
  Input bytes :                622                0 bps
  Output bytes :                 0                0 bps
  Input packets:                38                0 pps
  Output packets:               0                0 pps
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive statistics:
  Input : 33 (last seen 00:00:03 ago)
  Output: 34 (last sent 00:00:03 ago)
LCP state: Opened
NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured, mpls: Not-configured
CHAP state: Success
  Protocol inet, MTU: 4470, Generation: 24, Route table: 0
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
  Destination: 155.55.5.1, Local: 155.55.5.2, Broadcast: Unspecified, Generation: 45
VCI 0.35
  Flags: Active, 1024
  Total down time: 0 sec, Last down: Never
  ATM per-VC transmit statistics:
  Tail queue packet drops: 0
  Traffic statistics:
  Input bytes :                2432
  Output bytes :                 0
  Input packets:               116
  Output packets:               0

Logical interface at-3/0/0.32767 (Index 69) (SNMP ifIndex 25) (Generation 21)
  Flags: Point-To-Multipoint No-Multicast SNMP-Traps 16384 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
VCI 0.4
  Flags: Active, 1024
  Total down time: 0 sec, Last down: Never
  ATM per-VC transmit statistics:
  Tail queue packet drops: 0
  Traffic statistics:
  Input bytes :                 208
  Output bytes :                 208
  Input packets:                  4
  Output packets:                  4

```

**What It Means**

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 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.

For more information about `show interfaces` extensive, 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 **Configuration > View and Edit > View Configuration Text**. Alternatively, from configuration mode in the CLI, enter the `show interfaces interface-name` and the `show access` commands from the top level.

**Sample Output**

```
[edit]
user@host# show interfaces at-3/0/0
at-3/0/0 {
  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-3/0/0.0;
        passive;
      }
    }
    family inet {
      negotiate address;
    }
  }
}
user@host# show access
profile A-ppp-client {
```

```

    client A-ppp-server chap-secret "$9$G4ikPuOISyKP5cIKv7Nik.PT3"; ## SECRET-DATA
}

```

**What It Means** Verify that the output shows the intended configuration of PPPoA. For more information about the format of a configuration file, see “Viewing the Configuration Text” on page 8.

## 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**

```

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:
    Queued packets  Transmitted packets  Dropped packets
    0 best-effort    4                      4                0
    1 expedited-fo   0                      0                0
    2 assured-forw    0                      0                0
    3 network-cont   2340                   2340             0
  SHDSL alarms      : None
  SHDSL defects     : None
  SHDSL media:
    Seconds          Count  State
    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
    Frammer mode      :ATM

```

```

Dying Gasp      :Enabled
Chipset version :1
Firmware version :R3.0
SHDSL Statistics:
  Loop Attenuation (dB) :0.600
  Transmit power (dB)   :8.5
  Receiver gain (dB)    :21.420
  SNR sampling (dB)     :39.3690
  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

```

**What It Means**

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 router 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.

For more information about `show interfaces` extensive, see the *JUNOS Interfaces Command Reference*.

## Chapter 5

# Configuring Point-to-Point Protocol over Ethernet

The 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 J-series Services Router. 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 Services Router as a PPPoE client.



**NOTE:** Services Routers 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.

This chapter contains the following topics:

- PPPoE Terms on page 165
- PPPoE Overview on page 166
- Before You Begin on page 169
- Configuring a PPPoE Interface with Quick Configuration on page 169
- Configuring PPPoE with a Configuration Editor on page 172
- Verifying a PPPoE Configuration on page 180

## PPPoE Terms

Before configuring PPPoE on a Services Router, become familiar with the terms defined in Table 38.

**Table 38: PPPoE Terms**

<b>Term</b>	<b>Definition</b>
<b>access concentrator</b>	Router that acts as a server in a PPPoE session—for example, an E-series router.
<b>customer premises equipment (CPE)</b>	Router that acts as a PPPoE client in a PPPoE session—for example, a Services Router.
<b>Logical Link Control (LLC)</b>	Encapsulation protocol that allows transport of multiple protocols over a single ATM virtual connection.
<b>Point-to-Point Protocol (PPP)</b>	Encapsulation protocol for transporting IP traffic over point-to-point links.
<b>PPP over Ethernet (PPPoE)</b>	Network protocol that encapsulates PPP frames in Ethernet frames and connects multiple hosts over a simple bridging access device to a remote access concentrator.
<b>PPPoE Active Discovery Initiation (PADI) packet</b>	Initiation packet that is broadcast by the client to start the discovery process.
<b>PPPoE Active Discovery Offer (PADO) packet</b>	Offer packets sent to the client by one or more access concentrators in reply to a PADI packet.
<b>PPPoE Active Discovery Request (PADR) packet</b>	Packet sent by the client to one selected access concentrator to request a session.
<b>PPPoE Active Discovery Session-Confirmation (PADS) packet</b>	Packet sent by the selected access concentrator to confirm the session.
<b>PPPoE Active Discovery Termination (PADT) packet</b>	Packet sent by either the client or the access concentrator to terminate a session.
<b>PPPoE over ATM</b>	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.
<b>virtual path identifier (VPI)</b>	An identifier of the virtual path that establishes a route between two devices in a network.
<b>virtual channel identifier (VCI)</b>	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 Services Router, PPPoE establishes a point-to-point connection between the client (Services Router) and the server, also called an access concentrator. Multiple hosts can be connected to the Services Router, and their data can be authenticated, encrypted, and compressed before the traffic is sent to the PPPoE session on the Services Router's Fast 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 167
- PPPoE Stages on page 168
- Optional CHAP Authentication on page 169

## PPPoE Interfaces

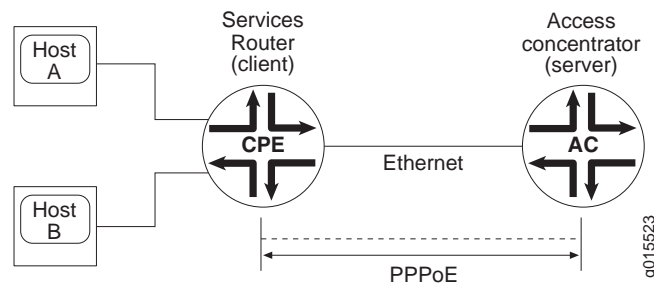
The PPPoE interface to the access concentrator can be a Fast Ethernet interface on any Services Router, an ATM-over-ADSL or ATM-over-SHDSL interface on a J4300 or J6300 Services Router, or an ATM-over-SHDSL interface on a J2300 Services Router. The PPPoE configuration is the same for both interfaces. The only difference is the encapsulation for the underlying interface to the access concentrator:

- If the interface is Fast Ethernet, use a PPPoE encapsulation.
- If the interface is ATM-over-ADSL or ATM-over-SHDSL, use a PPPoE over ATM encapsulation.

## Fast Ethernet Interface

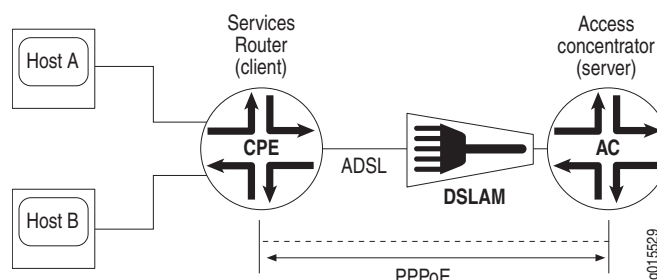
The Services Router encapsulates each PPP frame in an Ethernet frame and transports the frames over an Ethernet loop. Figure 31 shows a typical PPPoE session between a Services Router and an access concentrator on the Ethernet loop.

**Figure 31: 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 Services Router 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 32 shows a typical PPPoE over ATM session between a Services Router and an access concentrator on an ADSL loop.

**Figure 32: 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. For more information about PPPoE stages, see “Interfaces Overview” on page 39.

### PPPoE Discovery Stage

A Services Router 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 Services Router 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 Services Router supports multiple PPPoE sessions on each interface, but no more than 256 PPPoE sessions per Services Router.

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 *J-series Services Router Getting Started Guide*.
- Configure network interfaces. See “Configuring a Fast Ethernet Interface with Quick Configuration” on page 109 or “Configuring Digital Subscriber Line Interfaces” on page 131.

## Configuring a PPPoE Interface with Quick Configuration

---

To configure properties on a PPPoE interface:

1. In the J-Web user interface, select **Configuration > Quick Configuration > Interfaces**.

A list of the network interfaces present on the Services Router is displayed, as shown in Figure 22. 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 33.

**Figure 33: PPPoE Interfaces Quick Configuration Main Page**

The screenshot shows the Juniper J6300 router web interface. The top navigation bar includes 'Monitor', 'Configuration', 'Diagnose', 'Manage', and 'Alarms'. The 'Configuration' tab is active. On the left, a sidebar menu shows 'Quick Configuration' expanded, with sub-items like 'Set Up', 'Secure Access', 'Interfaces', 'Users', 'SNMP', 'Routing and Protocols', 'Class of Service', 'Firewall/NAT', 'DHCP', 'IPSec Tunnels', 'Realtime Performance Monitoring', and 'Firewall Filters'. The main content area is titled 'Quick Configuration' and 'Interfaces'. It features a 'Add a PPPoE Logical Interface' button. Below this, the 'Interface Information' section contains a 'Logical Interface Description' field and an 'IPv4 Addresses and Prefixes' table with 'Add' and 'Delete' buttons. The 'PPP Options' section includes 'Enable CHAP' (checkbox), 'CHAP Local Identity' (checkbox), 'Use System Host Name' (checkbox), 'Local Name' (text field), 'CHAP Peer Identity' (text field), and 'CHAP Secret' (text field). The 'PPPoE Options' section includes 'Access Concentrator' (text field), 'Auto Reconnect Time' (text field), 'Idle Timeout' (text field), 'Service Name' (text field), and 'Underlying Interface' (dropdown menu). At the bottom are 'OK' and 'Cancel' buttons.

3. Enter information into the Quick Configuration pages, as described in Table 39.
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 180.



**Table 39: PPPoE Quick Configuration Summary**

Field	Function	Your Action
<b>Logical Interfaces</b>		
Logical Interfaces	Lists the logical interfaces for the PPPoE physical interface.	<ul style="list-style-type: none"> <li>■ To add a logical interface, click <b>Add</b>.</li> <li>■ To edit a logical interface, select the interface from the list.</li> <li>■ To delete a logical interface, select the check box next to the name and click <b>Delete</b>.</li> </ul>
Add logical interfaces	Defines one or more logical units that you connect to this physical PPPoE interface. You must define at least one logical unit for a PPPoE interface.	Click <b>Add</b> .
Logical Interface Description	(Optional) Describes the logical interface.	Type a text description of the logical interface to more clearly identify it in monitoring displays.
IPv4 Addresses and Prefixes	Specifies one or more IPv4 addresses for the interface.	<ol style="list-style-type: none"> <li>1. Type one or more IPv4 addresses and prefixes. For example:  10.10.10.10/24</li> <li>2. Click <b>Add</b>.</li> <li>3. Click <b>OK</b>.</li> </ol>
Physical Interface Description	(Optional) Adds supplementary information about the physical PPPoE interface.	Type a text description of the PPPoE interface to more clearly identify it in monitoring displays.
<b>PPP Options</b>		
Enable CHAP	Enables or disables CHAP authentication on a PPPoE interface.	<ul style="list-style-type: none"> <li>■ To enable CHAP, select the check box.</li> <li>■ To disable CHAP, clear the check box.</li> </ul>
<b>CHAP Local Identity (available if CHAP is enabled)</b>		
Use System Host Name	Specifies that the PPPoE interface uses the Services Router's system hostname in CHAP challenge and response packets.	<ul style="list-style-type: none"> <li>■ To enable, select the check box (the default).</li> <li>■ To disable, clear the check box.</li> </ul>
Local Name	If Use System Host Name is disabled, specifies the local name for CHAP to use.	Type a local name for this PPPoE interface.
CHAP Peer Identity (required if CHAP is enabled)	Identifies the client or peer with which the Services Router communicates on this PPPoE interface.	Type the CHAP client name.
CHAP Secret (required if CHAP is enabled)	Specifies the secret password for CHAP authentication, known to both sides of the connection.	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.

**Table 39: PPPoE Quick Configuration Summary (continued)**

Field	Function	Your Action
<b>PPPoE Options</b>		
Access Concentrator	Identifies the access concentrator by a unique name.	Type a name for the access concentrator—for example, <code>ispl.com</code> .
Auto Reconnect Time	Specifies the number of seconds to wait before reconnecting after a PPPoE session is terminated.	Type a value from <b>1</b> through <b>4294947295</b> for automatic reconnection—for example, <b>100</b> seconds. Type <b>0</b> (the default) for immediate reconnection.
Idle Timeout	Specifies the number of seconds a session can be idle without disconnecting.	Type a value for the timeout. Type <b>0</b> if you do not want the session to time out.
Service Name	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.	Type the type of service provided by the access concentrator. For example, <code>video@ispl.com</code> .
Underlying Interface	Specifies the logical Ethernet interface or the logical ATM interface as the underlying interface for the PPPoE session.	From the list, select the underlying interface for the PPPoE session—for example, <code>fe-0/0/1.0</code> or <code>at-2/0/0.0</code> .

## Configuring PPPoE with a Configuration Editor

To configure PPPoE on a Services Router, you must perform the following tasks marked *(Required)*:

- Setting the Appropriate Encapsulation on the Interface (Required) on page 172
- Configuring a PPPoE Interface (Required) on page 175
- Configuring CHAP on a PPPoE Interface (Optional) on page 178

### Setting the Appropriate Encapsulation on the Interface (Required)

For PPPoE on an Ethernet interface, you must configure encapsulation on the logical interface. To configure encapsulation on an Ethernet logical interface, use PPP over Ethernet encapsulation.

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.

When you configure a point-to-point encapsulation such as PPP on a physical interface, the physical interface can have only one logical interface (only one unit statement) associated with it.

Perform the task appropriate for the interface on which you are using PPPoE:

- Configuring PPPoE Encapsulation on an Ethernet Interface on page 173
- Configuring PPPoE Encapsulation on an ATM-over-ADSL or ATM-over-SHDSL Interface on page 174

## Configuring PPPoE Encapsulation on an Ethernet Interface

Both the client and the server must be configured to support PPPoE.

To configure PPPoE encapsulation on an Ethernet 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 40.
3. If you are finished configuring the router, commit the configuration.
4. Go on to one of the following procedures:
  - To configure the PPPoE interface, see “Configuring a PPPoE Interface (Required)” on page 175.
  - To enable authentication on the interface, see “Configuring CHAP on a PPPoE Interface (Optional)” on page 178.
  - To check the configuration, see “Verifying a PPPoE Configuration” on page 180.

**Table 40: Configuring PPPoE Encapsulation on an Ethernet Interface**

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the <b>Interfaces</b> level in the configuration hierarchy.	In the configuration editor hierarchy select <b>Interfaces</b> .	From the top of the configuration hierarchy, enter  edit interfaces
Configure encapsulation on a logical Ethernet interface—for example, fe-0/0/1.0.	<ol style="list-style-type: none"> <li>1. In the Interface name box, click <b>fe-0/0/1</b>.</li> <li>2. In the Interface unit number box, click <b>0</b>.</li> <li>3. From the Encapsulation list, select <b>ppp-over-ether</b>.</li> <li>4. Click <b>OK</b>.</li> </ol>	Set PPP encapsulation on unit 0 of the Ethernet interface:  set fe-0/0/1 unit 0 encapsulation ppp-over-ether

## Configuring PPPoE Encapsulation on an ATM-over-ADSL or ATM-over-SHDSL Interface

To configure PPPoE encapsulation on an 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 41.
3. If you are finished configuring the router, commit the configuration.
4. Go on to one of the following procedures:
  - To configure the PPPoE interface, see “Configuring a PPPoE Interface (Required)” on page 175.
  - To enable authentication on the interface, see “Configuring CHAP on a PPPoE Interface (Optional)” on page 178.
  - To check the configuration, see “Verifying a PPPoE Configuration” on page 180.

**Table 41: Configuring PPPoE Encapsulation on an ATM-over-ADSL or ATM-over-SHDSL Interface**

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the <b>Interfaces</b> level in the configuration hierarchy.	In the configuration editor hierarchy select <b>Interfaces</b> .	From the top of the configuration hierarchy, enter  edit interfaces
Navigate to the ATM-over-ADSL or ATM-over-SHDSL interface—for example, <b>at-2/0/0</b> —and set the ATM virtual path identifier (VPI) to 0.	<ol style="list-style-type: none"> <li>1. In the Interface name box, click <b>at-2/0/0</b>.</li> <li>2. Next to ATM options, click <b>Configure</b>.</li> <li>3. Next to Vpi, click <b>Add new entry</b>.</li> <li>4. In the Vpi number box, type 0.</li> <li>5. Click <b>OK</b> twice.</li> </ol>	Enter  set at-2/0/0 atm-options vpi 0

**Table 41: Configuring PPPoE Encapsulation on an ATM-over-ADSL or ATM-over-SHDSL Interface (continued)**

Task	J-Web Configuration Editor	CLI Configuration Editor
Do one of the following:	To configure the ADSL operating mode on the physical ATM interface:	Enter
<ul style="list-style-type: none"> <li>Configure the ADSL operating mode on the physical ATM interface—for example, autonegotiation.</li> </ul>	<ol style="list-style-type: none"> <li>Next to Dsl options, click <b>Configure</b>.</li> <li>From the Operating mode list, select <b>auto</b>.</li> <li>Click <b>OK</b>.</li> </ol>	set at-2/0/0 dsl-options operating-mode auto
<ul style="list-style-type: none"> <li>Configure the SHDSL options:</li> </ul>	To configure the SHDSL options:	Enter
<ul style="list-style-type: none"> <li>Annex type—for example, Annex A.</li> <li>SHDSL line rate for SHDSL interface—for example, automatic selection of line rate.</li> <li>Loopback option for testing the SHDSL connection integrity on the physical ATM interface—for example, local.</li> </ul>	<ol style="list-style-type: none"> <li>Next to Shdsl options, click <b>Configure</b>.</li> <li>From the Annex list, select <b>Annex-a</b>.</li> <li>From the Line Rate list, select <b>auto</b>.</li> <li>From the Loopback list, select <b>local</b>.</li> <li>Click <b>OK</b> until you return to the Interfaces page.</li> </ol>	set at-2/0/0 shdsl-options annex annex-a line-rate auto loopback local
Configure Ethernet over ATM encapsulation on the physical ATM-over-ADSL or ATM-over-SHDSL interface.	From the Encapsulation list, select <b>ethernet-over-atm</b> .	Enter  set at-2/0/0 encapsulation ethernet-over-atm
Create an ATM-over-ADSL or ATM-over-SHDSL logical interface, configure LLC encapsulation, and specify a VCI number.	<ol style="list-style-type: none"> <li>Next to Unit, click <b>Add new entry</b>.</li> <li>In the Interface unit number box, type 0.</li> <li>From the Encapsulation list, select <b>ppp-over-ether-over-atm-llc</b>.</li> <li>In the Multicast vci box, type 0.120 and click <b>OK</b>.</li> </ol>	Enter  set at-2/0/0 unit 0 encapsulation ppp-over-ether-over-atm-llc vci 0.120

### Configuring a PPPoE Interface (Required)

To create and configure a PPPoE interface over the underlying Fast Ethernet and ATM interface:

- Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
- Perform the configuration tasks described in Table 42.
- If you are finished configuring the router, commit the configuration.
- Go on to one of the following procedures:

- To enable authentication on the PPPoE interface, see “Configuring CHAP on a PPPoE Interface (Optional)” on page 178.
- To check the configuration, see “Verifying a PPPoE Configuration” on page 180.

**Table 42: Configuring a PPPoE Interface**

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the <b>Interfaces</b> level in the configuration hierarchy.	In the configuration editor hierarchy select <b>Interfaces</b> .	From the top of the configuration hierarchy, enter  edit interfaces
Create a PPPoE interface with a logical interface unit 0.	<ol style="list-style-type: none"> <li>1. Next to Interface, click <b>Add new entry</b>.</li> <li>2. In the Interface name box, type <b>pp0</b> and click <b>OK</b>.</li> <li>3. Under Interface name, click <b>pp0</b>.</li> <li>4. Next to Unit, click <b>Add new entry</b>.</li> <li>5. In the Interface unit number box, type 0.</li> </ol>	Enter  edit pp0 unit 0
Configure an ISDN interface as the backup interface for the PPPoE interface—for example, <b>dl0.0</b> .	<ol style="list-style-type: none"> <li>1. Next to Backup options, click <b>Configure</b>.</li> <li>2. In the Interface box, type <b>dl0.0</b>.</li> <li>3. Click <b>OK</b>.</li> </ol>	Enter  set backup-options interface dl0.0
Specify the logical Ethernet interface or the logical ATM interface as the underlying interface for the PPPoE session—for example, <b>fe-0/0/1.0</b> or <b>at-2/0/0.0</b> .	<ol style="list-style-type: none"> <li>1. Next to Pppoe options, click <b>Edit</b>.</li> <li>2. In the Underlying Interface box, type one of the following interface names: <ul style="list-style-type: none"> <li>■ For a logical Ethernet interface, type <b>fe-0/0/1.0</b>.</li> <li>■ For a logical ATM interface type, <b>at-2/0/0.0</b>.</li> </ul> </li> </ol>	Enter one of the following commands: <ul style="list-style-type: none"> <li>■ set pppoe-options underlying-interface fe-0/0/1.0.</li> <li>■ set pppoe-options underlying-interface at-2/0/0.0.</li> </ul>
Identify the access concentrator by a unique name—for example, <b>ispl.com</b> .	In the Access concentrator box type <b>ispl.com</b> .	Enter  set pppoe-options access-concentrator ispl.com
Specify the number of seconds (from 1 through 4294967295) to wait before reconnecting after a PPPoE session is terminated—for example, <b>100</b> . A 0 value (the default) specifies immediate reconnection.	In the Auto reconnect box, type <b>100</b> .	Enter  set pppoe-options auto-reconnect 100
Specify the number of seconds a session can be idle—for example, <b>100</b> . A 0 value prevents the session from timing out.	In the Idle timeout box, type <b>100</b> .	Enter  set pppoe-options idle-timeout 100.

**Table 42: Configuring a PPPoE Interface (continued)**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
Specify the J-Series Services Router as the client for the PPPoE interface.	In the Client box, <b>Yes</b> .	Enter  set pppoe-options client.
Identify the type of service provided by the access concentrator, such as the name of the Internet service provider (ISP), class, or quality of service—for example, video@ispl.com.	<ol style="list-style-type: none"> <li>In the Service name box, type video@ispl.com.</li> <li>Click <b>OK</b>.</li> </ol>	Enter  set pppoe-options service-name video@ispl.com
Configure the maximum transmission unit (MTU) of the IPv4, IPv6, or Multiprotocol Label Switching (MPLS) protocol families—for example, 1492.	<ol style="list-style-type: none"> <li>Select one of the following protocol families: <ul style="list-style-type: none"> <li>For the IPv4 family, in the Inet box, select <b>Yes</b> and click <b>Configure</b>.</li> <li>For the IPv6 family, in the Inet6 box, select <b>Yes</b> and click <b>Configure</b>.</li> <li>For the MPLS family, in the Mpls box, select <b>Yes</b> and click <b>Configure</b>.</li> </ul> </li> <li>In the Mtu box, type 1492.</li> <li>Click <b>OK</b> until you return to the Unit page.</li> </ol>	Enter one of the following: <ul style="list-style-type: none"> <li>set family inet mtu 1492</li> <li>set family inet6 mtu 1492</li> <li>set family mpls mtu 1492</li> </ul>

**Table 42: Configuring a PPPoE Interface (continued)**

Task	J-Web Configuration Editor	CLI Configuration Editor
<p>Configure the PPPoE logical interface address in one of the following ways:</p> <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>■ Assign IPv4 or IPv6 source and destination addresses—for example: <ul style="list-style-type: none"> <li>■ 192.168.1.1/32 and 192.168.1.2 for IPv4</li> <li>■ 2004:1/128 and 2004:2 for IPv6.</li> </ul> </li> <li>■ Derive the IPv4 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.</li> <li>■ Obtain an IP address by negotiation with the remote end. This method might require the access concentrator to use a RADIUS authentication server.</li> </ul>	<p>Select one of the following IP address configurations:</p> <p>To assign the source and destination addresses:</p> <ol style="list-style-type: none"> <li>Next to Address, click <b>Add new entry</b>.</li> <li>In the Inet Source box, type <b>192.168.1.1/32</b>, or in the Inet6 Source box, type <b>2004::1/128</b>.</li> <li>In the Inet Destination box, type <b>192.168.1.2</b>, or in the Inet6 Destination box, type <b>2004::2</b>.</li> <li>Click <b>OK</b> until you return to the Unit page.</li> </ol> <p>To derive the IPv4 source address and assign the destination address:</p> <ol style="list-style-type: none"> <li>Next to Inet, click <b>Edit</b>.</li> <li>Next to Unnumbered address, select the <b>Yes</b> check box and click <b>Configure</b>.</li> <li>In the Destination box, type <b>192.168.1.2</b>.</li> <li>In the Source box, type <b>lo0.0</b>.</li> <li>Click <b>OK</b> until you return to the Unit page.</li> </ol> <p>To obtain an IP address from the remote end:</p> <ol style="list-style-type: none"> <li>Next to Negotiate address, select the <b>Yes</b> check box.</li> <li>Click <b>OK</b> until you return to the Unit page.</li> </ol>	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>■ To assign source and destination addresses enter one of the following sets of commands: <ul style="list-style-type: none"> <li>■ For IPv4 addresses, <b>set family inet address 192.168.1.1/32 destination 192.168.1.2</b>.</li> <li>■ For IPv6 addresses, <b>set family inet6 address 2004::1/128 destination 2004::2</b>.</li> </ul> </li> <li>■ To derive the IPv4 source address and assign the destination address, enter <b>set family inet unnumbered-address lo0.0 destination 192.168.1.2</b>.</li> <li>■ To obtain an IP address from the remote end, enter <b>set family inet negotiate-address</b>.</li> </ul>
<p>Disable the sending of keepalives on a logical interface.</p>	<ol style="list-style-type: none"> <li>From the Keepalive choices list, select <b>no keepalives</b>.</li> <li>Click <b>OK</b> to apply your entries to the configuration.</li> </ol>	<p>Enter</p> <p><b>set no-keepalives</b></p>

To clear a PPPoE session on the pp0.0 interface, enter the **clear pppoe sessions pp0.0** command. To clear all sessions on the PPPoE interface, enter the **clear pppoe sessions** command.

### Configuring CHAP on a PPPoE Interface (Optional)

To configure CHAP on the PPPoE interface:

- Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
- Perform the configuration tasks described in Table 43.



3. If you are finished configuring the router, commit the configuration.
4. To check the configuration, see “Verifying a PPPoE Configuration” on page 180.

**Table 43: Configuring CHAP on a PPPoE Interface**

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the <b>Profile</b> level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>1. In the configuration hierarchy, select <b>Configuration &gt; Edit Configuration &gt; View and Edit</b>.</li> <li>2. Next to Access, click <b>Configure</b> or <b>Edit</b>.</li> </ol>	<p>Enter</p> <pre>set access profile A-ppp-client client client1 chap-secret my-secret</pre>
Define a CHAP access profile—for example, <b>A-ppp-client</b> —with a client named <b>client 1</b> and the secret (password) <b>my-secret</b> .	<ol style="list-style-type: none"> <li>1. Next to Profile, click <b>Add new entry</b>.</li> <li>2. In the Profile name box, type <b>A-ppp-client</b>.</li> <li>3. Next to Client, click <b>Add new entry</b>.</li> <li>4. In the Name box, type <b>client1</b>.</li> <li>5. In the Chap secret box, type <b>my-secret</b>.</li> <li>6. Click <b>OK</b> until you return to the Configuration page.</li> </ol>	
Navigate to the <b>pp0 unit 0</b> interface level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>1. In the configuration hierarchy, select <b>Interfaces</b>.</li> <li>2. In the Interface name box, click <b>pp0</b>.</li> <li>3. In the Interface unit number box, click <b>0</b>.</li> </ol>	<p>From the top of the configuration hierarchy, enter</p> <pre>edit interfaces pp0 unit 0</pre>
Configure CHAP on the PPPoE interface, and specify a unique profile name containing a client list and access parameters—for example, <b>A-ppp-client</b> .	<ol style="list-style-type: none"> <li>1. Next to Ppp options, click <b>Configure</b>.</li> <li>2. Next to Chap, click <b>Configure</b>.</li> <li>3. In the Access profile box, type <b>A-ppp-client</b>.</li> </ol>	<p>Enter</p> <pre>set ppp-options chap access-profile A-ppp-client</pre>
Specify a unique hostname to be used in CHAP challenge and response packets—for example, <b>A-fe-0/0/1.0</b> or <b>A-at-2/0/0.0</b> .	<p>In the Local name box, type one of the following:</p> <ul style="list-style-type: none"> <li>■ For an Ethernet interface, type <b>A-fe-0/0/1.0</b>.</li> <li>■ For an ATM interface, type <b>A-at-2/0/0.0</b>.</li> </ul>	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>■ For the Ethernet interface, enter <b>set ppp-options chap local-name A-fe-0/0/1.0</b>.</li> <li>■ For the ATM interface, enter <b>set ppp-options chap local-name A-at-2/0/0.0</b>.</li> </ul>
Set the <b>passive</b> option to handle incoming CHAP packets only.	<ol style="list-style-type: none"> <li>1. In the Passive box, click <b>Yes</b>.</li> <li>2. Click <b>OK</b>.</li> </ol>	<p>Enter</p> <pre>set ppp-options chap passive</pre>

## Verifying a PPPoE Configuration

---

To verify PPPoE configuration perform the following tasks:

- Displaying a PPPoE Configuration for an Ethernet Interface on page 180
- Displaying a PPPoE Configuration for an ATM-over-ADSL or ATM-over-SHDSL Interface on page 181
- Verifying PPPoE Interfaces on page 182
- Verifying PPPoE Sessions on page 183
- Verifying the PPPoE Version on page 183
- Verifying PPPoE Statistics on page 184

### *Displaying a PPPoE Configuration for an Ethernet Interface*

**Purpose** Verify the PPPoE configuration for an Ethernet interface.

**Action** From the J-Web interface, select **Configuration > View and Edit > View Configuration Text**. Alternatively, from configuration mode in the CLI, enter the show interfaces command from the top level.

**Sample Output**

```
[edit]
user@host#show interfaces
fe-3/0/0 {
    unit 1{
    }
}
pp0 {
    unit 1{
        pppoe-options {
            underlying-interface fe-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;
            }
        }
    }
}
```

```
}

```

**What It Means** Verify that the output shows the intended configuration of PPPoE. For more information about the format of a configuration file, see “Viewing the Configuration Text” on page 8.

### ***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 **Configuration > View and Edit > View Configuration Text**. Alternatively, from configuration mode in the CLI, enter the show interfaces command from the top level.

**Sample Output**

```
[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;
    }
}
```

**What It Means** Verify that the output shows the intended configuration of PPPoE. For more information about the format of a configuration file, see “Viewing the Configuration Text” on page 8.

## Verifying PPPoE Interfaces

**Purpose** Verify that the PPPoE router 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: ispl.com, AC MAC address: 00:90:1a:40:f6:4c,
  Service name: video@ispl.com, Configured AC name: ispl.com,
  Auto-reconnect timeout: 60 seconds
  Underlying interface: fe-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
NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured, mpls:
Not-configured
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
```

**What It Means** 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—for example, `fe-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`.

For more information about the `show interfaces pp0` command, see the *JUNOS Interfaces Command Reference*.

## Verifying PPPoE Sessions

<b>Purpose</b>	Verify that a PPPoE session is running properly on the logical interface.
<b>Action</b>	From the CLI, enter the <code>show pppoe interfaces</code> command.
<b>Sample Output</b>	<pre> user@host&gt; show pppoe interfaces  pp0.0 Index 67   State: Session up, Session ID: 31,   Service name: video@ispl.com, Configured AC name: ispl.com,   Session AC name: belur, AC MAC address: 00:90:1a:40:f6:4e,   Auto-reconnect timeout: 1 seconds,   Underlying interface: fe-0/0/1.0 Index 69           </pre>
<b>What It Means</b>	<p>The output shows information about the PPPoE sessions. Verify the following information:</p> <ul style="list-style-type: none"> <li>■ The PPPoE session is running on the correct logical interface.</li> <li>■ Under <b>State</b>, the session is active (up).</li> <li>■ Under <b>Underlying interface</b>, the physical interface on which the PPPoE session is running is correct:               <ul style="list-style-type: none"> <li>■ For an Ethernet connection, the underlying interface is Fast Ethernet—for example, <code>fe-0/0/1.0</code>.</li> <li>■ For an ATM-over-ADSL or ATM-over-SHDSL connection, the underlying interface is ATM—for example, <code>at-2/0/0.0</code>.</li> </ul> </li> </ul>

For more information about the `show pppoe interfaces` command, see the *JUNOS Interfaces Command Reference*.

## Verifying the PPPoE Version

<b>Purpose</b>	Verify the version information of the PPPoE protocol configured on the Services Router 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

```

**What It Means** 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.

For more information about the show pppoe version command, 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
  PacketType      Sent      Received
  PADI            502         0
  PADO             0        219
  PADR            219         0
  PADS             0        219
  PADT             0        161
  Service name error  0         0
  AC system error    0         13
  Generic error      0         0
  Malformed packets  0         41
  Unknown packets    0         0
Timeout
  PADI            42
  PADO             0
  PADR             0

```

**What It Means** 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.

For more information about the `show pppoe statistics` command, see the *JUNOS Interfaces Command Reference*.





## Chapter 6

# Configuring ISDN

ISDN connectivity is supported on the J-series Services Routers as a backup for a primary Internet connection. The J-series Services Routers can be configured to “fail over” to an ISDN interface when the primary connection experiences interruptions in Internet connectivity.

You can use either J-Web Quick Configuration or a configuration editor to configure ISDN interfaces.

This chapter contains the following topics:

- ISDN Terms on page 187
- ISDN Overview on page 189
- Before You Begin on page 190
- Configuring ISDN Interfaces with Quick Configuration on page 191
- Configuring ISDN Interfaces with a Configuration Editor on page 198
- Verifying the ISDN Configuration on page 222

## ISDN Terms

Before configuring ISDN, become familiar with the terms defined in Table 44.

**Table 44: ISDN Terminology**

Term	Definition
bandwidth on demand	ISDN cost-control feature defining the bandwidth threshold that must be reached on all links before a Services Router initiates additional ISDN data connections to provide more bandwidth.
basic rate interface (BRI)	ISDN interface intended for home and small enterprise applications, BRI consists of two 64-Kbps B-channels and one 16-Kbps D-channel.
bearer channel (B-channel)	Channel that carries voice or data on an ISDN interface.

**Table 44: ISDN Terminology (continued)**

<b>Term</b>	<b>Definition</b>
<b>callback</b>	Alternative feature to dial-in that enables a J-series Services Router 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 router rejects the call, waits a configured period of time, and calls a number configured on the router's dialer interface. See also <i>dial-in</i> .
<b>caller ID</b>	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 router 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.
<b>delta-channel (D-channel)</b>	Channel that carries control and signaling information on an ISDN interface.
<b>demand circuit</b>	Interface 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.
<b>dial backup</b>	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.
<b>dialer filter</b>	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 router receives a packet for that address, the dialer interface initiates an ISDN backup connection and sends the packet over it. See also <i>dial-on-demand routing backup</i> ; <i>floating static route</i> .
<b>dial-in</b>	Feature that enables J-series Services Routers 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 router's dialer interface. See also <i>callback</i> .
<b>dialer interface (dl)</b>	Logical interface for configuring dialing properties and the control interface for a backup ISDN connection.
<b>dial-on-demand routing (DDR) backup</b>	<p>Feature that provides a J-series Services Router with full-time connectivity across an ISDN line.</p> <p>When routes on a primary serial T1, E1, T3, E3, Fast Ethernet, or PPPoE interface are lost, an ISDN dialer interface establishes a backup connection. To save connection time costs, the Services Router drops the ISDN connection after a configured period of inactivity. Services Routers with ISDN interfaces support two types of dial-on-demand routing backup: on-demand routing with a dialer filter and dialer watch. See also <i>dialer filter</i>; <i>dialer watch</i>.</p>
<b>dialer profile</b>	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.

**Table 44: ISDN Terminology (continued)**

Term	Definition
dialer watch	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 <i>dial-on-demand routing backup</i> .
floating static route	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.
Integrated Services Digital Network (ISDN)	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.
service profile identifier (SPID)	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.
terminal endpoint identifier (TEI)	Number that identifies a terminal endpoint, an ISDN-capable device attached to an ISDN network through an ISDN interface on the Services Router. 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.

## 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: a physical interface and a logical interface called the dialer interface.

ISDN provides a Services Router with a backup connection for network interfaces.

## ISDN Interfaces

There are four types of interfaces available for ISDN connectivity:

- 1-port S/T interface supporting ITU-T I.430, ETSI TS 101080, and GR-1089-Core Type III built into a J2300 Services Router with additional network interfaces.

- 1-port U interface supporting ANSI T.601 and GR-1089-Core built into a J2300 Services Router with additional network interfaces.
- 4-port S/T PIM supporting ITU-T I.430, ETSI TS 101080, and GR-1089-Core Type III as a field-replaceable unit (FRU) on J4300 and J6300 Services Routers.
- 4-port U PIM supporting ANSI T.601 and GR-1089-Core as a FRU on J4300 and J6300 Services Routers.

Each ISDN physical interface uses the naming convention `br-pim/0/port`.

Each B-channel is identified by `bc-pim/0/port:channel`, where *channel* represents the B-channel ID and has a value of 1 or 2.

The D-channel is identified by `dc-pim/0/port`.



**NOTE:** The B- and D-channel interfaces do not have any configurable parameters. However, when interface statistics are displayed, the B- and D-channel interfaces list statistical values.

---

The dialer interface, `dl n`, is a logical interface for configuring 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 cannot be configured simultaneously in the following modes:

- As a backup interface and a dialer filter
- As a backup interface and dialer watch interface
- As a dialer watch interface and a dialer filter
- As a backup interface for more than one primary interface

## Before You Begin

---

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

- Install Services Router hardware. For more information, see the *J-series Services Router Getting Started Guide*.
- Establish basic connectivity. For more information, see the *J-series Services Router Getting Started Guide*.

- 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 39.

Although it is not a requirement, you may also want to plan how you are going to use the ISDN interfaces on your network before you begin configuring them. You can see a list of ISDN interfaces by displaying the **Configuration > Quick Configuration > Interfaces** page.

## Configuring ISDN Interfaces with Quick Configuration

---

You can use the ISDN Interfaces Quick Configuration pages to configure ISDN interfaces on a router. The Quick Configuration pages allow you to configure ISDN connectivity on a router to back up a primary Internet connection.

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 Physical Interfaces with Quick Configuration on page 191
- Configuring ISDN Dialer Interfaces with Quick Configuration on page 194

### Configuring ISDN Physical Interfaces with Quick Configuration

To configure ISDN physical interfaces with Quick Configuration:

1. In the J-Web interface, select **Configuration > Quick Configuration > Interfaces**.  
A list of network interfaces installed on the router is displayed.
2. Click the *br-pim / 0 / port* interface name for the ISDN port you want to configure.

The ISDN Physical Interface Quick Configuration page is displayed as shown in Figure 34.

**Figure 34: ISDN Physical Interface Quick Configuration Page**

The screenshot shows the Juniper J6300 router configuration interface. The top navigation bar includes 'Monitor', 'Configuration', 'Diagnose', 'Manage', and 'Alarms'. The 'Configuration' tab is active, and the left sidebar shows 'Quick Configuration' with options like 'Set Up', 'Secure Access', 'Interfaces', 'Users', 'SNMP', 'Routing and Protocols', 'Class of Service', 'Firewall/NAT', 'DHCP', 'IPSec Tunnels', 'Realtime Performance Monitoring', and 'Firewall Filters'. The 'Interfaces' option is selected. The main content area is titled 'Quick Configuration' and 'Interfaces'. It shows the 'Physical Interface: 'br-6/0/0'' and fields for 'Physical Interface Description', 'Clocking' (set to 'internal'), and 'ISDN Options'. The 'ISDN Options' section includes fields for 'Calling Number', 'ISDN Switch Type' (set to 'nil'), 'Service Profile Identifier', 'Service Profile Identifier 2', 'Static TEI Value', 'TEI Option', and 'Timer T310 Value'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

3. Enter information into the ISDN Quick Configuration pages, as described in Table 45.
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 Dialer Interfaces with Quick Configuration” on page 194.

**Table 45: ISDN Quick Configuration Page Summary**

Field	Function	Your Action
<b>Configuring ISDN Interfaces</b>		

**Table 45: ISDN Quick Configuration Page Summary (continued)**

Field	Function	Your Action
Physical Interface Description	(Optional) Adds supplemental information about the ISDN physical interface on the router.	Type a text description of the physical ISDN interface in the box to clearly identify it in monitoring displays.
Clocking	<p>Enables internal or external clocking sources for the interface on the router.</p> <ul style="list-style-type: none"> <li>■ <b>internal</b>—Services Router's own system clock (the default)</li> <li>■ <b>external</b>—Clock received from the T1 interface</li> </ul>	Select <b>internal</b> or <b>external</b> from the list.
<b>Dialer Pool Options</b>		
Dialer Pools	Displays the list of configured ISDN dialer pools on the router.	<ul style="list-style-type: none"> <li>■ To add a dialer pool to the interface, click <b>Add</b>.</li> <li>■ To edit a dialer pool, select the name from the list. You can change the priority, but not the name.</li> <li>■ To delete a dialer pool, select the check box and click <b>Delete</b>.</li> </ul>
Dialer Pool Name (required)	Specifies the group of physical interfaces to be used by the dialer interface.	Type the dialer pool name—for example, <b>isdn-dialer-pool</b> .
Priority	Specifies the priority of this interface within the dialer pool. Interfaces with a higher priority are the first to interact with the dialer interface.	<ol style="list-style-type: none"> <li>1. Type a priority value from 0 (lowest) to 255 (highest). The default is 0.</li> <li>2. Click <b>OK</b> to return to the Quick Configuration page.</li> </ol>
<b>ISDN Options</b>		
Calling Number	Configures the dialing number used to connect with the service provider.	Type the outgoing calling number for the service provider.
ISDN Switch Type	Specifies the type of ISDN switch used by the service provider.	<p>Select one of the following switch types:</p> <ul style="list-style-type: none"> <li>■ <b>att5e</b>—AT&amp;T 5ESS</li> <li>■ <b>etsi</b>—NET3 for the UK and Europe</li> <li>■ <b>ni1</b>—National ISDN-1</li> <li>■ <b>ntdms-100</b>—Northern Telecom DMS-100</li> <li>■ <b>ntt</b>—NTT Group switch for Japan</li> </ul>
Service Profile Identifier Service Profile Identifier 2	Configures the service profile identifier (SPID) provided by your ISDN service.	Type the SPID in the box. If you have a NTDMS-100 or NI1 switch, an additional SPID field is provided.

**Table 45: ISDN Quick Configuration Page Summary (continued)**

<b>Field</b>	<b>Function</b>	<b>Your Action</b>
Static TEI Value	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 Services Router. 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 <b>0</b> and <b>63</b> . If this value is not supplied, the router dynamically acquires a TEI.  If you configured more than one SPID, the TEI must be acquired dynamically.
TEI Option	Configures when the TEI negotiates with the ISDN provider.	<ul style="list-style-type: none"> <li>■ Select <b>first-call</b> to activate the connection when the call setup is sent to the ISDN provider.</li> <li>■ Select <b>power-up</b> (the default) to activate the connection when the router is powered on.</li> </ul>
Timer T310 Value	Sets the Q.931 timer value in seconds.	Type a value between <b>1</b> and <b>65536</b> . The default value is <b>10</b> seconds.

### **Configuring ISDN Dialer Interfaces with Quick Configuration**

When ISDN interfaces are installed on the Services Router, links to ISDN Quick Configuration pages for dialer options are displayed on the Interfaces Quick Configuration page as shown in Figure 35.

You can use these Quick Configuration pages to configure a 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.



Figure 35: ISDN Dialer Options Quick Configuration Page

Juniper NETWORKS ROUTER - J6300

Logged in as: regress  
[Help](#) [About](#) [Logout](#)

Monitor Configuration Diagnose Manage **Alarms**

Configuration > Quick Configuration > Interfaces

**Quick Configuration**

**Interfaces**

Interface Name	Link State	Configured	Description
<a href="#">fe-0/0/0</a>	Up	Yes	Fast Ethernet Interface 'fe-0/0/0'
<a href="#">fe-0/0/0.0</a>	Up	Yes	Logical Unit 0 on Fast Ethernet Interface 'fe-0/0/0'
<a href="#">fe-0/0/1</a>	Up	Yes	Fast Ethernet Interface 'fe-0/0/1'
<a href="#">fe-0/0/1.0</a>	Up	Yes	Logical Unit 0 on Fast Ethernet Interface 'fe-0/0/1'
<a href="#">fe-5/0/0</a>	Down	Yes	Fast Ethernet Interface 'fe-5/0/0'
<a href="#">fe-5/0/0.0</a>	Down	Yes	Logical Unit 0 on Fast Ethernet Interface 'fe-5/0/0'
<a href="#">fe-5/0/1</a>	Down	Yes	Fast Ethernet Interface 'fe-5/0/1'
<a href="#">fe-5/0/1.0</a>	Down	Yes	Logical Unit 0 on Fast Ethernet Interface 'fe-5/0/1'
<a href="#">br-6/0/0</a>	Up	Yes	ISDN BRI Interface 'br-6/0/0'
<a href="#">br-6/0/1</a>	Up	No	ISDN BRI Interface 'br-6/0/1'
<a href="#">br-6/0/2</a>	Down	No	ISDN BRI Interface 'br-6/0/2'
<a href="#">br-6/0/3</a>	Down	No	ISDN BRI Interface 'br-6/0/3'
<a href="#">lo0</a>	Up	Yes	Loopback Interface 'lo0'
<a href="#">lo0.0</a>	Up	Yes	Logical Unit 0 on Loopback Interface 'lo0'
<a href="#">pp0</a>	Up	No	Point-to-Point Protocol over Ethernet Interface 'pp0'

► **ISDN Dialer Options**  
 Configure ISDN Dialer features Dial Backup, Dial Watch, and Dial on Demand.

To configure ISDN interfaces with Quick Configuration:

- In the J-Web interface, select **Configuration > Quick Configuration > Interfaces**.  
 A list of network interfaces installed on the Services Router is displayed.
- Click **ISDN Dialer Options** under the interfaces list.
- 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 serial 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.
  - 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 36 shows the ISDN Quick Configuration page for dialer logical interfaces.

**Figure 36: ISDN Dialer Interface Quick Configuration Page**

Juniper NETWORKS ROUTER - J6300

Logged in as: regress [Help](#) [About](#) [Logout](#)

Monitor Configuration Diagnose Manage **Alarms**

Configuration > Quick Configuration > Interfaces

### Quick Configuration

#### Interfaces

**Dialer Logical Interface: 'dl0.0'**

**Logical Interface Description**

**IPv4 Addresses and Prefixes**

---

#### Dialer Options

**Activation Delay**  

**Deactivation Delay**  

**\* Dial String**

**\* Pool**  


---

#### Backup Interface

**Interface to Backup**

5. Enter information into the ISDN Quick Configuration page for dialer logical interfaces, as described in Table 46.
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 222.

**Table 46: ISDN Dialer Interface Quick Configuration Page Summary**

Field	Function	Your Action
<b>Configuring Dialer Interfaces</b>		
Logical Interface Description	Describes the logical interface.	Type a text description of the interface in the box.
IPv4 Addresses and Prefixes	Displays the IPv4 addresses for the interfaces to which the dialer interface is assigned.	Type an IP address and a prefix in the boxes. Click <b>Add</b> .  To delete an IP address, highlight it in the list, and click <b>Delete</b> .
<b>Dialer Options</b>		
Activation Delay	Displays the time to wait before activating the backup interface once the primary interface is down.	Type a value, in seconds—for example, 30.  The default value is 0 seconds with a maximum value of 60 seconds.
Deactivation Delay	Displays the time to wait before deactivating the backup interface once the primary interface is up.	Type a value, in seconds—for example, 30.  The default value is 0 seconds with a maximum value of 60 seconds.
Dial String (required)	Displays the dialing number from your ISDN service provider.	Type the dialing number and click <b>Add</b> .  To delete a dial string, highlight it and click <b>Delete</b> .
Pool (required)	Displays a list of dialer pools configured on br interfaces.	Select a dialer pool from the list.
<b>Backup Interface (for dial backup only)</b>		
Interface to Backup	Displays a list of interfaces for ISDN backup.	Select an interface from the list for ISDN backup.

**Table 46: ISDN Dialer Interface Quick Configuration Page Summary (continued)**

Field	Function	Your Action
<b>Dialer Watch List (for dialer watch only)</b>		
IPv4 Addresses and Prefixes	Displays the IPv4 addresses in the list of routes to be monitored by the dialer interface.	Type an IP address and a prefix in the boxes. Click <b>Add</b> .  To delete an IP address, highlight it in the list, and click <b>Delete</b> .

## Configuring ISDN Interfaces with a Configuration Editor

To configure ISDN interfaces to back up primary serial interfaces on a Services Router, perform the following tasks marked (*Required*) and then configure a backup method—either dial backup, a dialer filter, or dialer watch. Perform other tasks if needed on your network.

- Adding an ISDN Interface (*Required*) on page 198
- Configuring a Dialer Interface (*Required*) on page 201
- Configuring Dial Backup on page 204
- Configuring a Dialer Filter for Dial-on-Demand Routing Backup on page 205
- Configuring Dialer Watch on page 207
- Configuring Dial-on-Demand Routing Backup with OSPF Support (*Optional*) on page 209
- Configuring Bandwidth on Demand (*Optional*) on page 210
- Configuring Dial-In and Callback (*Optional*) on page 215
- Configuring Dialer Profiles (*Optional*) on page 220

### Adding an ISDN Interface (*Required*)

To enable ISDN interfaces installed on your Services Router to work properly, you must configure the interface properties.

To configure an ISDN network interface for the Services Router:

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 47.
3. Go on to “Configuring a Dialer Interface (*Required*)” on page 201.

**Table 47: Adding an ISDN Interface**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
Navigate to the <b>Interfaces</b> level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to Interfaces, click <b>Configure</b> or <b>Edit</b>.</li> </ol>	<p>From the top of the configuration hierarchy, enter</p> <pre>edit interfaces br-1/0/3</pre>
Create the new interface—for example, br-1/0/3.	<ol style="list-style-type: none"> <li>1. Next to Interface, click <b>Add new entry</b>.</li> <li>2. In the Interface name box, type the name of the new interface, br-1/0/3.</li> <li>3. Click <b>OK</b>.</li> </ol>	
<p>Configure dialer options.</p> <ul style="list-style-type: none"> <li>■ Name the dialer pool—for example, ISDN-dialer-group.</li> <li>■ Set the dialer pool priority—for example, 25.</li> </ul> <p>Dialer pool priority has a range from 1 to 255, with 1 designating lowest-priority interfaces and 255 designating the highest-priority interfaces.</p>	<ol style="list-style-type: none"> <li>1. In the Encapsulation column, next to the new interface, click <b>Edit</b>.</li> <li>2. Next to Dialer options, select <b>Yes</b>, and then click <b>Configure</b>.</li> <li>3. Next to Pool, click <b>Add new entry</b>.</li> <li>4. In the Pool identifier box, type isdn-dialer-group.</li> <li>5. In the Priority box, type 25.</li> <li>6. Click <b>OK</b>.</li> </ol>	<p>From the [edit interfaces br-1/0/3] hierarchy, enter</p> <pre>set dialer-options pool isdn-dialer-group priority 25</pre>

**Table 47: Adding an ISDN Interface (continued)**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
<p>Configure ISDN properties.</p> <ul style="list-style-type: none"> <li>■ Calling number of your ISDN provider—for example, 18005555555.</li> <li>■ Service provider ID (SPID)—for example, 00108005555555.</li> <li>■ Static TEI between 0 and 63 from your service provider—for example, 23. If the field is left blank, the Services Router dynamically acquires a TEI. Also, if you have configured a second SPID, you cannot set a static TEI value.</li> </ul> <p>If you have a NTDMS-100 or NI1 switch, an additional box for a service provider ID is provided.</p> <p>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.</p> <ul style="list-style-type: none"> <li>■ Incoming called number—for example, 18883333456.</li> </ul> <p>Configure incoming call properties if you have remote locations dialing into the router through the ISDN interface.</p>	<ol style="list-style-type: none"> <li>1. Next to Isdn options, click <b>Configure</b>.</li> <li>2. In the Calling number box, type 18005555555.</li> <li>3. In the Spid1 box, type 00108005555555.</li> <li>4. In the Static tei val box, type 23.</li> <li>5. Next to Incoming called number, click <b>Add new entry</b>.</li> <li>6. In the Called number box, type 18883333456.</li> <li>7. Click <b>OK</b>.</li> </ol>	<ol style="list-style-type: none"> <li>1. To set the ISDN options, enter  <pre>set isdn-options calling-number 18005555555</pre> </li> <li>2. Enter  <pre>set isdn-options spid1 00108005555555</pre> </li> <li>3. Enter  <pre>set isdn-options static-tei-val 23</pre> </li> <li>4. <pre>set isdn-options incoming-called-number 18883333456</pre></li> </ol>
<p>Select the type of ISDN switch—for example, <b>att5e</b>. The following switches are compatible with Services Routers:</p> <ul style="list-style-type: none"> <li>■ <b>att5e</b>—AT&amp;T 5ESS</li> <li>■ <b>etsi</b>—NET3 for the UK and Europe</li> <li>■ <b>ni1</b>—National ISDN-1</li> <li>■ <b>ntdms-100</b>—Northern Telecom DMS-100</li> <li>■ <b>ntt</b>—NTT Group switch for Japan</li> </ul>	<p>From the Switch type list, select <b>att5e</b>.</p>	<p>To select the switch type, enter</p> <pre>set isdn-options switch-type att5e</pre>

**Table 47: Adding an ISDN Interface (continued)**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
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 <b>10</b> seconds, but can be configured between <b>1</b> and <b>65536</b> seconds—for example, <b>15</b> .	<ol style="list-style-type: none"> <li>1. In the T306 box, type <b>15</b>.</li> <li>2. In the T310 box, type <b>15</b>.</li> </ol>	<ol style="list-style-type: none"> <li>1. Enter  <code>set isdn-options t306 15</code></li> <li>2. Enter  <code>set isdn-options t310 15</code></li> </ol>
Configure when the TEI negotiates with the ISDN provider. <ul style="list-style-type: none"> <li>■ <b>first-call</b>—Activation does not occur until a call is sent.</li> <li>■ <b>power-up</b>—Activation occurs when the Services Router is powered on. This is the default value.</li> </ul>	<ol style="list-style-type: none"> <li>1. From the Tei option list, select <b>power-up</b>.</li> <li>2. Click <b>OK</b> to return to the Interfaces page.</li> </ol>	To initiate activation at power-up, enter  <code>set isdn-options tei-option power-up</code>

### **Configuring a Dialer Interface (Required)**

The dialer interface (di) is a logical interface configured to establish ISDN connectivity. You can configure multiple dialer interfaces for different functions on the Services Router.

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 Services Router:

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 48.
3. To configure a backup method, go on to one of the following tasks:
  - “Configuring Dial Backup” on page 204.
  - “Configuring a Dialer Filter for Dial-on-Demand Routing Backup” on page 205.
  - “Configuring Dialer Watch” on page 207.

**Table 48: Adding a Dialer Interface to a Services Router**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
Navigate to the <b>Interfaces</b> level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to Interfaces, click <b>Configure</b> or <b>Edit</b>.</li> </ol>	From the top of the configuration hierarchy, enter edit interfaces
Create the new interface—for example, <b>d10</b> .  Adding a description can differentiate between different dialer interfaces—for example, <b>T1-backup</b> .	<ol style="list-style-type: none"> <li>1. Next to Interface, click <b>Add new entry</b>.</li> <li>2. In the Interface name box, type <b>d10</b>.</li> <li>3. In the Description box, type <b>T1-backup</b>.</li> <li>4. Click <b>OK</b>.</li> </ol>	Create and name the interface:  <ol style="list-style-type: none"> <li>1. <b>edit d10</b></li> <li>2. <b>set description T1-backup</b></li> </ol>
Configure encapsulation options—for example, <b>cisco-hdlc</b> .  <ul style="list-style-type: none"> <li>■ <b>cisco-hdlc</b>—Cisco-compatible High-Level Data Link Control is a group of protocols for transmitting data between network points.</li> <li>■ <b>ppp</b>—Point-to-Point Protocol is a protocol used for communication between two computers using a serial interface.</li> </ul>	<ol style="list-style-type: none"> <li>1. In the Encapsulation column, next to the new interface, click <b>Edit</b>.</li> <li>2. From the Encapsulation list, select <b>cisco-hdlc</b>.</li> </ol>	Enter  <b>set encapsulation cisco-hdlc</b>
Enter a hold-time value in milliseconds—for example, <b>60</b> . 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 down for the hold-time period. Similarly, an interface is not advertised as up until it remains up for the hold-time period. The hold time is three times the interval at which keepalive messages are sent.	<ol style="list-style-type: none"> <li>1. In the Hold time section, type <b>60</b> in the Down box.</li> <li>2. In the Up box, type <b>60</b>.</li> </ol>	<ol style="list-style-type: none"> <li>1. Enter  <b>set hold-time down 60</b></li> <li>2. Enter  <b>set hold-time up 60</b></li> </ol>
Create the logical unit—for example, <b>0</b> .  <b>NOTE:</b> You can set the logical unit to <b>0</b> only, unless you are configuring the dialer interface for Multilink PPP encapsulation.	<ol style="list-style-type: none"> <li>1. Next to Unit, click <b>Add new entry</b>.</li> <li>2. In the Interface unit number box, type <b>0</b>.</li> <li>3. Next to Dialer options, select <b>Yes</b>, and then click <b>Configure</b>.</li> </ol>	Enter  <b>set unit 0</b>



**Table 48: Adding a Dialer Interface to a Services Router (continued)**

Task	J-Web Configuration Editor	CLI Configuration Editor
Configure dialer options. <ul style="list-style-type: none"> <li>■ <b>Activation delay</b>—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.</li> <li>■ <b>Deactivation delay</b>—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.</li> <li>■ <b>Idle timeout</b>—Time a connection is idle before disconnecting—for example, 30. Default value is 120 seconds with a range from 0 to 4294967295.</li> <li>■ <b>Initial route check</b>—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.</li> <li>■ <b>Pool</b>—Name of a group of ISDN interfaces configured to use the dialer interface—for example, 3.</li> <li>■ <b>Redial delay</b>—Number of seconds to wait before redialing an incoming ISDN call. Default value is 3 seconds with a range from 2 to 255.</li> </ul>	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 3. 6. In the Redial delay box, type 5.	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 3 5. Enter set redial-delay 5
Configure the remote destination to call—for example, 5551212.	1. Next to Dial string, click <b>Add new entry</b> . 2. In the Dial string box, type 5551212. 3. Click <b>OK</b> .	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.	1. Select <b>Inet</b> under Family, and click <b>Edit</b> . 2. Next to Address, click <b>Add new entry</b> . 3. In the Source box, type 172.20.10.2. 4. In the Destination box, type 172.20.10.1. 5. Click <b>OK</b> .	1. From the top of the configuration hierarchy, enter edit interfaces dl0 unit 0 2. Enter set family inet address 172.20.10.2 3. Enter 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 the primary serial interface. The backup dialer interfaces are activated only when the primary interface fails. ISDN backup connectivity is supported on all interfaces except `ls-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 49.
3. If you are finished configuring the router, 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 209.
  - “Configuring Bandwidth on Demand (Optional)” on page 210.
  - “Configuring Dial-In and Callback (Optional)” on page 215
  - “Configuring Dialer Profiles (Optional)” on page 220.
5. To verify that the network interface is configured correctly, see “Verifying the ISDN Configuration” on page 222.

**Table 49: Configuring an Interface for ISDN Backup**

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the <b>Interfaces</b> level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to Interfaces, click <b>Edit</b>.</li> </ol>	<p>From the top of the configuration hierarchy, enter</p> <pre>edit interfaces fe-0/0/0 unit 0</pre>
Select the physical interface for backup ISDN connectivity.	<ol style="list-style-type: none"> <li>1. In the Interface name column, click the physical interface name.</li> <li>1. Under Unit, in the Nested Configuration column, click <b>Edit</b>.</li> </ol>	
Configure the backup dialer interface—for instance, <code>dl0.0</code> .	<ol style="list-style-type: none"> <li>1. Next to Backup options, click <b>Configure</b>.</li> <li>2. In the Interface box, type <code>dl0.0</code>.</li> <li>3. Click <b>OK</b> until you return to the Interfaces page.</li> </ol>	<p>Enter</p> <pre>set backup-options interface dl0.0</pre>

## Configuring a Dialer Filter 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.

You define an interesting packet using the dialer filter feature of the Services Router. There are two steps to configuring dial-on-demand routing backup using a dialer filter:

- Configuring the Dialer Filter on page 205
- Applying the Dial-on-Demand Dialer Filter to the Dialer Interface on page 206

### 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 50.
3. Go on to “Applying the Dial-on-Demand Dialer Filter to the Dialer Interface” on page 206.

**Table 50: Configuring a Dialer Filter for Interesting Packets**

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the <b>Firewall</b> level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to Firewall, click <b>Configure</b> or <b>Edit</b>.</li> </ol>	<p>From the top of the configuration hierarchy, enter</p> <pre>edit firewall</pre>
Configure the dialer filter name—for example, <b>int-packet</b> .	<ol style="list-style-type: none"> <li>1. Next to Inet, click <b>Configure</b> or <b>Edit</b>.</li> <li>2. Next to Dialer filter, click <b>Add new entry</b>.</li> <li>3. In the Filter name box, type <b>int-packet</b>.</li> </ol>	<ol style="list-style-type: none"> <li>1. Enter <pre>edit family inet</pre> </li> <li>2. Then enter <pre>edit dialer-filter int-packet</pre> </li> </ol>

**Table 50: Configuring a Dialer Filter for Interesting Packets (continued)**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
Configure the dialer filter rule name—for example, <b>term1</b> .	1. Next to Term, click <b>Add new entry</b> .	Enter
Configure term behavior. For example, you might want to configure your interesting packet as an ICMP packet.	2. In the Rule name box, type <b>term1</b> .	set term term1 from protocol icmp
To configure the term completely, include both <b>from</b> and <b>then</b> statements.	3. Next to From, click <b>Configure</b> .	
	4. From the Protocol choice list, select <b>Protocol</b> .	
	5. Next to Protocol, click <b>Add new entry</b> .	
	6. From the Value keyword list, select <b>icmp</b> .	
	7. Click <b>OK</b> twice to return to the Term page.	
Configure the <b>then</b> part of the dialer filter.	1. Next to Then, click <b>Configure</b> .	Enter
	2. From the Designation list, select <b>Note</b> .	set term1 then note
	3. Click <b>OK</b> .	

## 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 51.
3. When you are finished configuring the router, 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 209.
  - “Configuring Bandwidth on Demand (Optional)” on page 210.
  - “Configuring Dial-In and Callback (Optional)” on page 215
  - “Configuring Dialer Profiles (Optional)” on page 220.
5. To verify that the network interface is configured correctly, see “Verifying the ISDN Configuration” on page 222.

**Table 51: Applying the Dialer Filter to the Dialer Interface**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
Navigate to the <b>Interfaces</b> level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to Interfaces, click <b>Edit</b>.</li> </ol>	<p>From the top of the configuration editor hierarchy, enter</p> <pre>edit interfaces d10 unit 0</pre>
Select the dialer interface to apply the filter—for example, d10.	<ol style="list-style-type: none"> <li>1. In the Interface name column, click <b>d10</b>.</li> <li>2. Under Unit, in the Mtu column, click <b>Edit</b>.</li> </ol>	
Select the dialer filter and apply it to the dialer interface.	<ol style="list-style-type: none"> <li>1. In the Family section, next to Inet, click <b>Edit</b>.</li> <li>2. Next to Filter, click <b>Configure</b>.</li> <li>3. In the Dialer box, type <b>int-packet</b>, the dialer-filter configured in “Configuring the Dialer Filter” on page 205, as the dialer-filter.</li> <li>4. Click <b>OK</b>.</li> </ol>	<ol style="list-style-type: none"> <li>1. Enter  edit family inet filter</li> <li>2. Enter  set dialer int-packet</li> </ol>

## 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 Services Router 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 Services Router

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 52.
3. Go on to “Configuring the ISDN Interface for Dialer Watch” on page 208.

**Table 52: Adding a Dialer Watch Interface**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
Navigate to the <b>Interfaces</b> level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to Interfaces, click <b>Edit</b>.</li> </ol>	From the top of the configuration hierarchy, enter  edit interfaces
Select a dialer interface—for example, <b>dl0</b> .  Adding a description, such as <b>dialer-watch</b> , can help you identify one dialer interface from another.	<ol style="list-style-type: none"> <li>1. Under Interface name, select <b>dl0</b>.</li> <li>2. In the Description box, type <b>dialer-watch</b>.</li> </ol>	<ol style="list-style-type: none"> <li>1. Enter  <b>edit dl0</b></li> <li>2. Enter  <b>set description dialer-watch</b></li> </ol>
On a logical interface—for example, <b>0</b> —configure the list of routes for dialer watch—for example, <b>172.27.27.0/24</b> .	<ol style="list-style-type: none"> <li>1. Under Unit, click the logical unit number <b>0</b>.</li> <li>2. Next to Dialer options, click <b>Edit</b>.</li> <li>3. Next to Watch list, click <b>Add new entry</b>.</li> <li>4. In the Prefix box, type <b>172.27.27.0/24</b>.</li> <li>5. Click <b>OK</b>.</li> </ol>	<ol style="list-style-type: none"> <li>1. Enter  <b>edit unit 0 dialer-options</b></li> <li>2. Enter  <b>set watch-list 172.27.27.0/24</b></li> </ol>

## 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 53.
3. If you are finished configuring the router, 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 209.
  - “Configuring Bandwidth on Demand (Optional)” on page 210.
  - “Configuring Dial-In and Callback (Optional)” on page 215
  - “Configuring Dialer Profiles (Optional)” on page 220.
5. To verify that the network interface is configured correctly, see “Verifying the ISDN Configuration” on page 222.

**Table 53: Configuring an ISDN Interface for Dialer Watch**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
Navigate to the <b>Interfaces</b> level in the configuration hierarchy, and select an ISDN physical interface—for example, br-1/0/3.	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to Interfaces, click <b>Edit</b>.</li> <li>3. Under Interface name, click <b>br-1/0/3</b>.</li> </ol>	<p>From the top of the configuration hierarchy, enter</p> <pre>edit interfaces br-1/0/3 dialer-options pool dw-group</pre>
Configure dialer watch options for each ISDN interface participating in the dialer watch feature.	<ol style="list-style-type: none"> <li>1. Next to Dialer options, click <b>Edit</b>.</li> <li>2. Next to Pool, click <b>Add new entry</b>.</li> </ol>	
Each ISDN interface must have the same pool identifier to participate in dialer watch. Therefore, the dialer pool name <b>dw-group</b> , for the dialer watch interface configured in Table 52, is used when configuring the ISDN interface.	<ol style="list-style-type: none"> <li>3. In the Pool identifier box, type <b>dw-group</b>.</li> <li>4. Click <b>OK</b>.</li> </ol>	

### **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 routers. 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 Services Router before configuring on-demand routing backup with OSPF support. For information on configuring OSPF, see “Configuring an OSPF Network” on page 295.

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 54.
3. If you are finished configuring the router, commit the configuration.
4. To verify that the network interface is configured correctly, see “Verifying the ISDN Configuration” on page 222.

**Table 54: Configuring OSPF Demand Circuits**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
Navigate to the <b>Protocols</b> level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to Protocols, click <b>Configure</b>.</li> <li>3. Next to Ospf, click <b>Configure</b>.</li> <li>4. Next to Area, click <b>Add new entry</b>.</li> <li>5. In the Area id box, type 0.0.0.0.</li> </ol>	<p>From the top of the configuration hierarchy, enter</p> <pre>edit protocols ospf area 0.0.0.0</pre>
Configure OSPF on-demand circuits for each ISDN dialer interface participating as an on-demand routing interface—for example, d10.	<ol style="list-style-type: none"> <li>1. Next to Interface, click <b>Add new entry</b>.</li> <li>2. In the Interface name box, type d10.0.</li> <li>3. Select <b>Demand circuit</b>.</li> <li>4. Click <b>OK</b>.</li> </ol>	<ol style="list-style-type: none"> <li>1. Enter <pre>edit interface d10</pre> </li> <li>2. Enter <pre>set demand-circuit</pre> </li> </ol>

### Configuring Bandwidth on Demand (Optional)

You can define a threshold for network traffic on the Services Router using the dialer interface and ISDN interfaces. A number of ISDN interfaces are aggregated together and assigned a single dialer profile. Initially, only one ISDN link is active and all packets are sent through this interface. When a predefined threshold is reached, the dialer interface activates another ISDN link and initiates a data connection.

#### Configuring a Dialer Interface 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 55.
3. Go on to “Configuring an ISDN Interface for Bandwidth on Demand” on page 214.



**Table 55: Configuring a Dialer Interface for Bandwidth on Demand**

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the <b>Interfaces</b> level in the configuration hierarchy, and select a dialer interface—for example, <b>d10</b> .	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to <b>Interfaces</b>, click <b>Edit</b>.</li> <li>3. Next to <b>d10</b>, click <b>Edit</b>.</li> </ol>	<p>From the top of the configuration hierarchy, enter</p> <pre>edit interfaces d10</pre>
Configure multilink properties on the dialer interface.	<ol style="list-style-type: none"> <li>1. Select <b>multilink-ppp</b> as the encapsulation type.</li> </ol>	<p>Enter</p> <pre>set encapsulation multilink-ppp</pre>
<p>Configure the dialer options.</p> <ul style="list-style-type: none"> <li>■ <b>Dial string</b>—Telephone number for the interface to dial that establishes ISDN connectivity—for example, <b>4085551515</b>. You can configure a maximum of 15 dial strings per dialer interface.</li> <li>■ <b>Idle timeout</b>—Time a connection is idle before disconnecting—for example, <b>300</b>. Default value is <b>120</b> seconds with a range from <b>0</b> to <b>4294967295</b>.</li> <li>■ <b>Load interval</b>—Interval of time between average network load calculations—for example, <b>90</b>. Default value is <b>60</b> seconds with a range of <b>20-180</b> seconds incremented in <b>10</b> seconds.</li> <li>■ <b>Load threshold</b>—Percentage of load on all links—for example <b>95</b>. Default value is <b>100</b> with a range from <b>0</b> to <b>100</b>.</li> <li>■ <b>Pool</b>—Name of a group of ISDN interfaces configured to use the dialer interface—for example, <b>bw-pool</b>.</li> </ul>	<ol style="list-style-type: none"> <li>1. In the Unit section, click <b>Dialer options</b> under Encapsulation.</li> <li>2. Next to Dial string, click <b>Add new entry</b>.</li> <li>3. In the Value box, type <b>4085551515</b> and click <b>OK</b>.</li> <li>4. In the Idle timeout box, type <b>300</b>.</li> <li>5. In the Load interval box, type <b>90</b>.</li> <li>6. In the Load threshold box, type <b>95</b>.</li> <li>7. In the Pool box, type <b>bw-pool</b>.</li> <li>8. Click <b>OK</b>.</li> </ol>	<ol style="list-style-type: none"> <li>1. Enter <pre>edit unit 0</pre></li> <li>2. Enter <pre>edit dialer-options</pre></li> <li>3. Enter <pre>set dial-string 4085551515</pre></li> <li>4. Enter <pre>set idle-timeout 300</pre></li> <li>5. Enter <pre>set load-interval 90</pre></li> <li>6. Enter <pre>set load-threshold 95</pre></li> <li>7. Enter <pre>set pool bw-pool</pre></li> </ol>

**Table 55: Configuring a Dialer Interface for Bandwidth on Demand (continued)**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
<p>Configure unit properties.</p> <p>To configure multiple dialer interfaces for bandwidth-on-demand, increment the unit number—for example, <b>d10.1</b>, <b>d10.2</b>, and so on.</p> <p><b>F max period</b> is the maximum number of compressed packets allowed between the transmission of full packets—for example, <b>100</b>. The value can be between <b>1</b> and <b>65535</b>.</p>	<ol style="list-style-type: none"> <li>Next to Compression, select <b>Yes</b>, and then click <b>Configure</b>.</li> <li>Select <b>Rtp</b>, and then click <b>Configure</b>.</li> <li>In the F max period box, type <b>100</b>.</li> <li>Next to Queues, click <b>Add new entry</b>.</li> <li>From the Value list, select <b>q3</b>.</li> <li>Click <b>OK</b> until you return to the Unit page.</li> </ol>	<ol style="list-style-type: none"> <li>From the top of the configuration hierarchy, enter edit interfaces d10 unit 0</li> <li>Enter set compression rtp f-max-period 500 queues q3</li> </ol>
<p>Configure logical properties.</p> <ul style="list-style-type: none"> <li>■ <b>Fragment threshold</b>—Maximum size, in bytes, for multilink packet fragments. The value can be between <b>128</b> and <b>16320</b> bytes, for example, <b>1024</b>. The default is 0 bytes (no fragmentation). Any nonzero value must be a multiple of 64 bytes.</li> <li>■ Maximum received reconstructed unit (MRRU) is expressed as a number between <b>1500</b> and <b>4500</b> bytes—for example, <b>1500</b>.</li> </ul>	<ol style="list-style-type: none"> <li>In the Fragment threshold box, type <b>1024</b>.</li> <li>In the Mrru box, type <b>1500</b>.</li> <li>Click <b>OK</b> until you return to the Configuration page.</li> </ol>	<ol style="list-style-type: none"> <li>Enter set fragment-threshold 1024</li> <li>Enter set mrru 1500</li> </ol>
<p>Define a CHAP access profile with a client and a secret password. For example, define <b>bw-profile</b> with client <b>1</b> and password <b>my-secret</b>.</p>	<ol style="list-style-type: none"> <li>Next to Access, click <b>Configure</b> or <b>Edit</b>.</li> <li>Next to Profile, click <b>Add new entry</b>.</li> <li>In the Profile name box, type <b>bw-profile</b>.</li> <li>Next to Client, click <b>Add new entry</b>.</li> <li>In the Name box, type <b>client1</b>.</li> <li>In the Chap secret box, type <b>my-secret</b>.</li> <li>Click <b>OK</b> until you return to the Configuration page.</li> </ol>	<p>From the top of the configuration hierarchy, enter</p> <p>set access profile bw-profile client client1 chap-secret my-secret</p>

**Table 55: Configuring a Dialer Interface for Bandwidth on Demand (continued)**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
Navigate to the appropriate dialer interface level in the configuration hierarchy—for example, <b>d10</b> unit <b>0</b> .	<ol style="list-style-type: none"> <li>1. Next to Interfaces, click <b>Edit</b>.</li> <li>2. In the interface name box, click <b>d10</b>.</li> <li>3. In the Interface unit number box, click <b>0</b>.</li> </ol>	<p>From the top of the configuration hierarchy, enter</p> <pre>edit interfaces d10 unit 0</pre>
Configure CHAP on the dialer interface and specify a unique profile name containing a client list and access parameters—for example, <b>bw-profile</b> .	<ol style="list-style-type: none"> <li>1. Next to Ppp options, click <b>Configure</b>.</li> <li>2. Next to Chap, click <b>Configure</b>.</li> <li>3. In the Access profile box, type <b>bw-profile</b>.</li> <li>4. Click <b>OK</b>.</li> </ol>	<p>Enter</p> <pre>set ppp-options chap access-profile bw-profile</pre>

**Table 55: Configuring a Dialer Interface for Bandwidth on Demand (continued)**

<b>Task</b>	<b>J-Web Configuration Editor</b>	<b>CLI Configuration Editor</b>
Configure packet compression.	1. Under Compression, select <b>Acfc</b> .	Enter
You can configure the following compression types:	2. Click <b>OK</b> until you return to the Unit page.	set ppp-options compression acfc
<ul style="list-style-type: none"> <li>■ <b>acfc (address and control field compression)</b>—Conserves bandwidth by compressing the address and control fields of PPP-encapsulated packets.</li> <li>■ <b>pfc (protocol field compression)</b>—Conserves bandwidth by compressing the protocol field of a PPP-encapsulated packet.</li> </ul>		
Configure the dialer interface to be assigned an IP address in one of the following ways:	<p>Next to Inet, select <b>Yes</b> and click <b>Configure</b>.</p> <p>Select one of the following IP address configurations:</p> <p>To obtain an IP address from the remote end:</p> <ol style="list-style-type: none"> <li>1. Next to Negotiate address, select the <b>Yes</b> check box.</li> <li>2. Click <b>OK</b>.</li> </ol> <p>To derive the source address and assign the destination address:</p> <ol style="list-style-type: none"> <li>1. Next to Unnumbered address, select the <b>Yes</b> check box and click <b>Configure</b>.</li> <li>2. In the Destination box, type <b>192.168.1.2</b>.</li> <li>3. In the Source box, type <b>lo0.0</b>.</li> <li>4. Click <b>OK</b>.</li> </ol>	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>■ To obtain an IP address from the remote end, enter  <b>set family inet negotiate-address</b></li> <li>■ To derive the source address and assign the destination address, enter  <b>set family inet unnumbered-address lo0.0 destination 192.168.1.2</b></li> </ul>

## 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 56.

3. If you are finished configuring the router, commit the configuration.
4. To verify that the network interface is configured correctly, see “Verifying the ISDN Configuration” on page 222.

**Table 56: Configuring an ISDN Interface for Bandwidth on Demand**

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the <b>Interfaces</b> level in the configuration hierarchy, and select an ISDN physical interface—for example, <b>br-1/0/3</b> .	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to Interfaces, click <b>Edit</b>.</li> <li>3. Under Interface name, click <b>br-1/0/3</b>.</li> </ol>	<p>From the top of the configuration hierarchy, enter</p> <pre>edit interfaces br-1/0/3</pre>
<p>Configure dialer options for each ISDN interface by following the instructions in Table 55.</p> <p>Each ISDN interface must have the same pool identifier to participate in bandwidth on demand. Therefore, the dialer pool name <b>bw-pool</b>, for the dialer interface configured in Table 55, is used when configuring the ISDN interface.</p> <p>You can group up to four <b>br</b> interfaces together when configuring bandwidth on demand with a total of eight B-channels providing connectivity.</p>	<ol style="list-style-type: none"> <li>1. Next to Dialer options, click <b>Dialer options</b>.</li> <li>2. Next to Pool, click <b>Add new entry</b>.</li> <li>3. In the Pool identifier box, type the name of the dialer pool—for example, <b>bw-pool</b>.</li> <li>4. Click <b>OK</b>.</li> </ol>	<p>Enter</p> <pre>set dialer-options pool bw-pool</pre>

## 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 the Services Router 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 Services Router. You can also configure the Services Router to reject all incoming ISDN calls.



**NOTE:** Incoming voice calls are currently not supported.

When it receives an incoming ISDN call, the Services Router 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 Services Router 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 4085321091 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.

The dialer interface of the Services Router and the dialer interface of the remote router must have the same encapsulation—PPP, Multilink PPP, or Cisco HDLC. If the encapsulation is different, the ISDN call is dropped. Table 57 describes how the Services Router performs encapsulation monitoring.

**Table 57: Encapsulation Monitoring by Services Router**

Encapsulation on Services Router's Dialer Interface	Encapsulation on Remote Router's Dialer Interface	Possible Action on Services Router's Dialer Interface	Encapsulation Monitoring and Call Status
PPP	PPP	■ Accepts an incoming call	Services Router performs encapsulation monitoring.
Multilink PPP	Multilink PPP	■ Rejects an incoming call and calls back the incoming number when callback is enabled on the dialer interface	ISDN call is <i>successful</i> because encapsulation matches.
PPP	Multilink PPP or Cisco HDLC		Services Router performs encapsulation monitoring.
Multilink PPP	PPP or Cisco HDLC		ISDN call is <i>dropped</i> because of encapsulation mismatch.
PPP or Multilink PPP	PPP, Multilink PPP, or Cisco HDLC	■ Dials out	Services Router does not perform encapsulation monitoring.
		■ Accepts an incoming call as a result of having originally dialed out, because the dialer interface of the remote router has callback enabled	Success of the ISDN call depends on the encapsulation monitoring capability of the remote router.
Cisco HDLC	PPP, Multilink PPP, or Cisco HDLC	■ Dials out	
		■ Accepts an incoming call	
		■ Accepts an incoming call as a result of having originally dialed out, because the dialer interface of the remote router has callback enabled	
		■ Rejects an incoming call and calls back the incoming number when callback is enabled on the dialer interface	

This section contains the following topics:

- Configuring a Dialer Interface for Dial-In and Callback on page 217
- Configuring an ISDN Interface to Screen Incoming Calls on page 219
- Configuring the Services Router to Reject Incoming ISDN Calls on page 220

## Configuring a Dialer Interface 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 58.
3. If you are finished configuring the router, commit the configuration.
4. To verify that the network interface is configured correctly, see “Verifying the ISDN Configuration” on page 222.

**Table 58: Configuring the Dialer Interface for Dial-In and Callback**

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the <b>Interfaces</b> level in the configuration hierarchy, and select a dialer interface—for example, d10.	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to Interfaces, click <b>Edit</b>.</li> <li>3. Next to d10, click <b>Edit</b>.</li> </ol>	<p>From the top of the configuration hierarchy, enter</p> <pre>edit interfaces d10</pre>

**Table 58: Configuring the Dialer Interface for Dial-In and Callback (continued)**

Task	J-Web Configuration Editor	CLI Configuration Editor
On a logical interface—for example, 0—configure the incoming map options for the dialer interface.	1. In the Unit section, for logical unit number 0, click <b>Dialer options</b> under Encapsulation.	1. Enter edit unit 0
<ul style="list-style-type: none"> <li>■ <b>accept-all</b>—Dialer interface accepts all incoming calls.  You can configure the <b>accept-all</b> option for only one of the dialer interfaces associated with an ISDN physical interface. The dialer interface with the <b>accept-all</b> option configured is used only if the incoming call's caller ID does not match the caller IDs configured on other dialer interfaces.</li> </ul>	2. Next to Incoming map, click <b>Configure</b> .  3. From the Caller type menu, select <b>Caller</b> .  Next to Caller, click <b>Add new entry</b> .	2. Enter edit dialer-options
<ul style="list-style-type: none"> <li>■ <b>caller</b>—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.</li> </ul>	4. In the Caller id box, type 4085551515.	3. Enter  set incoming-map caller 4085551515
Configure callback options for the dialer interface	1. Select <b>Callback</b> .	1. Enter
<ul style="list-style-type: none"> <li>■ <b>Callback</b>—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: <ul style="list-style-type: none"> <li>■ The dialer interface is not configured as a backup for a primary interface.</li> <li>■ The dialer interface does not have a watch list configured.</li> <li>■ Only one dial string is configured for the dialer interface.</li> <li>■ Dial-in is configured on the dialer interface of the remote router that is dialing in.</li> </ul> </li> <li>■ <b>Callback wait period</b>—Number of seconds to wait before redialing an incoming ISDN call.</li> </ul>	2. In the Callback wait period box, type 5.	2. Enter set callback  set callback-wait-period 5



## 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 Services Router 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 59.
3. If you are finished configuring the router, commit the configuration.
4. To verify that the network interface is configured correctly, see “Verifying the ISDN Configuration” on page 222.

**Table 59: Configuring an ISDN Interface to Screen Incoming ISDN Calls**

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the <b>Interfaces</b> level in the configuration hierarchy, and select an ISDN physical interface—for example, br-1/0/3.	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to Interfaces, click <b>Edit</b>.</li> <li>3. Next to br-1/0/3, click <b>Edit</b>.</li> </ol>	<p>From the top of the configuration hierarchy, enter</p> <pre>edit interfaces br-1/0/3</pre>
Configure the incoming called number—for example, 4085551091—for the ISDN interface.	<ol style="list-style-type: none"> <li>1. Next to Isdn options, click <b>Edit</b>.</li> <li>2. Next to Incoming called number, click <b>Add new entry</b>.</li> </ol>	<p>Enter</p> <pre>set isdn-options incoming-called-number 4085551091</pre>
To configure the ISDN interface to ignore the incoming called number, use the <b>reject</b> option.	<ol style="list-style-type: none"> <li>3. In the Called number box, type 4085551091.</li> <li>4. Click <b>OK</b>.</li> </ol>	

## Configuring the Services Router to Reject Incoming ISDN Calls

By default, the Services Router is configured to accept incoming ISDN calls. The incoming calls are accepted if dial-in is configured on the Services Router. You can configure the Services Router to reject all incoming ISDN calls.

To configure the Services Router 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 60.
3. If you are finished configuring the router, commit the configuration.
4. To verify that the network interface is configured correctly, see “Verifying the ISDN Configuration” on page 222.

**Table 60: Configuring the Services Router to Reject Incoming ISDN Calls**

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the <b>Processes</b> level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>2. Next to System, click <b>Edit</b>.</li> <li>3. Next to Processes, click <b>Configure</b>.</li> <li>4. Next to Isdn signaling, click <b>Configure</b>.</li> </ol>	<p>From the top of the configuration hierarchy, enter</p> <pre>set system processes isdn-signaling reject-incoming</pre>
Configure the Services Router to reject incoming calls.	<ol style="list-style-type: none"> <li>1. Under Isdn signaling, select <b>Reject Incoming</b>.</li> <li>2. Click <b>OK</b>.</li> </ol>	

## Configuring Dialer Profiles (Optional)

You can configure multiple dialer interfaces to participate as part of a dialer profile. After configuring dialer interfaces, you configure an ISDN interface on the Services Router to participate as part of a dialer profile. In the configuration in Table 61, dialer interfaces dl0 and dl1 and ISDN interface br-1/0/3 are used as examples.

To configure a logical dialer interface for the Services Router:

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 61.

- When you are finished configuring the router, commit the configuration.

**Table 61: Dialer Profile Configuration**

Task	J-Web Configuration Editor	CLI Configuration Editor
Navigate to the <b>Interfaces</b> level in the configuration hierarchy.	<ol style="list-style-type: none"> <li>In the configuration editor hierarchy, select <b>Configuration &gt; View and Edit &gt; Edit Configuration</b>.</li> <li>Next to Interfaces, click <b>Configure</b> or <b>Edit</b>.</li> <li>Under Interface name, click <b>dl0</b>.</li> </ol>	<p>From the top of the configuration editor hierarchy, enter</p> <pre>edit interfaces dl0 unit 0</pre>
Add a dialer pool, <b>pool1</b> , to a dialer interface.	<ol style="list-style-type: none"> <li>In the Unit table, click <b>Dialer options</b>.</li> <li>In the Pool box, type <b>pool1</b>.</li> <li>Click <b>OK</b>.</li> </ol>	<pre>Enter set dialer-options pool pool1</pre>
<p>Configure a source IP address—for example, <b>172.20.10.1</b>—for the dialer interface.</p> <p>Configure a destination IP address—for example, <b>172.20.10.2</b>—for the dialer interface.</p>	<ol style="list-style-type: none"> <li>Select <b>Inet</b> under Family, and click <b>Edit</b>.</li> <li>Next to Address, click <b>Add new entry</b>.</li> <li>In the Source box, type <b>172.20.10.1</b>.</li> <li>In the Destination box, type <b>172.20.10.2</b>.</li> <li>Click <b>OK</b> until you return to the Interfaces page.</li> </ol>	<pre>1. Enter set family inet address 172.20.10.1 2. Enter set family inet address destination 172.20.10.2</pre>
<p>Configure the ISDN interface—for example, <b>br-1/0/3</b>—with a dialer profile that uses either dialer interface to initiate an ISDN connection.</p> <p><b>Priority</b> has a range from <b>0</b> to <b>255</b>, with <b>255</b> having the highest priority.</p> <p>The <b>br-1/0/3</b> interface now uses <b>pool2</b> to establish connectivity first, and then <b>pool1</b>.</p>	<ol style="list-style-type: none"> <li>Next to br-1/0/3, click <b>Dialer options</b>.</li> <li>Next to Pool, click <b>Add new entry</b>.</li> <li>In the Pool identifier box, type <b>pool1</b>.</li> <li>In the Priority box, type <b>10</b>.</li> <li>Click <b>OK</b>.</li> <li>Click <b>Add new entry</b> again, and add <b>pool2</b> to the interface.</li> <li>In the Priority box, type <b>25</b>.</li> <li>Click <b>OK</b>.</li> </ol>	<pre>1. Enter edit interfaces br-1/0/3 dialer-options 2. Enter set pool pool1 priority 10 3. Enter set pool pool2 priority 25</pre>

## Verifying the ISDN Configuration

---

To verify an ISDN configuration, perform the following tasks:

- Displaying the ISDN Status on page 222
- Verifying an ISDN Interface on page 223
- Checking B-Channel Statistics on page 224
- Checking D-Channel Interface Statistics on page 225
- Displaying the Status of ISDN Calls on page 226
- Verifying Dialer Interface Configuration on page 227

### Displaying the ISDN Status

**Purpose** Display the status of ISDN parameters on the ISDN interface. For example, you can display ISDN parameters on the br-6/0/0 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
T306              : 10 seconds
T310              : 10 seconds
Tei Option       : Power Up
```

**What It Means** The output shows a summary of interface information. Verify the following information:

- Interface—ISDN interface currently active on the Services Router.
- Layer 1 status—Displays as active or inactive.
- Layer 2 status—Displays Q.921 as up or down.
- TEI—Displays the assigned TEI number.
- Layer 3 status—Displays the number of active calls.
- Switch Type—Type of ISDN switch connected to the Services Router interface.
- Interface Type—Default value for the local interface.

- Calling number—Displays the telephone number configured for dial out.
- T306 and T310—Q.931 specific timers.
- TEI Option—Determines when TEI negotiations occur on the interface.

## Verifying an ISDN Interface

**Purpose** Verify that the ISDN interface is correctly configured.

**Action** From the CLI, enter the show interfaces extensive command.

**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

```

**What It Means** 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.

## Checking B-Channel Statistics

**Purpose** Verify that the ISDN B-channel interface is correctly configured.

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

**Sample Output** `user@host> show interfaces bc-0/0/4 extensive`

```
Physical interface: bc-6/0/4:1, 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
Packet Forwarding Engine configuration:
Destination slot: 5, PLP byte: 1 (0x00)
CoS transmit queue      Bandwidth      Buffer Priority  Limit
                        %      bps      %      usec
0 best-effort           95      60800   95         0    low    none
3 network-control        5       3200    5         0    low    none

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
```

- What It Means** 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).
  - 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.

## Checking D-Channel Interface Statistics

- Purpose** Verify that the ISDN D-channel interface is correctly configured.
- Action** From the CLI, enter the show interfaces extensive command.
- 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:
Seconds      Count  State
LOF          0      1    0K
LOS          0      0    0K

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

```

**What It Means**

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).
- 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.

## 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 227.
- Action** From the CLI, enter the show isdn calls command.



**Sample Output**      `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

```

**What It Means**      The output shows a summary of active ISDN calls on B-channel interfaces. 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

## 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 226.

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

**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:
    Input bytes      :                13859                0 bps
    Output bytes     :                   0                0 bps
    Input packets    :                 317                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

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
  0 bps
  0 bps
  0 pps
  0 pps
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

```

**What It Means** The output shows a summary of dialer 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 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.
- 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 *J-series Services Router Administration Guide*.

For complete descriptions of the interface output, see the *JUNOS Network and Services Interfaces Command Reference*.



## **Part 3**

# **Configuring Routing Protocols**

- Routing Overview on page 233
- Configuring Static Routes on page 267
- Configuring a RIP Network on page 279
- Configuring an OSPF Network on page 295
- Configuring the IS-IS Protocol on page 315
- Configuring BGP Sessions on page 323



## Chapter 7

# Routing Overview

Routing is the process of 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.

To use the routing capabilities of a J-series Services Router, you must understand the fundamentals of IP routing and the routing protocols that are primarily responsible for the transmission of unicast traffic. To read this chapter, you need a basic understanding of IP addressing and TCP/IP.



**NOTE:** Unless otherwise specified, J-series Services Routers support IPv6 addressing and routing. For information about IPv6, see the *JUNOS Routing Protocols Configuration Guide*.

---

This chapter includes the following topics. For more information, see the *JUNOS Routing Protocols Configuration Guide*.

- Routing Terms on page 233
- Routing Overview on page 237
- RIP Overview on page 243
- OSPF Overview on page 247
- IS-IS Overview on page 252
- BGP Overview on page 255

## Routing Terms

---

To understand routing, become familiar with the terms defined in Table 62 .

**Table 62: Routing Terms**

| <b>Term</b>                            | <b>Definition</b>                                                                                                                                                                                                                                                                                             |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>adjacency</b>                       | Portion of the local routing information that pertains to the reachability of a single neighbor over a single circuit or interface.                                                                                                                                                                           |
| <b>area</b>                            | Administrative group of OSPF networks within an autonomous system (AS) that operates independently from other areas in the AS. Multiple areas within an AS reduce the amount of link-state advertisement (LSA) traffic on the network and the size of topology databases.                                     |
| <b>area border router (ABR)</b>        | In OSPF, a router having interfaces in multiple areas of an autonomous system (AS) so that it can link the areas to each other. An area border router maintains a separate topological database for each area it is connected to and shares topology information between areas.                               |
| <b>AS path</b>                         | In BGP, the list of autonomous system (ASs) that a packet must traverse to reach a given set of destinations within a single AS.                                                                                                                                                                              |
| <b>autonomous system (AS)</b>          | Network, collection of routers, or portion of a large internetwork under a single administrative authority.                                                                                                                                                                                                   |
| <b>backbone area</b>                   | In OSPF, the central area in an autonomous system (AS) to which all other areas are connected by area border routers (ABRs). The backbone area always has the area ID 0.0.0.0.                                                                                                                                |
| <b>bidirectional connectivity</b>      | Ability of directly connected devices to communicate with each other over the same link.                                                                                                                                                                                                                      |
| <b>Border Gateway Protocol (BGP)</b>   | Exterior gateway protocol used to exchange routing information among routers in different autonomous systems.                                                                                                                                                                                                 |
| <b>broadcast</b>                       | Operation of sending network traffic from one network node to all other network nodes.                                                                                                                                                                                                                        |
| <b>cluster</b>                         | In BGP, a set of routers that have been grouped together. A cluster consists of one system that acts as a route reflector, along with any number of client peers. The client peers receive their route information only from the route reflector system. Routers in a cluster do not need to be fully meshed. |
| <b>confederation</b>                   | In BGP, a group of autonomous systems (ASs) that appears to external ASs to be a single AS.                                                                                                                                                                                                                   |
| <b>confederation sequence</b>          | Ordered set of autonomous systems (ASs) for a confederation. The closest AS in the path is first in the sequence.                                                                                                                                                                                             |
| <b>convergence</b>                     | After a topology change, the time all the routers in a network take to receive the information and update their routing tables.                                                                                                                                                                               |
| <b>cost</b>                            | Unitless number assigned to a path between neighbors, based on throughput, round-trip time, and reliability. The sum of path costs between source and destination hosts determines the overall path cost. OSPF uses the lowest cost to determine the best path.                                               |
| <b>designated router (DR)</b>          | In OSPF, a node designated to process link-state advertisements (LSAs) and distribute topology updates for an autonomous system (AS).                                                                                                                                                                         |
| <b>distance vector</b>                 | Number of hops to a routing destination.                                                                                                                                                                                                                                                                      |
| <b>dynamic routing</b>                 | Routing method that enables the route of a message through a network to change as network conditions change. Compare <i>static routing</i> .                                                                                                                                                                  |
| <b>end systems</b>                     | Network entities that send and receive packets.                                                                                                                                                                                                                                                               |
| <b>exterior gateway protocol (EGP)</b> | Protocol that exchanges routing information between autonomous systems (ASs). BGP is an EGP. Compare <i>interior gateway protocol (IGP)</i> .                                                                                                                                                                 |
| <b>external BGP (EBGP)</b>             | BGP configuration in which sessions are established between routers in different autonomous systems (ASs).                                                                                                                                                                                                    |
| <b>external peer</b>                   | In BGP, a peer that resides in a different autonomous system (AS) from the Services Router.                                                                                                                                                                                                                   |
| <b>external route</b>                  | Route to an area outside the network.                                                                                                                                                                                                                                                                         |



**Table 62: Routing Terms (continued)**

| <b>Term</b>                                               | <b>Definition</b>                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>flooding</b>                                           | Technique by which a router forwards traffic to every node attached to the router, except the node from which the traffic arrived. Flooding is a simple but sometimes inefficient way to distribute routing information quickly to every node in a network. RIP and OSPF are flooding protocols, but BGP is not.                     |
| <b>forwarding table</b>                                   | JUNOS software forwarding information base (FIB). 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 is responsible for determining which interface transmits the packets. |
| <b>full mesh</b>                                          | Network in which devices are organized in a mesh topology, with each node connected to every other network node.                                                                                                                                                                                                                     |
| <b>gateway router</b>                                     | Node on a network that serves as an entrance to another network.                                                                                                                                                                                                                                                                     |
| <b>global AS</b>                                          | Global autonomous system (AS). An AS consisting of multiple subautonomous systems (sub-ASs).                                                                                                                                                                                                                                         |
| <b>handshake</b>                                          | Process of exchanging signaling information between two communications devices to establish the method and transmission speed of a connection.                                                                                                                                                                                       |
| <b>hello packet</b>                                       | In OSPF, a packet sent periodically by a router to first establish and then maintain network adjacency, and to discover neighbor routers.                                                                                                                                                                                            |
| <b>hold time</b>                                          | Maximum number of seconds allowed to elapse between the time a BGP system receives successive keepalive or update messages from a peer.                                                                                                                                                                                              |
| <b>hop</b>                                                | Trip a data packet takes from one router to another in the network. The number of routers through which a packet passes to get from its source to its destination is known as the hop count. In general, the best route is the one with the shortest hop count.                                                                      |
| <b>intermediate systems</b>                               | Network entities that relay (forward) packets as well as send and receive them on the network. Intermediate systems are also known as routers.                                                                                                                                                                                       |
| <b>Intermediate System-to-Intermediate System (IS-IS)</b> | Link-state, interior gateway routing protocol for IP networks that also uses the shortest-path-first (SPF) algorithm to determine routes.                                                                                                                                                                                            |
| <b>interior gateway protocol (IGP)</b>                    | Protocol that exchanges routing information within autonomous systems (ASs). IS-IS, OSPF, and RIP are IGPs. Compare <i>exterior gateway protocol (EGP)</i> .                                                                                                                                                                         |
| <b>Internal BGP (IBGP)</b>                                | BGP configuration in which sessions are established between routers in the same autonomous systems (ASs).                                                                                                                                                                                                                            |
| <b>internal peer</b>                                      | In BGP, a peer that resides in the same autonomous system (AS) as the Services Router.                                                                                                                                                                                                                                               |
| <b>keepalive message</b>                                  | Periodic message sent by one BGP peer to another to verify that the session between them is still active.                                                                                                                                                                                                                            |
| <b>latency</b>                                            | Delay that occurs when a packet or signal is transmitted over a communications system.                                                                                                                                                                                                                                               |
| <b>link-state advertisement (LSA)</b>                     | Messages that announce the presence of OSPF-enabled interfaces to adjacent OSPF interfaces (neighbors). The exchange of LSAs establishes bidirectional connectivity between neighbors.                                                                                                                                               |
| <b>local preference</b>                                   | Optional BGP path attribute carried in internal BGP update packets that indicates the degree of preference for an external route.                                                                                                                                                                                                    |
| <b>mesh</b>                                               | Network topology in which devices are organized in a manageable, segmented manner with many, often redundant, interconnections between network nodes. See also <i>full mesh</i> .                                                                                                                                                    |
| <b>metric</b>                                             | Numerical value that determines how quickly a packet can reach its destination. See also <i>cost</i> .                                                                                                                                                                                                                               |
| <b>multiple exit discriminator (MED)</b>                  | Optional BGP path attribute consisting of a metric value that is used to determine the exit point to a destination when all other factors in determining the exit point are equal.                                                                                                                                                   |

**Table 62: Routing Terms (continued)**

| <b>Term</b>                                     | <b>Definition</b>                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>neighbor</b>                                 | Adjacent router interface. A node can directly route packets to its neighbors only. See also <i>peer</i> .                                                                                                                                                                                                                                    |
| <b>network</b>                                  | Series of nodes interconnected by communication paths.                                                                                                                                                                                                                                                                                        |
| <b>network diameter</b>                         | Maximum hop count in a network.                                                                                                                                                                                                                                                                                                               |
| <b>network topology</b>                         | Arrangement of nodes and connections in a network.                                                                                                                                                                                                                                                                                            |
| <b>node</b>                                     | Connection point that operates as a redistribution point or an end point in a network, recognizing data transmissions and either forwarding or processing them.                                                                                                                                                                               |
| <b>notification message</b>                     | Message sent between BGP peers to inform the receiving peer that the sending peer is terminating the session because an error occurred, and explaining the error.                                                                                                                                                                             |
| <b>not-so-stubby area (NSSA)</b>                | In OSPF, a type of stub area in which external route advertisements can be flooded.                                                                                                                                                                                                                                                           |
| <b>open message</b>                             | Message sent between BGP peers to establish communication.                                                                                                                                                                                                                                                                                    |
| <b>Open Shortest Path First protocol (OSPF)</b> | A link-state interior gateway protocol (IGP) that makes routing decisions based on the shortest-path-first (SPF) algorithm (also referred to as the Dijkstra algorithm).                                                                                                                                                                      |
| <b>origin</b>                                   | Value assigned to a BGP route to indicate whether the first router to advertise the route learned it from an external, internal, or unknown source.                                                                                                                                                                                           |
| <b>path-vector protocol</b>                     | Protocol that uses the path between autonomous systems (ASs) to select the best route, rather than the shortest distance or the characteristics of the route (link state). BGP is a path-vector protocol. In contrast, RIP is a distance-vector protocol, and OSPF and IS-IS are link-state protocols.                                        |
| <b>peer</b>                                     | Immediately adjacent router with which a protocol relationship has been established. See also <i>neighbor</i> .                                                                                                                                                                                                                               |
| <b>peering</b>                                  | The practice of exchanging Internet traffic with directly connected peers according to commercial and contractual agreements.                                                                                                                                                                                                                 |
| <b>point of presence (POP)</b>                  | Access point to the Internet, having a unique IP address, where telecommunications equipment is located. POPs usually belong to Internet service providers (ISPs) or telephone companies.                                                                                                                                                     |
| <b>poison reverse</b>                           | An efficiency technique in a RIP network. By setting the number of hops to an unavailable router to 16 hops or more, a router informs all the other routers in the network. Because RIP allows only up to 15 hops to another router, this technique reduces RIP updates and helps defeat large routing loops. See also <i>split horizon</i> . |
| <b>propagation</b>                              | Process of translating and forwarding route information discovered by one routing protocol in the update messages of another routing protocol. Route propagation is also called route redistribution.                                                                                                                                         |
| <b>reachability</b>                             | In BGP, the feasibility of a route.                                                                                                                                                                                                                                                                                                           |
| <b>round-robin</b>                              | Scheduling algorithm in which items have the same priority and are handled in a fixed cyclic order.                                                                                                                                                                                                                                           |
| <b>route advertisement</b>                      | Distribution of routing information at specified intervals throughout a network, to establish adjacencies with neighbors and communicate usable routes to active destinations. See also <i>link-state advertisement (LSA)</i> .                                                                                                               |
| <b>route aggregation</b>                        | Combining groups of routes with common addresses into a single entry in the routing table, to decrease routing table size and the number of route advertisements sent by a router.                                                                                                                                                            |
| <b>route reflection</b>                         | In BGP, configuring a group of routers into a cluster and having one system act as a route reflector, redistributing routes from outside the cluster to all routers in the cluster. Routers in a cluster do not need to be fully meshed.                                                                                                      |

**Table 62: Routing Terms (continued)**

| Term                                      | Definition                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Routing Information Protocol (RIP)</b> | Distance-vector routing protocol that keeps a database of routing information gathered from periodic broadcasts by each router in a network.                                                                                                                                                                                                                                  |
| <b>routing table</b>                      | Table stored on a router that keeps track of all possible paths (routes) between sources and destinations in a network and, in some cases, metrics associated with the routes.                                                                                                                                                                                                |
| <b>split horizon</b>                      | An efficiency technique in a RIP network. A router reduces the number of RIP updates in the network by not retransmitting a route advertisement out the interface through which it was received. Split-horizon updates also help prevent routing loops. See also <i>poison reverse</i> .                                                                                      |
| <b>static routing</b>                     | Routing method in which routes are manually entered in the routing table and do not change unless you explicitly update them. Unlike dynamic routes, which must be imported into the routing table each time a host comes online, static routes are available immediately. Static routes are generally preferred over other types of routes. Compare <i>dynamic routing</i> . |
| <b>stub area</b>                          | In OSPF, an area through which or into which autonomous system (AS) external route advertisements are not flooded.                                                                                                                                                                                                                                                            |
| <b>subautonomous system (sub-AS)</b>      | Autonomous system (AS) members of a BGP confederation.                                                                                                                                                                                                                                                                                                                        |
| <b>subnetwork</b>                         | Subdivision of a network, which functions exactly like a network except that it has a more specific address and subnet mask (destination prefix).                                                                                                                                                                                                                             |
| <b>three-way handshake</b>                | Process by which two routers synchronize protocols and establish a bidirectional connection.                                                                                                                                                                                                                                                                                  |
| <b>topology database</b>                  | Map of connections between the nodes in a network. The topology database is stored in each node.                                                                                                                                                                                                                                                                              |
| <b>triggered update</b>                   | In a network that uses RIP, a routing update that is automatically sent whenever routing information changes.                                                                                                                                                                                                                                                                 |
| <b>virtual link</b>                       | In OSPF, a link you create between two area border routers (ABRs) that have an interface to a common nonbackbone area, to connect a third area to the backbone area. One of the area border routers must be directly connected to the backbone area.                                                                                                                          |

## Routing Overview

Routing is the transmission of data packets from a source to a destination address. 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.

This overview contains the following topics:

- Networks and Subnetworks on page 238
- Autonomous Systems on page 238
- Interior and Exterior Gateway Protocols on page 238
- Routing Tables on page 239

- Forwarding Tables on page 239
- Dynamic and Static Routing on page 240
- Route Advertisements on page 241
- Route Aggregation on page 241

## **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**

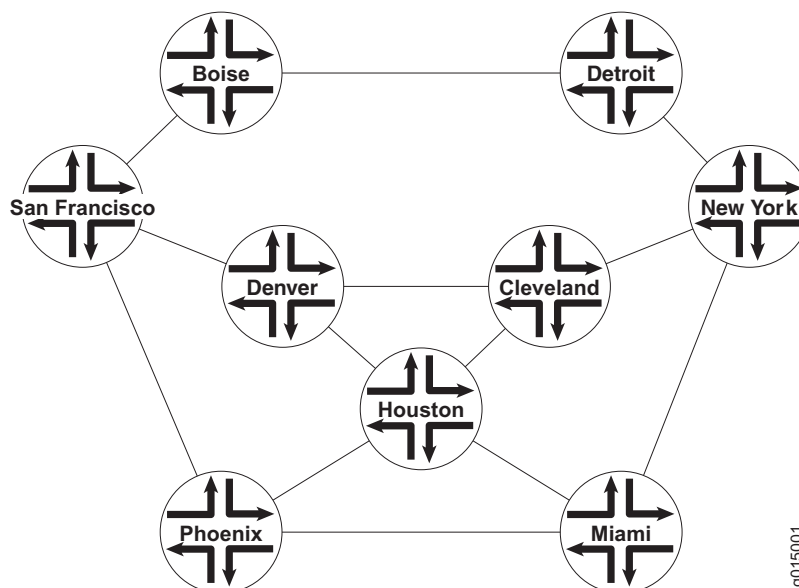
Routing information that is shared within an AS is transmitted by an interior gateway protocol (IGP). Of the different IGPs, the most common are RIP, OSPF, and IS-IS. IGPs are designed to be fast acting and light duty. They typically incorporate only a moderate security system, because trusted internal 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 routers 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 37 shows a simple network of routers.

**Figure 37: Simple Network Topology**



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 37 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 37, 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.

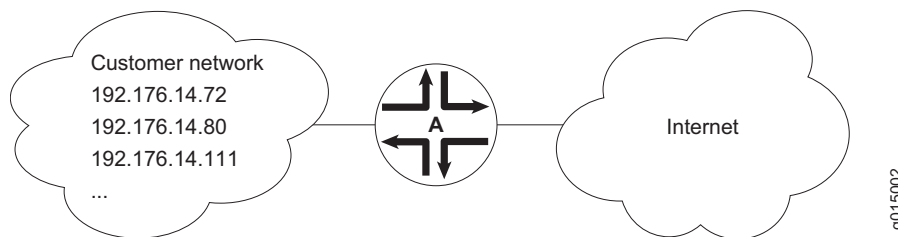
## Dynamic and Static Routing

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 38 shows a network that uses static routes.

**Figure 38: Static Routing Example**



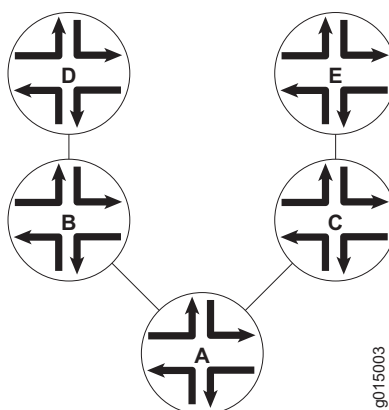
In Figure 38, the customer routes in the 192.176.14/24 subnetwork are static routes. These are hard links to specific customer hosts that never change. Because all traffic destined for any of these routes is forwarded through router A, these routes are included as static routes in router A's routing 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 39.

**Figure 39: Route Advertisement**



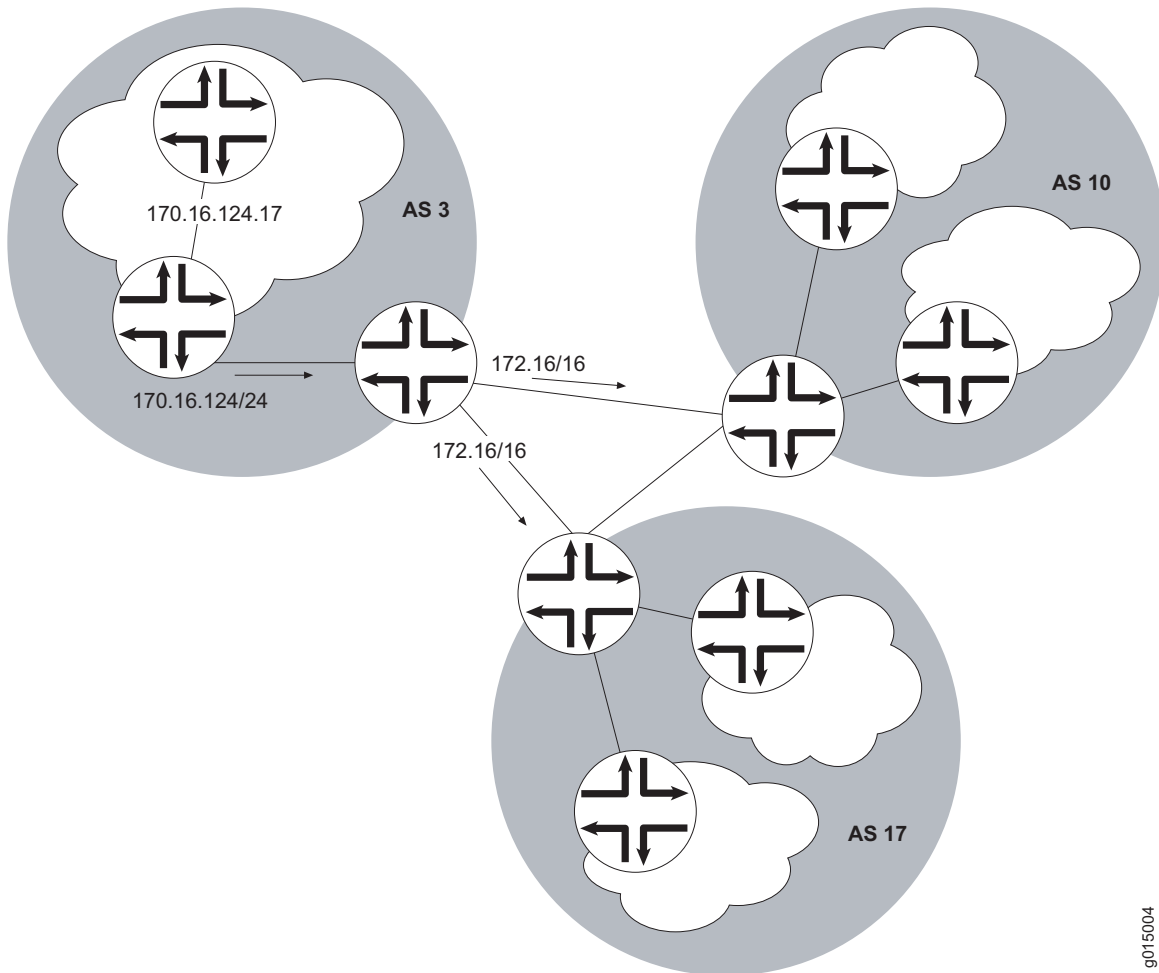
In Figure 39, router A sends out hello packets to each of its neighbors. Routers B and C detect these packets and establish an adjacent relationship with router A. Router B and C then share this information with their neighbors, routers D and E, respectively. By sharing information throughout the network, 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 40.

**Figure 40: Route Aggregation**



9015004

Figure 40 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.

## RIP Overview

---

In a Routing Information Protocol (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.

This overview contains the following topics:

- Distance-Vector Routing Protocols on page 243
- Maximizing Hop Count on page 244
- RIP Packets on page 245
- Split Horizon and Poison Reverse Efficiency Techniques on page 245
- Limitations of Unidirectional Connectivity on page 246

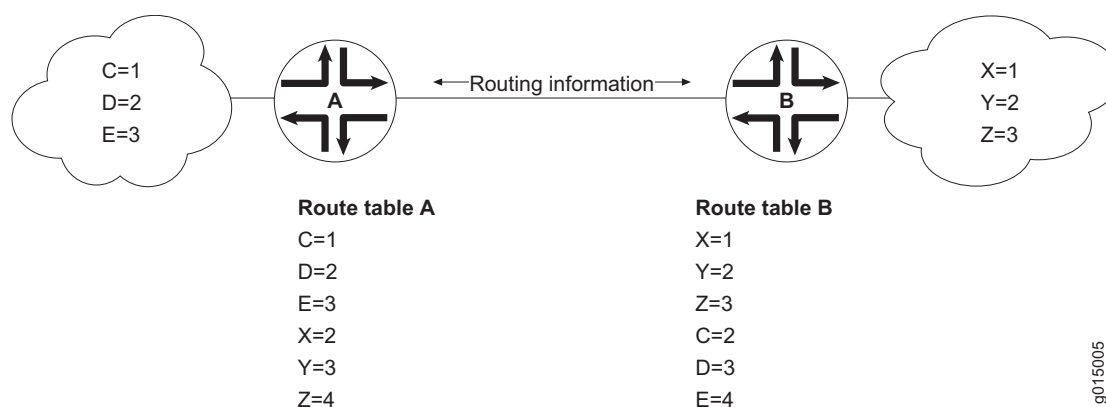


**NOTE:** The J-series Services Router supports both RIP version 1 and RIP version 2. In this guide, the term RIP refers to both versions of the protocol.

---

## 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 41 shows how distance-vector routing works.

**Figure 41: Distance-Vector Protocol**

In Figure 41, 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.

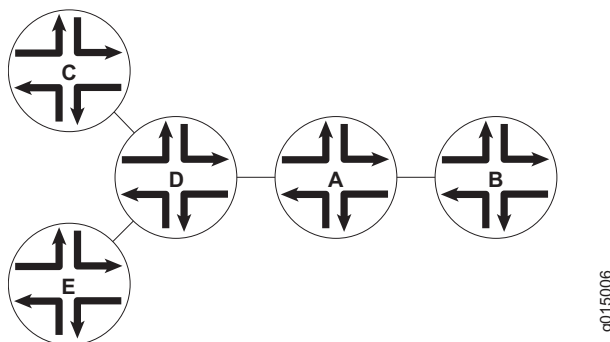
In addition to the regular transmission of RIP packets every 30 seconds, if a router detects a new neighbor or detects that an interface is unavailable, it generates a triggered update. The new routing information is immediately broadcast out all RIP-enabled interfaces, and the change is reflected in 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 42 shows an example of the split horizon technique.

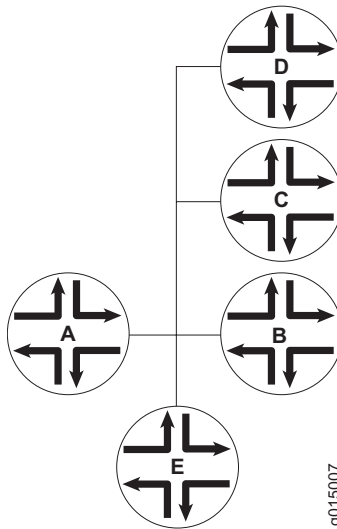
**Figure 42: Split Horizon Example**



In Figure 42, 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 43 shows an example of the poison reverse technique.

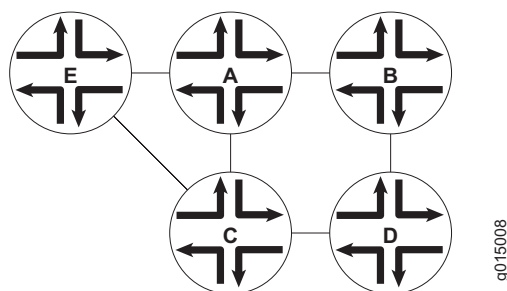
**Figure 43: Poison Reverse Example**



In Figure 43, 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 44 shows, RIP networks are limited by their unidirectional connectivity.

**Figure 44: Limitations of Unidirectional Connectivity**

In Figure 44, 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 due to 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. For more information, see "Link-State Advertisements" on page 248.

## OSPF Overview

In an Open Shortest Path First (OSPF) network, the network topology is distributed among the nodes of the autonomous system (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.

This overview contains the following topics:

- Link-State Advertisements on page 248
- Role of the Designated Router on page 248
- Path Cost Metrics on page 249
- Areas and Area Border Routers on page 249
- Role of the Backbone Area on page 250
- Stub Areas and Not-So-Stubby Areas on page 251

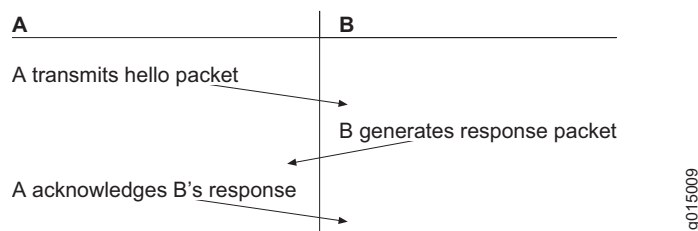


**NOTE:** The J-series Services Router supports both OSPF version 2 and OSPF version 3. In this guide, the term OSPF refers to both versions of the protocol.

## Link-State Advertisements

OSPF creates a topology map by flooding link-state advertisements (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 45.

**Figure 45: OSPF Three-Way Handshake**



In Figure 45, 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.

## Role of the Designated Router

Large local area networks (LANs) that have many routers and therefore many OSPF adjacencies can produce heavy control-packet traffic as LSAs are flooded across the network. To alleviate the potential traffic problem, OSPF uses designated routers (DRs). 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 (BDR). If the designated router fails or loses connectivity, the BDR assumes its role and a new BDR election takes place between all the routers in the OSPF network.

## **Path Cost Metrics**

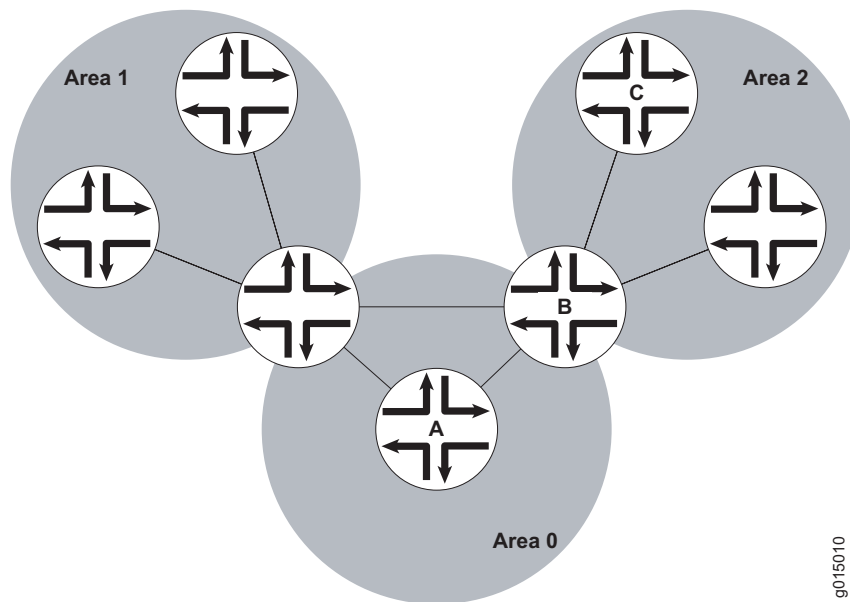
Once the topology is shared across the network, OSPF uses it to route packets between network nodes. Each path between neighbors is assigned a cost based on the throughput, round-trip time, and reliability of the link. The sum of the costs across a particular path between hosts determines the overall 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.

OSPF allows you to manually assign a cost (or metric) to a particular path segment to control the flow of packets across the network.

## **Areas and Area Border Routers**

The OSPF networks in an 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, 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. 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 46 shows an OSPF topology of three areas connected by two area border routers.

**Figure 46: Multiarea OSPF Topology**

g015010

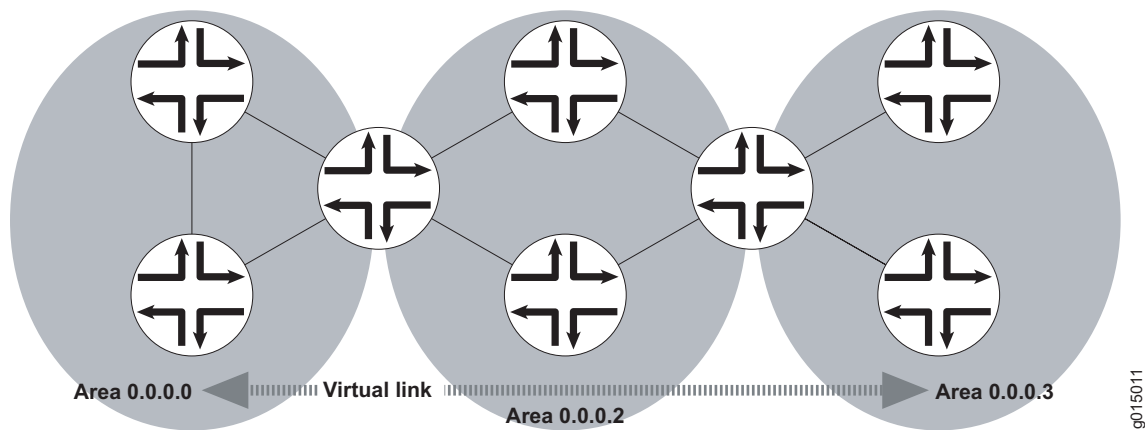
Area border routers are responsible for sharing topology information between areas. They summarize the link-state records of each area and advertise destination address summaries to neighboring areas. The advertisements contain the ID of the area in which each destination lies, so that packets are routed to the appropriate area border router. For example, in the OSPF areas shown in Figure 46, packets sent from router A to router C are automatically routed through area border router B.

### **Role of the Backbone Area**

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 area border router 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 47 shows a virtual link between a noncontiguous area and the backbone area through an area connected to both.

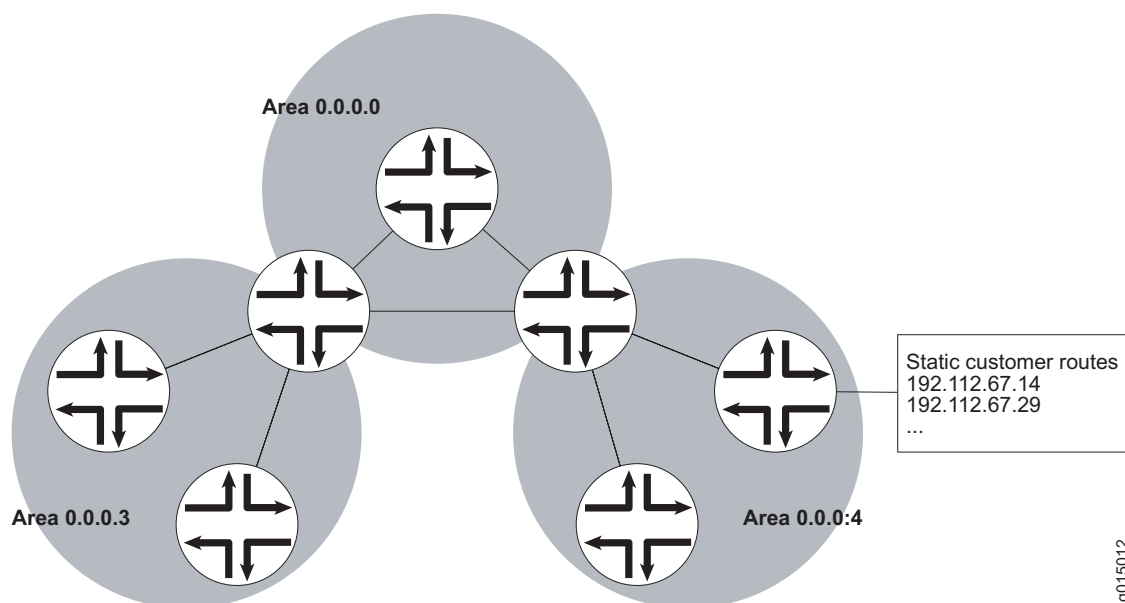


**Figure 47: OSPF Topology with a Virtual Link**

In the topology shown in Figure 47, 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 area border router. All inbound traffic destined for area 0.0.0.3 is routed to the backbone area and then through area 0.0.0.2.

### **Stub Areas and Not-So-Stubby Areas**

Figure 48 shows an AS across which many external routes are advertised. If external routes make up a significant portion of a topology database, you can suppress the advertisements in areas that do not have links outside the network. By doing so, you can reduce the amount of memory the nodes use to maintain the topology database and free it for other uses.

**Figure 48: OSPF AS Network with Stub Areas and NSSAs**

g015012

To control the advertisement of external routes into an area, OSPF uses stub areas. By designating an area border router interface to the area as a stub interface, you suppress external route advertisements through the area border router. Instead, the area border router automatically advertises a default route (through itself) in place of the external routes. Packets destined for external routes are automatically sent to the area border router, which acts as a gateway for outbound traffic and routes them appropriately.

For example, area 0.0.0.3 in Figure 48 is not directly connected to the outside network. All outbound traffic is routed through the area border router to the backbone and then to the destination addresses. By designating area 0.0.0.3 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.

Like area 0.0.0.3 in Figure 48, 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.

## 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.

This overview contains the following topics:

- IS-IS Areas on page 253
- Network Entity Titles and System Identifiers on page 253
- IS-IS Path Selection on page 254
- Protocol Data Units on page 254

## **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.

## **Network Entity Titles and System Identifiers**

In IS-IS, special network addresses are called network entity titles (NETs) and 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.

### **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 Services Router receives a CSNP, it checks the database entries against its own local link-state database. If it detects missing information, the router 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 Services Router 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.

## BGP Overview

---

The Border Gateway Protocol (BGP) is an exterior gateway protocol (EGP) used primarily to establish point-to-point connections and transmit data between peer ASs. Unlike the IGPs RIP, OSPF and IS-IS, 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:

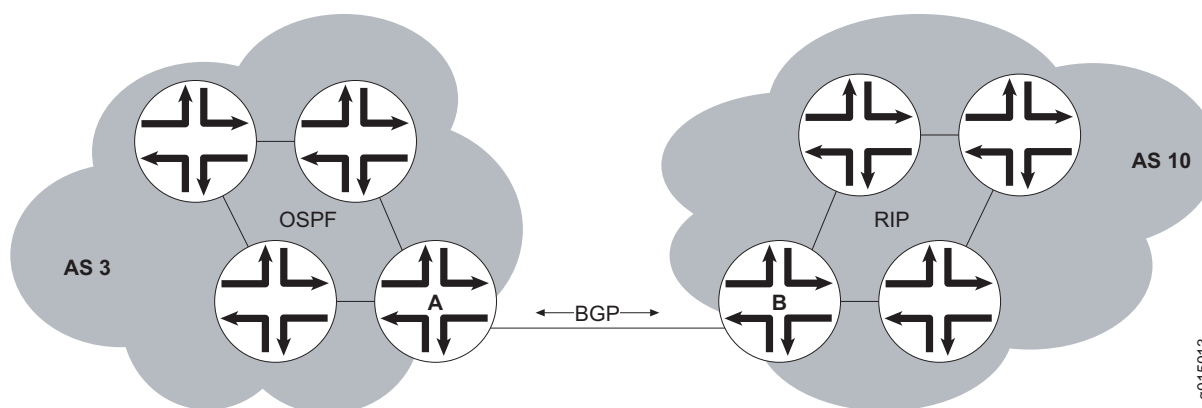
- Point-to-Point Connections on page 256
- BGP Messages for Session Establishment on page 256
- BGP Messages for Session Maintenance on page 257
- IBGP and EBGP on page 257
- Route Selection on page 258
- Local Preference on page 258
- AS Path on page 259

- Origin on page 260
- Multiple Exit Discriminator on page 260
- Scaling BGP for Large Networks on page 261

### Point-to-Point Connections

To establish point-to-point connections between peer ASs, you configure a BGP session on each interface of a point-to-point link. Figure 49 shows an example of a BGP peering session.

**Figure 49: BGP Peering Session**



In Figure 49, 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.

### 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 a 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 EBG**

BGP uses two primary modes of information exchange, internal BGP (IBGP) and external BGP (EBGP), to communicate with internal and external peers, respectively.

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 EBG 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 EBG.

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. Instead, BGP requires that all internal peers be fully meshed so that any route advertised by one router is advertised to all peers within the AS.

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.

For information about route reflection, see “Scaling BGP for Large Networks” on page 261. For information about routing confederations, see “Scaling BGP for Large Networks” on page 261.

## **Route Selection**

A local BGP router uses the following primary criteria to select a route from the routing table for the forwarding table:

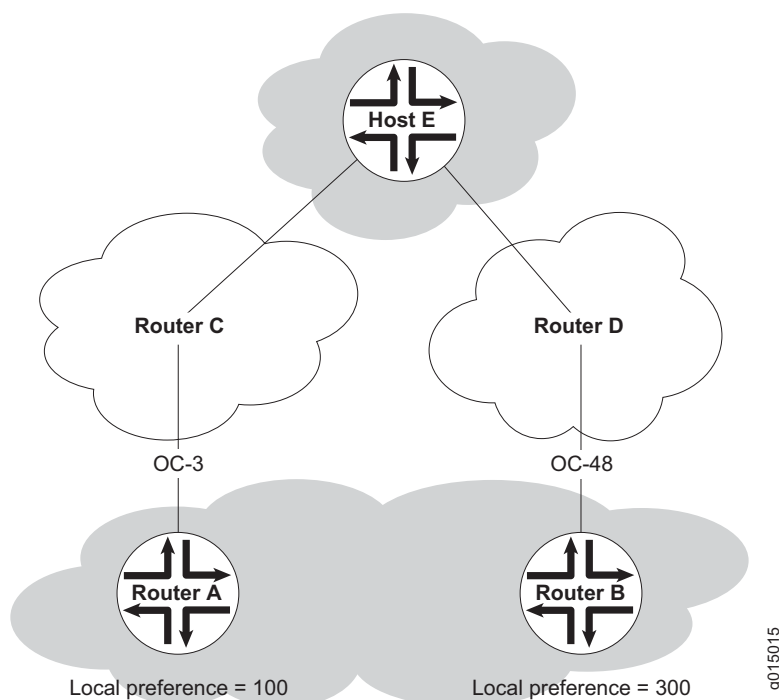
1. **Next-hop accessible**—If the next hop is inaccessible, the local router does not consider the route. The router must verify that it has a route to the BGP next-hop address. If a local route to the next hop does not exist, the local route does not include the router in its forwarding table. If such 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. (For more information, see “Local Preference” on page 258.)
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. (For more information, see “AS Path” on page 259.)
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. (For more information, see “Origin” on page 260.)
5. **Lowest MED value**—The local router selects the route with the lowest multiple exit discriminator (MED) value. If multiple routes have the same MED value, route selection continues. (For more information, see “Multiple Exit Discriminator” on page 260.)

If more than one route remains after all these criteria are evaluated, the local BGP router evaluates a set of secondary criteria to select the single route to a destination for its forwarding table. The secondary criteria include whether the route was learned through an EBGp or Ibgp, the Igp route metric, and the router ID.

## **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 50 illustrates how to use local preference to determine BGP route selection.



**Figure 50: Local Preference**

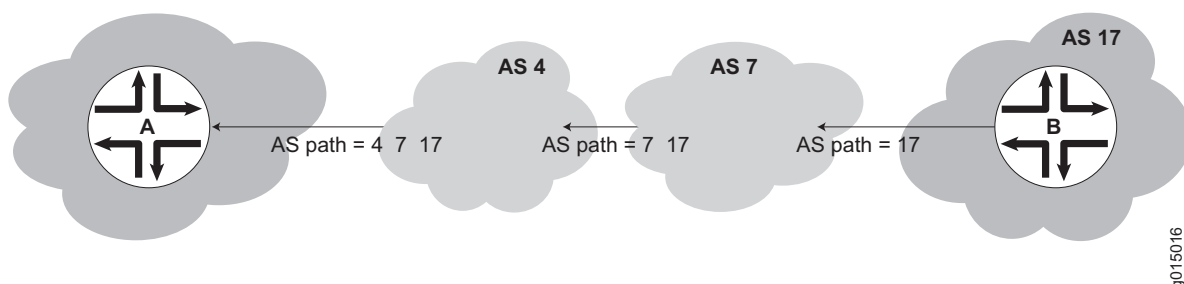
The network in Figure 50 shows two possible routes to the prefixes accessible through host E. The first route, through router A, uses an OC3 link to router C and is then forwarded to host E. The second route, through router B, uses an OC48 link to router D and is then forwarded to host E. Although the 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.

## 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 51 shows how BGP creates an AS path.

**Figure 51: BGP AS Path**

In the network shown in Figure 51, 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 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

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 neighbor AS can have multiple equivalent AS paths. When the routing table contains two routes to the same host in a neighboring AS, a multiple exit discriminator (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 52 illustrates how to use an MED metric to determine route selection.

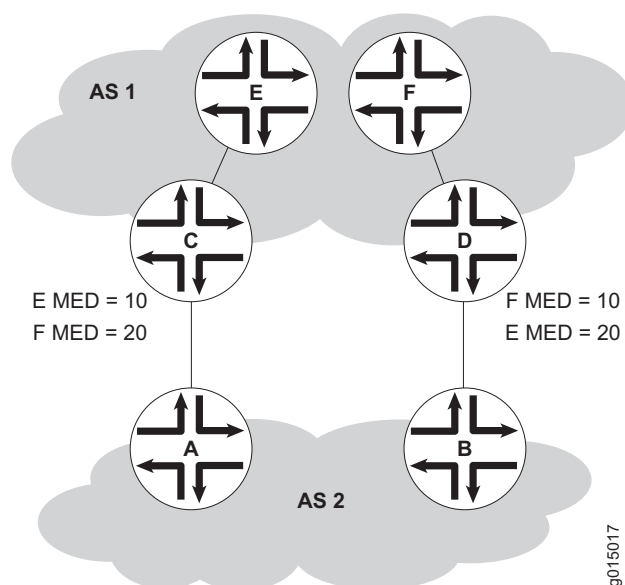
**Figure 52: MED Example**

Figure 52 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 router C. Host F also in AS 1, and is located nearer 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, 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.

## 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 with the following methods:

- Route Reflectors—for Added Hierarchy on page 261
- Confederations—for Subdivision on page 264

### Route Reflectors—for Added Hierarchy

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 53.



**NOTE:** You must have an Advanced BGP Feature license installed on each Services Router that uses a route reflector. For license details, see the *J-series Services Router Administration Guide*.

**Figure 53: Simple Route Reflector Topology (One Cluster)**

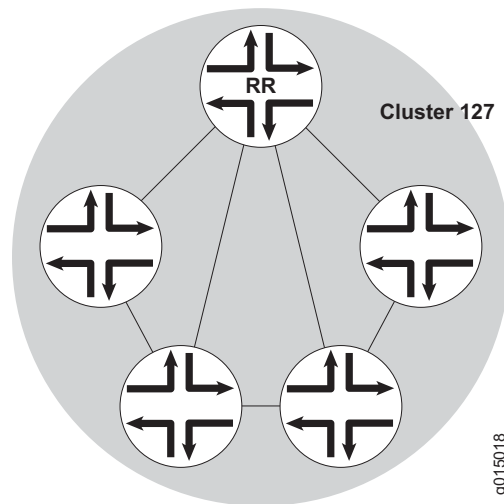


Figure 53 shows router RR configured as the route reflector for cluster 127. The other routers are designated internal peers within the cluster. BGP routes are advertised to router RR by any of the internal peers. RR then readvertises those routes to all other peers within the cluster.

You can configure multiple clusters and link them by configuring a full mesh of route reflectors (see Figure 54).

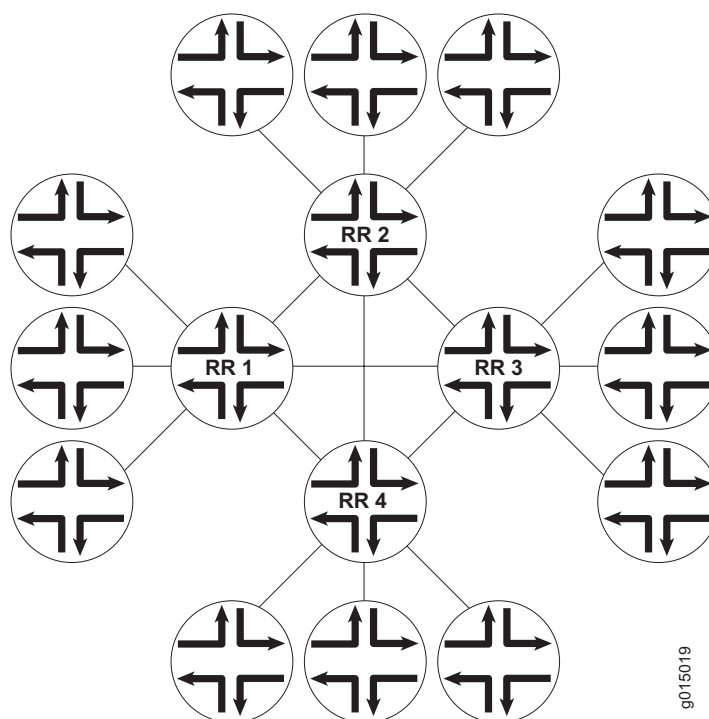
**Figure 54: Basic Route Reflection (Multiple Clusters)**

Figure 54 shows route reflectors RR1, RR2, RR3, and RR4 as fully meshed internal peers. When a router advertises a route to reflector 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 55).

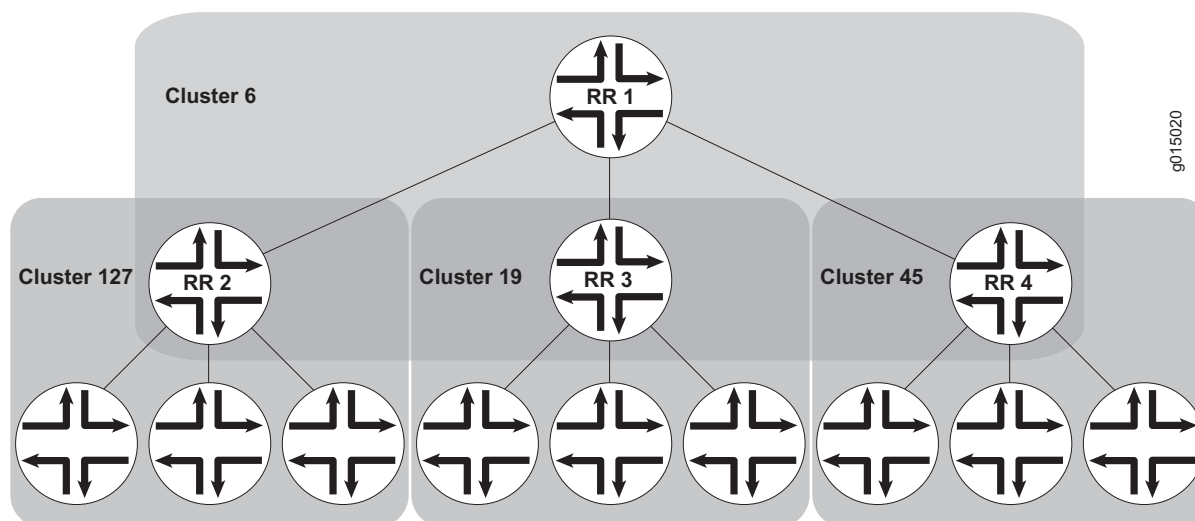
**Figure 55: Hierarchical Route Reflection (Clusters of Clusters)**

Figure 55 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.

### Confederations—for Subdivision

BGP confederations are another way to solve the scaling problems created by the BGP full mesh requirement. BGP confederations effectively break up a large 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 64512 and 65535.

Within a sub-AS, the same IBGP full mesh requirement exists. Connections to other confederations are made with standard 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 56 shows an AS divided into four confederations.

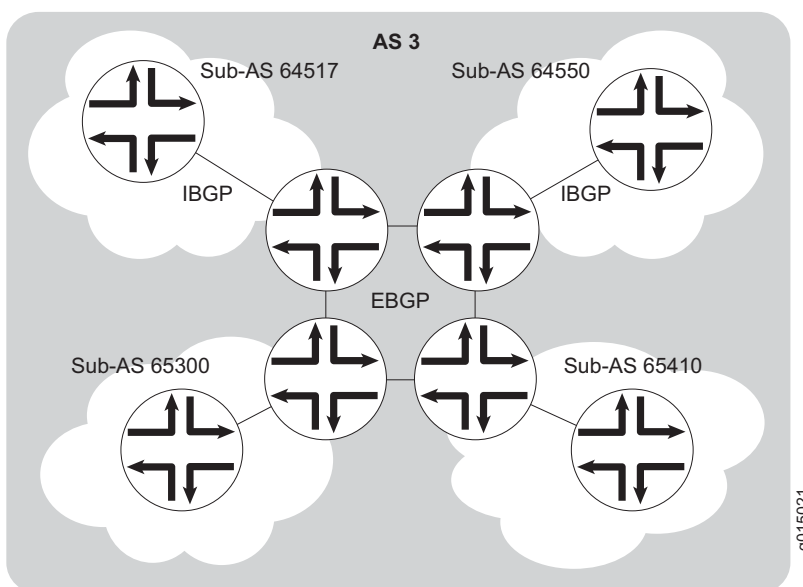
**Figure 56: BGP Confederations**

Figure 56 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.





## Chapter 8

# Configuring Static Routes

Static routes are routes that you explicitly enter into the routing table as permanent additions. Traffic through static routes is always routed the same way.

You can use either J-Web Quick Configuration or a configuration editor to configure static routes.

This chapter contains the following topics. For more information about static routes, see the *JUNOS Routing Protocols Configuration Guide*.

- Static Routing Overview on page 267
- Before You Begin on page 270
- Configuring Static Routes with Quick Configuration on page 270
- Configuring Static Routes with a Configuration Editor on page 272
- Verifying the Static Route Configuration on page 277

## Static Routing Overview

---

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.

This overview contains the following topics:

- Static Route Preferences on page 268
- Qualified Next Hops on page 268
- Control of Static Routes on page 268
- Default Properties on page 269

## Static Route Preferences

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.

## Qualified Next Hops

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:

```
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.

## Control of Static Routes

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 Services Router reboots. For more information, see “Route Retention” on page 269.
- **no-readvertise**—Prevents the route from being readvertised to other routing protocols. For more information, see “Readvertisement Prevention” on page 269.
- **passive**—Rejects traffic destined for the route. For more information, see “Forced Rejection of Passive Route Traffic” on page 269.

## 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.

## 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:

```
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.

## Before You Begin

Before you begin configuring static routes, complete the following tasks:

- Establish basic connectivity. See the *J-series Services Router Getting Started Guide*.
- Configure network interfaces. See “Configuring Network Interfaces” on page 99.

## Configuring Static Routes with Quick Configuration

J-Web Quick Configuration allows you to configure static routes. Figure 57 shows the Quick Configuration Routing page for static routing.

**Figure 57: Quick Configuration Routing Page for Static Routing**

The screenshot shows the Juniper J-Web interface for a J4300 router. The user is logged in as 'regress'. The navigation menu on the left includes 'Monitor', 'Configuration', 'Diagnose', and 'Manage'. Under 'Configuration', the 'Quick Configuration' section is expanded, showing options like 'Set Up', 'SSL', 'Interfaces', 'Users', 'SNMP', 'Routing', 'Firewall/NAT', 'IPSec Tunnels', and 'Realtime Performance Monitoring'. The 'Routing' section is selected, and the 'Quick Configuration' page is displayed. The page title is 'ROUTER - J4300'. The breadcrumb trail is 'Configuration > Quick Configuration > Routing'. The 'Quick Configuration' section is titled 'Routing'. Below this, there is a 'Default Route' section with a text input field. The 'Static Routes' section contains a table with columns 'Static Route Address' and 'Next Hop'. The table lists six static routes, each with a checkbox in the first column. The routes are: 10.74.10.0/24, 172.16.0.0/12, 192.168.0.0/18, 192.168.64.0/18, 207.17.136.192/32, and 192.168.40.0/22. All routes have a next hop of 192.168.124.254. At the bottom of the table are 'Add...' and 'Delete' buttons.

Juniper NETWORKS

ROUTER - J4300

Logged in as: regress

[Help](#) [About](#) [Logout](#)

Monitor Configuration Diagnose Manage

Configuration > Quick Configuration > Routing

Quick Configuration

Routing

Default Route

Default Route

Static Routes

|                          | Static Route Address              | Next Hop        |
|--------------------------|-----------------------------------|-----------------|
| <input type="checkbox"/> | <a href="#">10.74.10.0/24</a>     |                 |
| <input type="checkbox"/> | <a href="#">172.16.0.0/12</a>     | 192.168.124.254 |
| <input type="checkbox"/> | <a href="#">192.168.0.0/18</a>    | 192.168.124.254 |
| <input type="checkbox"/> | <a href="#">192.168.64.0/18</a>   | 192.168.124.254 |
| <input type="checkbox"/> | <a href="#">207.17.136.192/32</a> | 192.168.124.254 |
| <input type="checkbox"/> | <a href="#">192.168.40.0/22</a>   | 192.168.124.254 |

Add... Delete

To configure static routes with Quick Configuration:

1. In the J-Web user interface, select **Configuration > Routing > Static Routing**.
2. Enter information into the Static Routing Quick Configuration page, as described in Table 63.
3. From the main static routing Quick Configuration page, click one of the following buttons:
  - To apply the configuration and stay on the Quick Configuration Routing page for static routing, click **Apply**.
  - To apply the configuration and return to the Quick Configuration Routing page, click **OK**.
  - To cancel your entries and return to the Quick Configuration Routing page, click **Cancel**.
4. To check the configuration, see “Verifying the Static Route Configuration” on page 277.

**Table 63: Static Routing Quick Configuration Summary**

| Field                           | Function                                                                                         | Your Action                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|--------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default Route</b>            |                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Default Route                   | Specifies the default gateway for the router.                                                    | Type the 32-bit IP address of the Services Router's default route in dotted decimal notation.                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Static Routes</b>            |                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Static Route Address (required) | Specifies the static route to add to the routing table.                                          | <ol style="list-style-type: none"> <li>1. On the main static routing Quick Configuration page, click <b>Add</b>.</li> <li>2. In the Static Route Address box, type the 32-bit IP address of the static route in dotted decimal notation.</li> </ol>                                                                                                                                                                                                             |
| Next-Hop Addresses              | Specifies the next-hop address or addresses to be used when routing traffic to the static route. | <ol style="list-style-type: none"> <li>1. In the Add box, type the 32-bit IP address of the next-hop host.</li> <li>2. Click <b>Add</b>.</li> <li>3. Add more next-hop addresses as necessary.</li> </ol> <p><b>NOTE:</b> If a route has multiple next-hop addresses, traffic is routed across each address in round-robin fashion.</p> <ol style="list-style-type: none"> <li>4. When you have finished adding next-hop addresses, click <b>OK</b>.</li> </ol> |

## Configuring Static Routes with a Configuration Editor

To configure static routes on the Services Router, you must perform the following tasks marked *(Required)*.

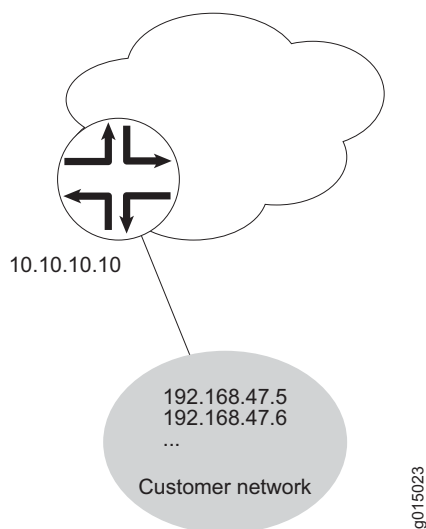
- Configuring a Basic Set of Static Routes (Required) on page 272
- Controlling Static Route Selection (Optional) on page 273
- Controlling Static Routes in the Routing and Forwarding Tables (Optional) on page 275
- Defining Default Behavior for All Static Routes (Optional) on page 276

For information about using the J-Web and CLI configuration editors, see “Using J-Web Configuration Tools” on page 3.

### Configuring a Basic Set of Static Routes (Required)

Customer routes that are connected to stub networks are often configured as static routes. Figure 58 shows a sample network.

**Figure 58: Customer Routes Connected to a Stub Network**



To configure customer routes as static routes, like the ones in Figure 58, follow these steps on the Services Router to which the customer routes are connected:

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 64.

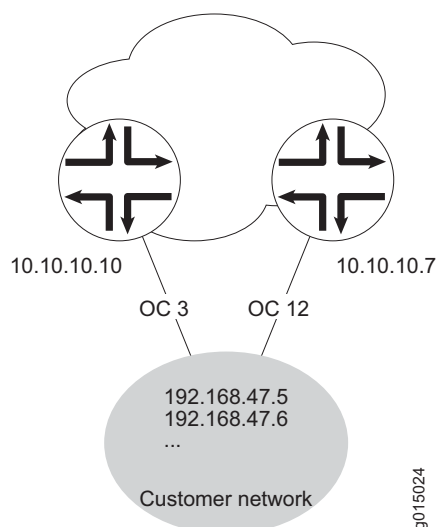
3. If you are finished configuring the router, commit the configuration.
4. Go on to one of the following procedures:
  - To manually control static route selection, see “Controlling Static Route Selection (Optional)” on page 273.
  - To determine how static routes are imported into the routing and forwarding tables, see “Controlling Static Routes in the Routing and Forwarding Tables (Optional)” on page 275.
  - To define default properties for static routes, see “Defining Default Behavior for All Static Routes (Optional)” on page 276.
  - To check the configuration, see “Verifying the Static Route Configuration” on page 277.

**Table 64: Configuring Basic Static Routes**

| Task                                                                                               | J-Web Configuration Editor                                                                                                                                                                                                                                                                                                                                                 | CLI Configuration Editor                                                                                        |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Navigate to the <b>Static</b> level in the configuration hierarchy.                                | In the configuration editor hierarchy, select <b>Routing options &gt; Static</b> .                                                                                                                                                                                                                                                                                         | From the top of the configuration hierarchy, enter<br><br>edit routing-options static                           |
| Add the static route <b>192.168.47.5/32</b> , and define the next-hop address <b>10.10.10.10</b> . | <ol style="list-style-type: none"> <li>1. Next to Route, click <b>Add new entry</b>.</li> <li>2. In the Destination box, type <b>192.168.47.5/32</b>.</li> <li>3. From the Next hop list, select <b>Next hop</b>.</li> <li>4. Next to Next hop, click <b>Add new entry</b>.</li> <li>5. In the Value box, type <b>10.10.10.10</b>.</li> <li>6. Click <b>OK</b>.</li> </ol> | Define the static route and set the next-hop address:<br><br><b>set route 192.168.47.5 next-hop 10.10.10.10</b> |

### Controlling Static Route Selection (Optional)

When multiple next hops exist for a single static route (see Figure 59), you can specify how traffic is to be routed to the destination.

**Figure 59: Controlling Static Routes in the Routing and Forwarding Tables**

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 in either the J-Web or the CLI configuration editor.
2. Perform the configuration tasks described in Table 65.
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 “Controlling Static Routes in the Routing and Forwarding Tables (Optional)” on page 275.
  - To define default properties for static routes, see “Defining Default Behavior for All Static Routes (Optional)” on page 276.
  - To check the configuration, see “Verifying the Static Route Configuration” on page 277.



**Table 65: Controlling Static Route Selection**

| <b>Task</b>                                                                                        | <b>J-Web Configuration Editor</b>                                                                                                                                                                                                                                                                                                                           | <b>CLI Configuration Editor</b>                                                                                 |
|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Navigate to the <b>Static</b> level in the configuration hierarchy.                                | In the configuration editor hierarchy, select <b>Routing options &gt; Static</b> .                                                                                                                                                                                                                                                                          | From the top of the configuration hierarchy, enter<br><br>edit routing-options static                           |
| Add the static route <b>192.168.47.5/32</b> , and define the next-hop address <b>10.10.10.10</b> . | <ol style="list-style-type: none"> <li>Next to Route, click <b>Add new entry</b>.</li> <li>In the Destination box, type <b>192.168.47.5/32</b>.</li> <li>From the Next hop list, select <b>Next hop</b>.</li> <li>In the Next hop box, click <b>Add new entry</b>.</li> <li>In the Value box, type <b>10.10.10.10</b>.</li> <li>Click <b>OK</b>.</li> </ol> | Define the static route and set the next-hop address:<br><br><b>set route 192.168.47.5 next-hop 10.10.10.10</b> |
| Set the preference for the <b>10.10.10.10</b> next hop to <b>7</b> .                               | <ol style="list-style-type: none"> <li>Next to Preference, select the <b>Yes</b> check box.</li> <li>Click <b>Configure</b>.</li> <li>In the Metric value box, type <b>7</b>.</li> <li>Click <b>OK</b>.</li> </ol>                                                                                                                                          | Set the preference to 7:<br><br><b>set route 192.168.47.5 next-hop 10.10.10.10 preference 7</b>                 |
| Define the qualified next-hop address <b>10.10.10.7</b> .                                          | <ol style="list-style-type: none"> <li>Next to Qualified next hop, click <b>Add new entry</b>.</li> <li>In the Nexthop box, type <b>10.10.10.7</b>.</li> </ol>                                                                                                                                                                                              | Set the qualified-next-hop address:<br><br><b>set route 192.168.47.5 qualified-next-hop 10.10.10.7</b>          |
| Set the preference for the <b>10.10.10.7</b> qualified next hop to <b>6</b> .                      | <ol style="list-style-type: none"> <li>In the Preference box, type <b>6</b>.</li> <li>Click <b>OK</b>.</li> </ol>                                                                                                                                                                                                                                           | Set the preference to 6:<br><br><b>set route 192.168.47.5 qualified-next-hop 10.10.10.7 preference 6</b>        |

### **Controlling Static Routes in the Routing and Forwarding Tables (Optional)**

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:

- Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
- Perform the configuration tasks described in Table 66.
- If you are finished configuring the router, commit the configuration.
- Go on to one of the following procedures:

- To define default properties for static routes, see “Defining Default Behavior for All Static Routes (Optional)” on page 276.
- To check the configuration, see “Verifying the Static Route Configuration” on page 277.

**Table 66: Controlling Static Routes in the Routing and Forwarding Tables**

| Task                                                                                                                                                                       | J-Web Configuration Editor                                                                                                                     | CLI Configuration Editor                                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Navigate to the <b>192.168.47.5/32</b> level in the configuration hierarchy.                                                                                               | In the configuration editor hierarchy, select <b>Routing options &gt; Static</b> , then click <b>192.168.47.5/32</b> in the Destination field. | From the top of the configuration hierarchy, enter<br><br>edit routing-options static route 192.168.47.5/32 |
| 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.                         | Next to Retain, select the <b>Yes</b> check box.                                                                                               | Set the <b>retain</b> attribute:<br><br>set retain                                                          |
| Specify that the static route is not to be readvertised. By default, static routes are eligible to be readvertised.                                                        | Next to Readvertise, select the <b>No</b> check box.                                                                                           | Set the <b>no-readvertise</b> attribute:<br><br>set no-readvertise                                          |
| 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. | <ol style="list-style-type: none"> <li>1. From the Passive flag list, select <b>Passive</b>.</li> <li>2. Click <b>OK</b>.</li> </ol>           | Set the <b>passive</b> attribute:<br><br>set passive                                                        |

### Defining Default Behavior for All Static Routes (Optional)

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. To configure static route defaults, perform these steps:

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 67.
3. If you are finished configuring the router, commit the configuration.
4. To check the configuration, see “Verifying the Static Route Configuration” on page 277.

**Table 67: Defining Static Route Defaults**

| Task                                                                                                                                                                       | J-Web Configuration Editor                                                                                                     | CLI Configuration Editor                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Navigate to the <b>Defaults</b> level in the configuration hierarchy.                                                                                                      | In the configuration editor hierarchy, select <b>Protocols &gt; Static</b> , and then click <b>Configure</b> next to Defaults. | From the top of the configuration hierarchy, enter<br><br>edit routing-options static defaults |
| 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.                         | 1. Next to Retain, select the <b>Yes</b> check box.<br>2. Click <b>OK</b> .                                                    | Set the <b>retain</b> attribute:<br><br>set retain                                             |
| Specify that the static route is not to be readadvertised. By default, static routes are eligible to be readadvertised.                                                    | 1. Next to Readvertise, select the <b>No</b> check box.<br>2. Click <b>OK</b> .                                                | Set the <b>no-readvertise</b> attribute:<br><br>set no-readvertise                             |
| 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. | 1. From the Passive flag list, select <b>Passive</b> .<br>2. Click <b>OK</b> .                                                 | Set the <b>passive</b> attribute:<br><br>set passive                                           |

## Verifying the Static Route Configuration

Verify that the static routes are in the routing table and that those routes are active.

### Displaying the Routing Table

**Purpose** Verify static route configuration as follows by displaying the routing table and checking its contents.

**Action** From the CLI, enter the show route terse command.

**Sample Output**

```

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           >fe-0/0/1.0
* 192.168.220.5/32     L   0           Local
* 192.168.220.8/30     D   0           >fe-0/0/2.0
* 192.168.220.9/32     L   0           Local
* 192.168.220.12/30    D   0           >fe-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

```

**What It Means** 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.

## Chapter 9

# Configuring a RIP Network

The Routing Information Protocol (RIP) is an interior gateway protocol that routes packets within a single autonomous system (AS). To use RIP, you must understand the basic components of a RIP network and configure the J-series Services Router to act as a node in the network.



**NOTE:** The J-series Services Router supports RIP version 1 (RIPv1) and RIP version 2 (RIPv2) only. Unless otherwise specified, the term *RIP* in this chapter refers to these versions of the protocol.

You can use either J-Web Quick Configuration or a configuration editor to configure a RIP network.

This chapter contains the following topics. For more information about RIP, see the *JUNOS Routing Protocols Configuration Guide*.

- RIP Overview on page 279
- Before You Begin on page 280
- Configuring a RIP Network with Quick Configuration on page 280
- Configuring a RIP Network with a Configuration Editor on page 283
- Verifying the RIP Configuration on page 291

## RIP 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. To enable RIP on an interface, you define RIP groups, which are logical groupings of interfaces, and add interfaces to the groups. Additionally, you must configure a routing policy to export directly connected routes and routes learned through RIP routing exchanges.

## 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.

## Authentication

RIPv2 provides authentication support so that RIP links can require authentication keys (passwords) before they become active. These authentication keys can be specified in either plain-text or MD5 form. Authentication provides an additional layer of security on the network beyond the other security features.

This type of authentication is not supported on RIPv1 networks.

## Before You Begin

---

Before you begin configuring a RIP network, complete the following tasks:

- Establish basic connectivity. See the *J-series Services Router Getting Started Guide*.
- Configure network interfaces. See “Configuring Network Interfaces” on page 99.

## Configuring a RIP Network with Quick Configuration

---

J-Web Quick Configuration allows you to create RIP networks. Figure 60 shows the Quick Configuration Routing page for RIP.

**Figure 60: Quick Configuration Routing Page for RIP**

Juniper NETWORKS **ROUTER - J4300** Logged in as: **regress**  
[Help](#) [About](#) [Logout](#)

**Monitor** **Configuration** **Diagnose** **Manage**

[Configuration](#) > [Quick Configur](#)

**Quick Configuration**

Set Up  
 SSL  
 Interfaces  
 Users  
 SNMP  
**Routing**  
 Firewall/NAT  
 IPSec Tunnels  
 Realtime Performance Monitoring

► **View and Edit**  
 ► **History**  
 ► **Rescue**

**Quick Configuration**

**Routing**

**RIP**

**Enable RIP** ☐ ?

**Advertise Default Route** ☐ ?

**RIP-Enabled Interfaces**

**RIP Interfaces**

**Logical Int**

fe-0/0/0.0  
 fxp0.0  
 lo0.0

OK Cancel Apply

Copyright © 2004-2005, Juniper Networks, Inc. All Rights Reserved. [Trademark Notice](#).

To configure a RIP network with Quick Configuration:

1. In the J-Web user interface, select **Configuration > Routing > RIP Routing**.
2. Enter information into the Quick Configuration page for RIP, as described in Table 68.
3. From the main RIP routing Quick Configuration page, click one of the following buttons:
  - To apply the configuration and stay on the Quick Configuration Routing page for RIP, click **Apply**.
  - To apply the configuration and return to the Quick Configuration Routing page, click **OK**.
  - To cancel your entries and return to the Quick Configuration Routing page, click **Cancel**.

4. To check the configuration, see “Verifying the RIP Configuration” on page 291.

**Table 68: RIP Routing Quick Configuration Summary**

| Field                   | Function                                                                   | Your Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RIP</b>              |                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Enable RIP              | Enables or disables RIP.                                                   | <ul style="list-style-type: none"> <li>■ To enable RIP, select the check box.</li> <li>■ To disable RIP, clear the check box.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Advertise Default Route | Advertises the default route using RIPv2.                                  | <ul style="list-style-type: none"> <li>■ To advertise the default route using RIPv2, select the check box.</li> <li>■ To disable the default route advertisement, clear the check box.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| RIP-Enabled Interfaces  | Designates one or more Services Router interfaces on which RIP is enabled. | <p>The first time you configure RIP, the Logical Interfaces box displays a list of all the logical interfaces configured on the Services Router. Do any of the following:</p> <ul style="list-style-type: none"> <li>■ To enable RIP on an interface, click the interface name to highlight it, and click the left arrow to add the interface to the RIP interfaces list.</li> <li>■ To enable RIP on multiple interfaces at once, press Ctrl while you click multiple interface names to highlight them. Then click the left arrow to add the interfaces to the RIP interfaces list.</li> <li>■ To enable RIP on all logical interfaces except the special <b>fxp0</b> management interface, select <b>All Interfaces</b> in the Logical Interfaces list and click the left arrow.</li> <li>■ To enable RIP on all the interfaces displayed in the Logical Interfaces list, click <b>All</b> to highlight every interface. Then click the left arrow to add the interfaces to the RIP interfaces list.</li> <li>■ To disable RIP on one or more interfaces, highlight the interface or interfaces in the RIP interfaces box and click the right arrow to move them back to the Logical Interfaces list.</li> </ul> |



## Configuring a RIP Network with a Configuration Editor

To configure the Services Router as a node in a RIP network, you must perform the following task marked *(Required)*.

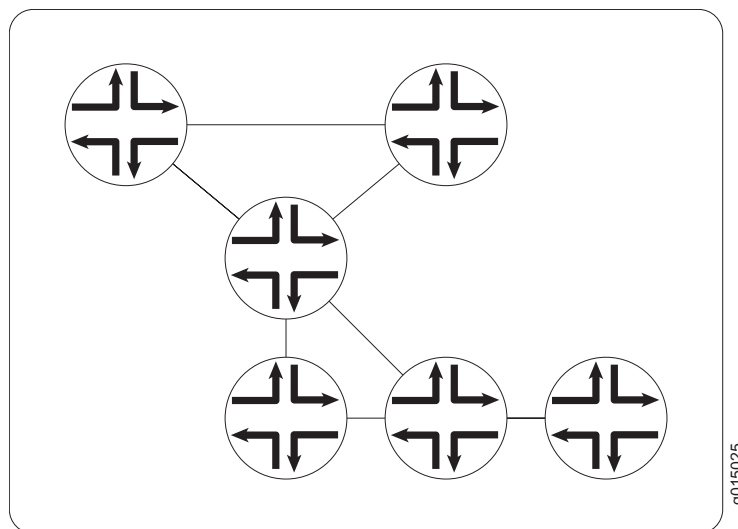
- Configuring a Basic RIP Network (Required) on page 283
- Controlling Traffic in a RIP Network (Optional) on page 286
- Enabling Authentication for RIP Exchanges (Optional) on page 289

For information about using the J-Web and CLI configuration editors, see “Using J-Web Configuration Tools” on page 3.

### Configuring a Basic RIP Network (Required)

To use RIP on the Services Router, you must configure RIP on all the RIP interfaces within a network like the one shown in Figure 61.

**Figure 61: Typical RIP Network Topology**



By default, RIP does not advertise the subnets that are directly connected through the Services Router'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.

To configure a RIP network like the one in Figure 61, with a routing policy, perform these steps on each Services Router in the network:

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 69.
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.

4. Go on to one of the following procedures:
  - To control RIP traffic on the network, see “Controlling Traffic in a RIP Network (Optional)” on page 286.
  - To authenticate RIP exchanges, see “Enabling Authentication for RIP Exchanges (Optional)” on page 289.
  - To check the configuration, see “Verifying the RIP Configuration” on page 291.

**Table 69: Configuring a RIP Network**

| Task                                                             | J-Web Configuration Editor                                                                                                                                                                                                                                                                                                                                                                   | CLI Configuration Editor                                                                                                                                                            |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Navigate to the <b>Rip</b> level in the configuration hierarchy. | In the configuration editor hierarchy, select <b>Protocols &gt; Rip</b> .                                                                                                                                                                                                                                                                                                                    | From the top of the configuration hierarchy, enter<br><br>edit protocols rip                                                                                                        |
| Create the RIP group <b>alpha1</b> .                             | <ol style="list-style-type: none"> <li>1. Next to Group, click <b>Add new entry</b>.</li> <li>2. In the Group name box, type <b>alpha1</b>.</li> </ol>                                                                                                                                                                                                                                       | <ol style="list-style-type: none"> <li>1. Create the RIP group <b>alpha1</b>, and add an interface:<br/><br/><b>set group alpha1 neighbor fe-0/0/0.0</b></li> </ol>                 |
| Add interfaces to the RIP group <b>alpha1</b> .                  | <ol style="list-style-type: none"> <li>1. Next to Neighbor, click <b>Add new entry</b>.</li> <li>2. In the Neighbor name box, type the name of an interface on the Services Router—for example, <b>fe-0/0/0.0</b>—and click <b>OK</b>.</li> <li>3. Repeat Step 2 for each interface on this Services Router that you are adding to the RIP group. Only one interface is required.</li> </ol> | <ol style="list-style-type: none"> <li>2. Repeat Step 1 for each interface on this Services Router that you are adding to the RIP group. Only one interface is required.</li> </ol> |

**Table 69: Configuring a RIP Network (continued)**

| <b>Task</b>                                                                 | <b>J-Web Configuration Editor</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <b>CLI Configuration Editor</b>                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure a routing policy to advertise directly connected routes.          | <ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Policy Options</b>.</li> <li>2. Next to Policy statement, click <b>Add new entry</b>.</li> <li>3. In the Policy name box, type the name of the policy statement—for example, <b>advertise-rip-routes</b>.</li> <li>4. Next to Term, click <b>Add new entry</b>.</li> <li>5. In the Term name box, type the name of the policy statement—for example, <b>from-direct</b>.</li> <li>6. Next to From, click <b>Configure</b>.</li> <li>7. Next to Protocol, click <b>Add new entry</b>.</li> <li>8. From the Value list, select <b>Direct</b>.</li> <li>9. Click <b>OK</b> until you return to the Policy statement page.</li> <li>10. Next to Then, click <b>Configure</b>.</li> <li>11. From the Accept reject list, select <b>Accept</b>.</li> <li>12. Click <b>OK</b>.</li> </ol> | <ol style="list-style-type: none"> <li>1. From the top of the configuration hierarchy, enter<br/><code>edit policy-options</code></li> <li>2. Set the match condition to match on direct routes:<br/><code>set policy-statement advertise-rip-routes term from-direct from protocol direct</code></li> <li>3. Set the match action to accept these routes:<br/><code>set policy-statement advertise-rip-routes term from-direct then accept</code></li> </ol> |
| Configure the previous routing policy to advertise routes learned from RIP. | <ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Policy Options</b>.</li> <li>2. Next to Policy statement, click <b>advertise-rip-routes</b>.</li> <li>3. Next to Term, click <b>Add new entry</b>.</li> <li>4. In the Term name box, type the name of the policy statement—for example, <b>from-rip</b>.</li> <li>5. Next to From, click <b>Configure</b>.</li> <li>6. Next to Protocol, click <b>Add new entry</b>.</li> <li>7. From the Value list, select <b>rip</b>.</li> <li>8. Click <b>OK</b> until you return to the Policy statement page.</li> <li>9. Next to Then, click <b>Configure</b>.</li> <li>10. From the Accept reject list, select <b>Accept</b>.</li> <li>11. Click <b>OK</b>.</li> </ol>                                                                                                                     | <ol style="list-style-type: none"> <li>1. From the top of the configuration hierarchy, enter<br/><code>edit policy-options</code></li> <li>2. Set the match condition to match on direct routes:<br/><code>set policy-statement advertise-rip-routes term from-rip from protocol rip</code></li> <li>3. Set the match action to accept these routes:<br/><code>set policy-statement advertise-rip-routes term from-rip then accept</code></li> </ol>          |

## Controlling Traffic in a RIP Network (Optional)

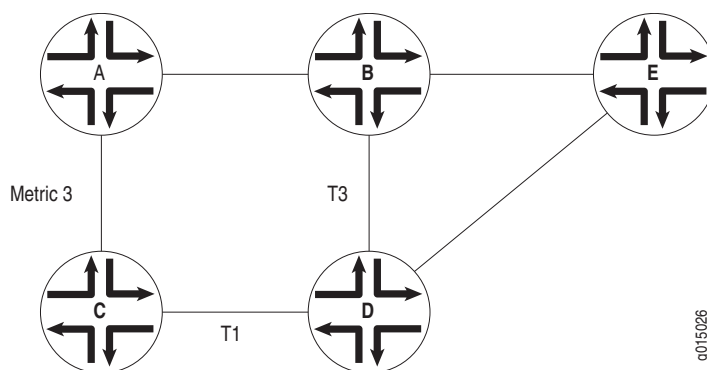
There are two primary means for controlling traffic in a RIP network: the incoming metric and the outgoing metric. To modify these attributes, see the following sections:

- Controlling Traffic with the Incoming Metric on page 286
- Controlling Traffic with the Outgoing Metric on page 287

### Controlling Traffic with the Incoming Metric

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 62 shows a network with alternate routes between routers A and D.

**Figure 62: 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 force traffic through router B:

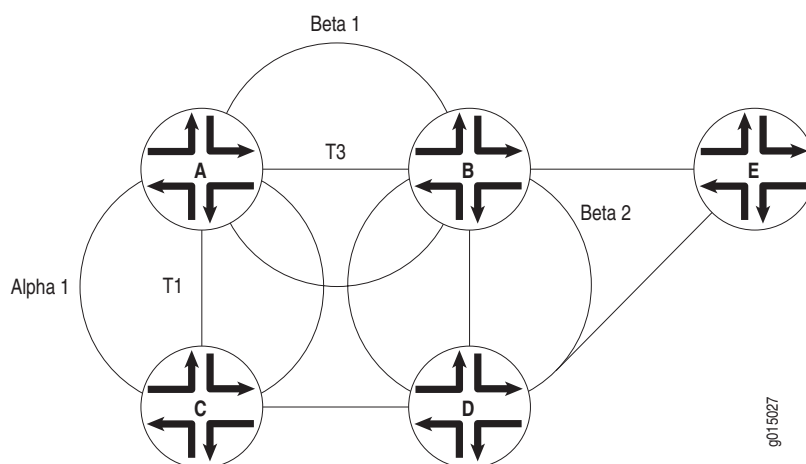
1. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 70.
3. If you are finished configuring the router, commit the configuration.
4. Go on to one of the following procedures:
  - To authenticate RIP exchanges, see “Enabling Authentication for RIP Exchanges (Optional)” on page 289.
  - To check the configuration, see “Verifying the RIP Configuration” on page 291.

Table 70: Modifying the Incoming Metric

| Task                                                                                                  | J-Web Configuration Editor                                                                                                                                                                                                                                                  | CLI Configuration Editor                                                                                    |
|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| In the configuration hierarchy, navigate to the level of an interface in the <b>alpha1</b> RIP group. | <ol style="list-style-type: none"><li>1. In the configuration editor hierarchy, select <b>Protocols &gt; Rip</b>, and click <b>alpha1</b> in the Group name field.</li><li>2. Click the interface name—for example, <b>fe-0/0/0.0</b>—in the Neighbor name field.</li></ol> | From the top of the configuration hierarchy, enter<br><br>edit protocols rip group alpha1 neighbor fe-0/0/0 |
| Increase the incoming metric to <b>3</b> .                                                            | In the Metric in box, type <b>3</b> , and click <b>OK</b> .                                                                                                                                                                                                                 | Set the incoming metric to <b>3</b> :<br><br>set metric-in 3                                                |

Controlling Traffic with the Outgoing Metric

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. Figure 63 shows a network with alternate routes between routers A and D.

**Figure 63: 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 in either the J-Web or CLI configuration editor.
2. Perform the configuration tasks described in Table 71.
3. If you are finished configuring the router, commit the configuration.
4. Go on to one of the following procedures:
  - To authenticate RIP exchanges, see “Enabling Authentication for RIP Exchanges (Optional)” on page 289.
  - To check the configuration, see “Verifying the RIP Configuration” on page 291.

**Table 71: Modifying the Outgoing Metric**

| <b>Task</b>                                                         | <b>J-Web Configuration Editor</b>                                                                                               | <b>CLI Configuration Editor</b>                                                           |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Navigate to the <b>alpha1</b> level in the configuration hierarchy. | In the configuration editor hierarchy, select <b>Protocols &gt; Rip</b> , and then click <b>alpha1</b> in the Group name field. | From the top of the configuration hierarchy, enter<br><br>edit protocols rip group alpha1 |
| Increase the outgoing metric to 3.                                  | In the Metric out box, type <b>3</b> , and click <b>OK</b> .                                                                    | Set the outgoing metric to 3:<br><br>set metric-out 3                                     |

### ***Enabling Authentication for RIP Exchanges (Optional)***

All RIPv2 protocol exchanges can be authenticated to guarantee that only trusted routers participate in the AS's routing. By default, this authentication is disabled. Authentication requires all routers within the RIP network or subnetwork to have the same authentication type and key (password) configured.

You can enable RIP authentication exchanges by either of the following methods:

- Enabling Authentication with Plain-Text Passwords on page 289
- Enabling Authentication with MD5 Authentication on page 290

#### **Enabling Authentication with Plain-Text Passwords**

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 Services Routers in the network:

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 72.
3. If you are finished configuring the router, commit the configuration.
4. To check the configuration, see “Verifying the RIP Configuration” on page 291.

**Table 72: Configuring Simple RIP Authentication**

| <b>Task</b>                                                  | <b>J-Web Configuration Editor</b>                                         | <b>CLI Configuration Editor</b>                                              |
|--------------------------------------------------------------|---------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Navigate to <b>Rip</b> level in the configuration hierarchy. | In the configuration editor hierarchy, select <b>Protocols &gt; Rip</b> . | From the top of the configuration hierarchy, enter<br><br>edit protocols rip |

**Table 72: Configuring Simple RIP Authentication (continued)**

| <b>Task</b>                                                                                                                                                      | <b>J-Web Configuration Editor</b>                                                 | <b>CLI Configuration Editor</b>                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Set the authentication type to <b>simple</b> .                                                                                                                   | From the Authentication type list, select <b>simple</b> .                         | Set the authentication type to <b>simple</b> :<br><br>set authentication-type simple                |
| Set the authentication key to a simple-text password.<br><br>The password can be from 1 through 16 contiguous characters long and can include any ASCII strings. | In the Authentication key box, type a simple-text password, and click <b>OK</b> . | Set the authentication key to a simple-text password:<br><br>set authentication-key <i>password</i> |

## Enabling Authentication with MD5 Authentication

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 Services Routers in the network:

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 73.
3. If you are finished configuring the router, commit the configuration.
4. To check the configuration, see “Verifying the RIP Configuration” on page 291.

**Table 73: Configuring MD5 RIP Authentication**

| <b>Task</b>                                                                                                                                      | <b>J-Web Configuration Editor</b>                                                    | <b>CLI Configuration Editor</b>                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Navigate to <b>Rip</b> level in the configuration hierarchy.                                                                                     | In the configuration editor hierarchy, select <b>Protocols &gt; Rip</b> .            | From the top of the configuration hierarchy, enter<br><br>edit protocols rip   |
| Set the authentication type to <b>MD5</b> .                                                                                                      | From the Authentication type list, select <b>md5</b> .                               | Set the authentication type to <b>md5</b> :<br><br>set authentication-type md5 |
| Set the MD5 authentication key (password).<br><br>The key can be from 1 through 16 contiguous characters long and can include any ASCII strings. | In the Authentication key box, type an MD5 authentication key, and click <b>OK</b> . | Set the MD5 authentication key:<br><br>set authentication-key <i>password</i>  |



## Verifying the RIP Configuration

To verify the RIP configuration, perform these tasks:

- Verifying the RIP-Enabled Interfaces on page 291
- Verifying the Exchange of RIP Messages on page 291
- Verifying Reachability of All Hosts in the RIP Network on page 292

### 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 | Send Address  | Receive Address | In | Mode  | Mode | Met |
|-----------------|-------------------|---------------|-----------------|----|-------|------|-----|
| fe-0/0/0.0      | Dn                | (null)        | (null)          |    | mcast | both | 1   |
| fe-0/0/1.0      | Up                | 192.168.220.5 | 224.0.0.9       |    | mcast | both | 1   |

**What It Means** The output shows a list of the RIP neighbors that are configured on the Services Router. 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 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; update interval 30s; holddown 180s; timeout 120s.
      rts learned  rts held down  rqsts dropped  resps dropped
              10              0              0              0

t1-0/0/2.0: 0 routes learned; 13 routes advertised
Counter              Total  Last 5 min  Last minute
-----
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 |
| RIPv2 Updates Received  | 41 | 0 | 0 |
| RIPv2 Bad Route Entries | 0  | 0 | 0 |
| RIPv2 Updates Ignored   | 0  | 0 | 0 |
| Authentication Failures | 0  | 0 | 0 |
| RIP Requests Received   | 0  | 0 | 0 |
| RIP Requests Ignored    | 0  | 0 | 0 |

| fe-0/0/1.0: 10 routes learned; 3 routes advertised |       |            |             |
|----------------------------------------------------|-------|------------|-------------|
| Counter                                            | Total | Last 5 min | Last minute |
| -----                                              |       |            |             |
| Updates Sent                                       | 2855  | 11         | 2           |
| Triggered Updates Sent                             | 3     | 0          | 0           |
| Responses Sent                                     | 0     | 0          | 0           |
| Bad Messages                                       | 1     | 0          | 0           |
| RIPv1 Updates Received                             | 0     | 0          | 0           |
| RIPv1 Bad Route Entries                            | 0     | 0          | 0           |
| RIPv1 Updates Ignored                              | 0     | 0          | 0           |
| RIPv2 Updates Received                             | 2864  | 11         | 2           |
| RIPv2 Bad Route Entries                            | 14    | 0          | 0           |
| RIPv2 Updates Ignored                              | 0     | 0          | 0           |
| Authentication Failures                            | 0     | 0          | 0           |
| RIP Requests Received                              | 0     | 0          | 0           |
| RIP Requests Ignored                               | 0     | 0          | 0           |

**What It Means**

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 might indicate an authentication error.

## 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 Services Router.

**Action** For each Services Router in the RIP network:

1. In the J-Web interface, select **Diagnose > Traceroute**.
2. In the Remote Host box, type the name of a host for which you want to verify reachability from the Services Router.

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 router-a-fxp0.englab.mycompany.net (192.168.71.246) 0.251 ms 0.235 ms 0.200 ms
```

**What It Means**

Each numbered row in the output indicates a router (“hop”) in the path to the host. The three time increments indicate the round-trip time (RTT) between the Services Router 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.

For information about the `traceroute` command and its output, see the *JUNOS System Basics and Services Command Reference*.



## Chapter 10

# Configuring an OSPF Network

The Open Shortest Path First protocol (OSPF) is an interior gateway protocol (IGP) that routes packets within a single autonomous system (AS). To use OSPF, you must understand the basic components of an OSPF network and configure the J-series Services Router to act as a node in the network.



**NOTE:** The J-series Services Router supports both OSPF version 2 and OSPF version 3. In this chapter, the term *OSPF* refers to both versions of the protocol.

You can use either J-Web Quick Configuration or a configuration editor to configure an OSPF network.

This chapter contains the following topics. For more information about OSPF, see the *JUNOS Routing Protocols Configuration Guide*.

- OSPF Overview on page 295
- Before You Begin on page 297
- Configuring an OSPF Network with Quick Configuration on page 297
- Configuring an OSPF Network with a Configuration Editor on page 299
- Tuning an OSPF Network for Efficient Operation on page 307
- Verifying an OSPF Configuration on page 311

## OSPF Overview

In an OSPF network, the network topology is distributed among the nodes of the autonomous system (AS) and is regularly updated. 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.

### Enabling OSPF

To activate OSPF on a network, you must enable the protocol on all interfaces within the network on which OSPF traffic is to travel. To enable OSPF on

one or more interfaces, you must configure one or more interfaces on the Services Router 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.

## **OSPF Areas**

OSPF is enabled on a per-interface basis. Those interfaces are configured as OSPF enabled, and are assigned to an area. In a simple, single-area network, the area has the numeric identifier 0.0.0.0, which designates it as the backbone area. As the network grows, it is divided into multiple subnetworks or areas that are identified by numeric identifiers unique to the AS.

In a multiarea network, all areas must be directly connected to the backbone area by area border routers (ABRs). 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.

## **Path Cost Metrics**

Once the topology is shared across the network, OSPF uses it 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. 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.

OSPF allows you to manually assign a cost (or metric) to a particular path segment to control the flow of packets across the network.

## **OSPF Dial-on-Demand Circuits**

If you are configuring OSPF across a demand circuit such as an ISDN link, you must enable dial-on-demand routing backup on the OSPF-enabled 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.

To configure an ISDN link, see “Configuring ISDN” on page 187. For information about configuring OSPF demand circuits, see “Configuring Dial-on-Demand Routing Backup with OSPF Support (Optional)” on page 209.

## Before You Begin

Before you begin configuring an OSPF network, complete the following tasks:

- Establish basic connectivity. See the *J-series Services Router Getting Started Guide*.
- Configure network interfaces. See “Configuring Network Interfaces” on page 99.

## Configuring an OSPF Network with Quick Configuration

J-Web Quick Configuration allows you to create single-area OSPF networks. Figure 64 shows the Quick Configuration Routing page for OSPF.

**Figure 64: Quick Configuration Routing Page for OSPF**

Juniper NETWORKS **ROUTER - J4300** Logged in as: **regress**  
[Help](#) [About](#) [Logout](#)

**Monitor Configuration Diagnose Manage**

**Quick Configuration**

Set Up  
SSL  
Interfaces  
Users  
SNMP

**Routing**  
Firewall/NAT  
IPSec Tunnels  
Realtime Performance Monitoring

► **View and Edit**  
► **History**  
► **Rescue**

**Quick Configuration**

**Routing**

**Router Identification**

**Router Identifier**  ?

**OSPF**

**Enable OSPF** ☒

**OSPF Area ID**

**Area Type**  ?

**Enable OSPF on All Interfaces** ☒

**OSPF-Enabled Interfaces**

fe-0/0/0.0  
lo0.0

**OSP**

fxp0.

OK Cancel Apply

To configure a single-area OSPF network with Quick Configuration:

1. In the J-Web user interface, select **Configuration > Routing > OSPF Routing**.
2. Enter information into the Quick Configuration Routing page for OSPF, as described in Table 74.
3. Click one of the following buttons:
  - To apply the configuration and stay on the Quick Configuration Routing page for OSPF, click **Apply**.
  - To apply the configuration and return to the Quick Configuration Routing page, click **OK**.
  - To cancel your entries and return to the Quick Configuration Routing page, click **Cancel**.
4. To check the configuration, see “Verifying an OSPF Configuration” on page 311.

**Table 74: OSPF Routing Quick Configuration Summary**

| Field                        | Function                                    | Your Action                                                                                                                                                                                                          |
|------------------------------|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Router Identification</b> |                                             |                                                                                                                                                                                                                      |
| Router Identifier (required) | Uniquely identifies the router.             | Type the Services Router’s 32-bit IP address, in dotted decimal notation.                                                                                                                                            |
| <b>OSPF</b>                  |                                             |                                                                                                                                                                                                                      |
| Enable OSPF                  | Enables or disables OSPF.                   | <ul style="list-style-type: none"> <li>■ To enable OSPF, select the check box.</li> <li>■ To disable OSPF, clear the check box.</li> </ul>                                                                           |
| OSPF Area ID                 | Uniquely identifies the area within its AS. | Type a 32-bit numeric identifier for the area, or an integer.<br><br>If you enter an integer, the value is converted to a 32-bit equivalent. For example, if you enter 3, the value assigned to the area is 0.0.0.3. |



**Table 74: OSPF Routing Quick Configuration Summary (continued)**

| Field                   | Function                                                                    | Your Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Area Type               | Designates the type of OSPF area.                                           | <p>From the list, select the type of OSPF area you are creating:</p> <ul style="list-style-type: none"> <li>■ <b>regular</b>—A regular OSPF area, including the backbone area</li> <li>■ <b>stub</b>—A stub area</li> <li>■ <b>nssa</b>—A not-so-stubby area (NSSA)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| OSPF-Enabled Interfaces | Designates one or more Services Router interfaces on which OSPF is enabled. | <p>The first time you configure OSPF, the Logical Interfaces box displays a list of all the logical interfaces configured on the Services Router. Do any of the following:</p> <ul style="list-style-type: none"> <li>■ To enable OSPF on an interface, click the interface name to highlight it, and click the left arrow to add the interface to the OSPF interfaces list.</li> <li>■ To enable OSPF on multiple interfaces at once, press Ctrl while you click multiple interface names to highlight them. Then click the left arrow to add the interfaces to the OSPF interfaces list.</li> <li>■ To enable OSPF on all logical interfaces except the special <b>fxp0</b> management interface, select <b>All Interfaces</b> in the Logical Interfaces list and click the left arrow.</li> <li>■ To enable OSPF on all the interfaces displayed in the Logical Interfaces list, click <b>All</b> to highlight every interface. Then click the left arrow to add the interfaces to the OSPF interfaces list.</li> <li>■ To disable OSPF on one or more interfaces, highlight the interface or interfaces in the OSPF interfaces box and click the right arrow to move them back to the Logical Interfaces list.</li> </ul> |

## Configuring an OSPF Network with a Configuration Editor

To configure the Services Router as a node in an OSPF network, you must perform the following tasks marked *(Required)*.

- Configuring the Router Identifier (Required) on page 300
- Configuring a Single-Area OSPF Network (Required) on page 300
- Configuring a Multiarea OSPF Network (Optional) on page 302
- Configuring Stub and Not-So-Stubby Areas (Optional) on page 305

To configure an OSPF demand circuit, see “Configuring Dial-on-Demand Routing Backup with OSPF Support (Optional)” on page 209. (You must have already configured an ISDN interface as described in “Configuring ISDN” on page 187.)

For information about using the J-Web and CLI configuration editors, see “Using J-Web Configuration Tools” on page 3.

## Configuring the Router Identifier (Required)

The router identifier is the IP address that uniquely identifies the J-series Services Router.

OSPF uses the router identifier to elect a designated router, unless you manually specify a priority value. When the OSPF network first becomes active, by default, the router with the highest router identifier is elected the designated router.

To configure the router identifier for the Services Router:

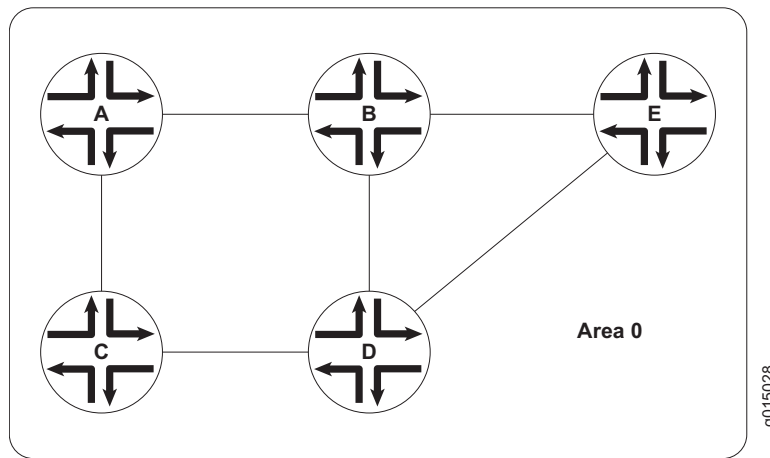
1. Navigate to the top of the configuration hierarchy in either the J-Web or the CLI configuration editor.
2. Perform the configuration tasks described in Table 75.
3. Go on to “Configuring a Single-Area OSPF Network (Required)” on page 300.

**Table 75: Configuring the Router Identifier**

| Task                                                                                        | J-Web Configuration Editor                                                                                                 | CLI Configuration Editor                                                   |
|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Navigate to the <b>Routing-options</b> level in the configuration hierarchy.                | In the configuration editor hierarchy, select <b>Routing-options</b> .                                                     | From the top of the configuration hierarchy, enter<br>edit routing-options |
| Set the router ID value to the IP address of the Services Router—for example, 177.162.4.24. | <ol style="list-style-type: none"> <li>1. In the Router Id box, type 177.162.4.24.</li> <li>2. Click <b>OK</b>.</li> </ol> | Enter<br>set router-id 177.162.4.24                                        |

## Configuring a Single-Area OSPF Network (Required)

To use OSPF on the Services Router, you must configure at least one OSPF area, like the one shown in Figure 65.

**Figure 65: Typical Single-Area OSPF Network Topology**

To configure a single-area OSPF network with a backbone area, like the one in Figure 65, perform these steps on each Services Router in the network:

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 76.
3. If you are finished configuring the router, commit the configuration.

After you create the backbone area and add the appropriate interfaces to the area, OSPF begins sending LSAs. No additional configuration is required to enable OSPF traffic on the network.

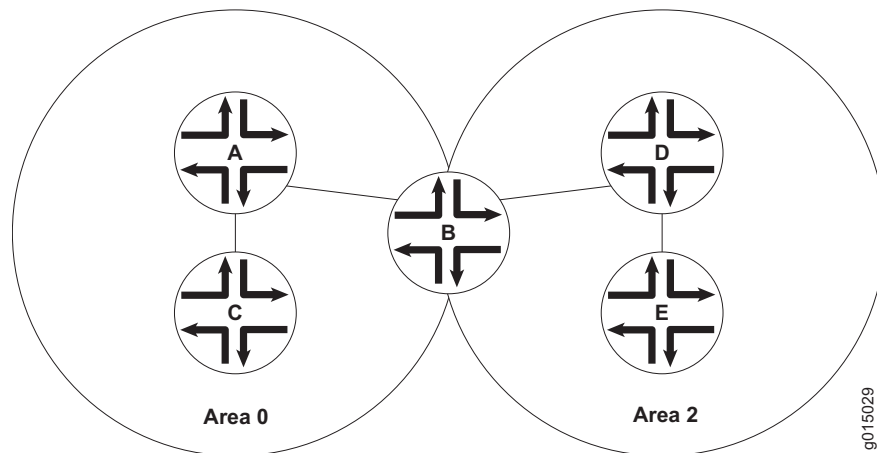
4. Go on to one of the following procedures:
  - To add more areas to the AS, see “Configuring a Multiarea OSPF Network (Optional)” on page 302.
  - To control external route advertisement in the AS, see “Configuring Stub and Not-So-Stubby Areas (Optional)” on page 305.
  - To configure an OSPF demand circuit, see “Configuring Dial-on-Demand Routing Backup with OSPF Support (Optional)” on page 209. (You must have already configured an ISDN interface as described in “Configuring ISDN” on page 187.)
  - To improve network operation, see “Tuning an OSPF Network for Efficient Operation” on page 307.
  - To check the configuration, see “Verifying an OSPF Configuration” on page 311.

**Table 76: Configuring a Single-Area OSPF Network**

| Task                                                              | J-Web Configuration Editor                                                                                                                                                                                                                                                                                                                              | CLI Configuration Editor                                                                                                                                                                |
|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Navigate to the <b>Ospf</b> level in the configuration hierarchy. | In the configuration editor hierarchy, select <b>Protocols &gt; Ospf</b> .                                                                                                                                                                                                                                                                              | From the top of the configuration hierarchy, enter<br><br>edit protocols ospf                                                                                                           |
| Create the backbone area with area ID 0.0.0.0.                    | <ol style="list-style-type: none"> <li>1. In the Area box, click <b>Add new entry</b>.</li> <li>2. In the Area ID box, type 0.0.0.0.</li> </ol>                                                                                                                                                                                                         | <ol style="list-style-type: none"> <li>1. Set the backbone area ID to 0.0.0.0 and add an interface:<br/><br/>set area 0.0.0.0 interface fe-0/0/0</li> </ol>                             |
| Add interfaces as needed to the OSPF area—for example, fe-0/0/0.  | <ol style="list-style-type: none"> <li>1. In the Interface box, click <b>Add new entry</b>.</li> <li>2. In the Interface name box, type fe-0/0/0.</li> <li>3. Click <b>OK</b>.</li> <li>4. Repeat Step 1 through Step 3 for each interface on this Services Router that you are adding to the backbone area. Only one interface is required.</li> </ol> | <ol style="list-style-type: none"> <li>2. Repeat Step 1 for each interface on this Services Router that you are adding to the backbone area. Only one interface is required.</li> </ol> |

### Configuring a Multiarea OSPF Network (Optional)

To reduce traffic and topology maintenance for the Services Routers in an OSPF autonomous system (AS), you can group them into multiple areas, as shown in Figure 66.

**Figure 66: Typical Multiarea OSPF Network Topology**

To configure a multiarea OSPF network shown in Figure 66, perform the following tasks on the appropriate Services Routers in the network. You must create a backbone area. To link each additional area to the backbone area, you must configure one of the Services Routers as an area border router (ABR).

- Creating the Backbone Area on page 303
- Creating Additional OSPF Areas on page 303
- Configuring Area Border Routers on page 304

## Creating the Backbone Area

On each Services Router 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 “Configuring a Single-Area OSPF Network (Required)” on page 300.

## Creating Additional OSPF Areas

To create additional OSPF areas:

1. Navigate to the top of the configuration hierarchy in either the J-Web or the CLI configuration editor.
2. Perform the configuration tasks described in Table 77.
3. If you are finished configuring the router, commit the configuration.
4. Go on to one of the following procedures:
  - To configure this Services Router as an area border router, see “Configuring Area Border Routers” on page 304.
  - To control external route advertisement in the AS, see “Configuring Stub and Not-So-Stubby Areas (Optional)” on page 305.
  - To configure an OSPF demand circuit, see “Configuring Dial-on-Demand Routing Backup with OSPF Support (Optional)” on page 209. (You must have already configured an ISDN interface as described in “Configuring ISDN” on page 187.)
  - To improve network operation, see “Tuning an OSPF Network for Efficient Operation” on page 307.
  - To check the configuration, see “Verifying an OSPF Configuration” on page 311.

**Table 77: Configuring a Multiarea OSPF Network**

| <b>Task</b>                                                                                        | <b>J-Web Configuration Editor</b>                                                                                                                                                                                                                                                                                                                       | <b>CLI Configuration Editor</b>                                                                                                                                                |
|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Navigate to the <b>Ospf</b> level in the configuration hierarchy.                                  | In the configuration editor hierarchy, select <b>Protocols &gt; Ospf</b> .                                                                                                                                                                                                                                                                              | From the top of the configuration hierarchy, enter<br><br>edit protocols ospf                                                                                                  |
| Create the additional area with a unique area ID, in dotted decimal notation—for example, 0.0.0.2. | <ol style="list-style-type: none"> <li>1. In the Area box, click <b>Add new entry</b>.</li> <li>2. In the Area ID box, type 0.0.0.2.</li> </ol>                                                                                                                                                                                                         | <ol style="list-style-type: none"> <li>1. Set the area ID to 0.0.0.2 and add an interface:<br/><br/>set area 0.0.0.2 interface fe-0/0/0</li> </ol>                             |
| Add interfaces as needed to the OSPF area—for example, fe-0/0/0.                                   | <ol style="list-style-type: none"> <li>1. In the Interface box, click <b>Add new entry</b>.</li> <li>2. In the Interface name box, type fe-0/0/0.</li> <li>3. Click <b>OK</b>.</li> <li>4. Repeat Step 1 through Step 3 for each interface on this Services Router that you are adding to the backbone area. Only one interface is required.</li> </ol> | <ol style="list-style-type: none"> <li>2. Repeat Step 1 for each interface on this Services Router that you are adding to the area. Only one interface is required.</li> </ol> |

## Configuring Area Border Routers

A Services Router operating as an area border router (ABR) has interfaces enabled for OSPF in the backbone area and in the area you are linking to the backbone. For example, Services Router B acts as the ABR in Figure 66 and has interfaces in both the backbone area and area 0.0.0.3.

1. Navigate to the top of the configuration hierarchy in either the J-Web or the CLI configuration editor.
2. Perform the configuration tasks described in Table 78.
3. If you are finished configuring the router, commit the configuration.

After you create the areas on the appropriate Services Routers and add and enable the appropriate interfaces to the areas, no additional configuration is required to enable OSPF traffic within or across the areas.

4. Go on to one of the following procedures:
  - To control external route advertisement in the AS, see “Configuring Stub and Not-So-Stubby Areas (Optional)” on page 305.
  - To configure an OSPF demand circuit, see “Configuring Dial-on-Demand Routing Backup with OSPF Support (Optional)” on page 209. (You must have already configured an ISDN interface as described in “Configuring ISDN” on page 187.)

- To improve network operation, see “Tuning an OSPF Network for Efficient Operation” on page 307.
- To check the configuration, see “Verifying an OSPF Configuration” on page 311.

**Table 78: Configuring Area Border Routers**

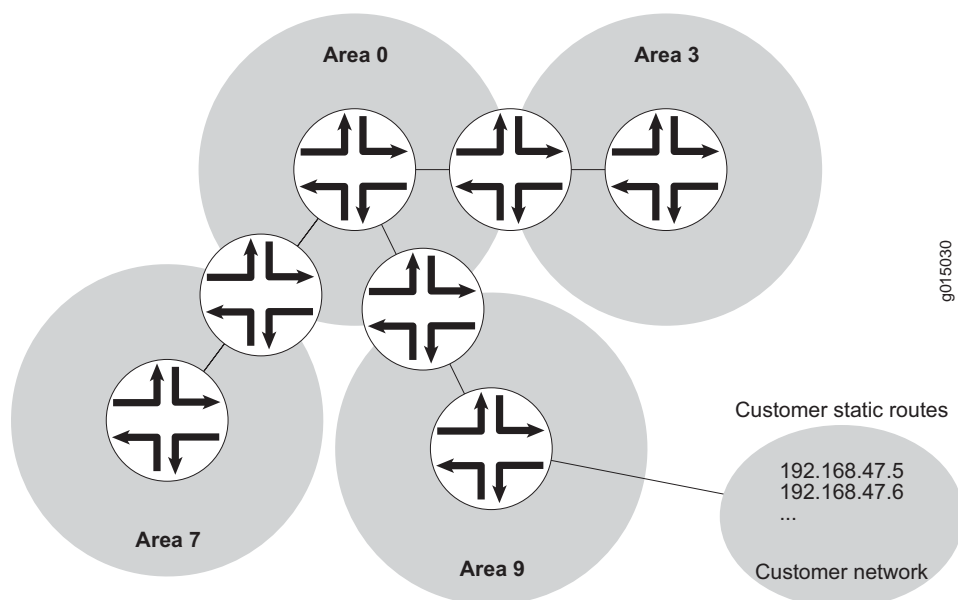
| Task                                                                       | J-Web Configuration Editor                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | CLI Configuration Editor                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Navigate to the <b>Ospf</b> level in the configuration hierarchy.          | In the configuration editor hierarchy, select <b>Protocols &gt; Ospf</b> .                                                                                                                                                                                                                                                                                                                                                                                                                        | From the top of the configuration hierarchy, enter<br><br>edit protocols ospf                                                                                                                                                                                                                                                                                                                       |
| Verify that the backbone area has at least one interface enabled for OSPF. | Click <b>0.0.0.0</b> to display the Area ID <b>0.0.0.0</b> page, and verify that the backbone area has at least one interface enabled for OSPF.<br><br>For example, Services Router B in Figure 66 has the following interfaces enabled for OSPF in the backbone area: <ul style="list-style-type: none"> <li>■ Interface fe-0/0/0.0</li> <li>■ Interface fe-0/0/1.0</li> </ul> To enable an interface on the backbone area, see “Configuring a Single-Area OSPF Network (Required)” on page 300. | View the configuration using the <b>show</b> command:<br><br><b>show</b><br><br>For example, Services Router B in Figure 66 has the following interfaces enabled for OSPF in the backbone area:<br><br><b>area 0.0.0.0 { interface fe-0/0/0.0; interface fe-0/0/1.0; }</b><br><br>To enable an interface on the backbone area, see “Configuring a Single-Area OSPF Network (Required)” on page 300. |
| Create the additional area with a unique area ID—for example, 0.0.0.2.     | 1. In the Area box, click <b>Add new entry</b> .<br><br>2. In the Area ID box, type 0.0.0.2.                                                                                                                                                                                                                                                                                                                                                                                                      | 1. Set the area ID to 0.0.0.2 and add an interface:<br><br><b>set area 0.0.0.2 interface fe-0/0/0</b>                                                                                                                                                                                                                                                                                               |
| Add interfaces as needed to the OSPF area—for example, fe-0/0/0.           | 1. In the Interface box, click <b>Add new entry</b> .<br><br>2. In the Interface name box, type fe-0/0/0.<br><br>3. Click <b>OK</b> .<br><br>4. Repeat Step 1 through Step 3 for each interface on this Services Router that you are adding to the backbone area. Only one interface is required.                                                                                                                                                                                                 | 2. Repeat Step 1 for each interface on this Services Router that you are adding to the area. Only one interface is required.                                                                                                                                                                                                                                                                        |

### Configuring Stub and Not-So-Stubby Areas (Optional)

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 67, 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 67: OSPF Network Topology with Stub Areas and NSSAs**



To configure stub areas and NSSAs in an OSPF network like the one shown in Figure 67:

1. Create the area and enable OSPF on the interfaces within that area.  
For instructions, see “Creating Additional OSPF Areas” on page 303.
2. Configure an area border router to bridge the areas.  
For instructions, see “Configuring Area Border Routers” on page 304.
3. Navigate to the top of the configuration hierarchy in either the J-Web or the CLI configuration editor.
4. To configure each Services Router in area 0.0.0.7 as a stub area router, perform the configuration tasks described in Table 79.
5. If you are finished configuring the router, commit the configuration.
6. Go on to one of the following procedures:
  - To configure an OSPF demand circuit, see “Configuring Dial-on-Demand Routing Backup with OSPF Support (Optional)” on page 209. (You must have already configured an ISDN interface as described in “Configuring ISDN” on page 187.)



- To improve network operation, see “Tuning an OSPF Network for Efficient Operation” on page 307.
- To check the configuration, see “Verifying an OSPF Configuration” on page 311.

**Table 79: Configuring Stub Area and Not-So-Stubby Area Routers**

| Task                                                                     | J-Web Configuration Editor                                                                                                                                                                                                                                | CLI Configuration Editor                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Navigate to the <b>0.0.0.7</b> level in the configuration hierarchy.     | In the configuration editor hierarchy, select <b>Protocols &gt; Ospf &gt; Area id 0.0.0.7</b> .                                                                                                                                                           | From the top of the configuration hierarchy, enter<br><br>edit protocols ospf area 0.0.0.7                                                                                                                                                |
| Configure each Services Router in area <b>0.0.0.7</b> as a stub router.  | <ol style="list-style-type: none"> <li>1. In the Stub option list, select <b>Stub</b> and click <b>OK</b>.</li> <li>2. Repeat Step 1 for every Services Router in the stub area to configure them with the <b>stub</b> parameter for the area.</li> </ol> | <ol style="list-style-type: none"> <li>1. Set the stub attribute:<br/><br/><b>set stub</b></li> <li>2. Repeat Step 1 for every Services Router in the stub area to configure them with the <b>stub</b> parameter for the area.</li> </ol> |
| Navigate to the <b>0.0.0.9</b> level in the configuration hierarchy.     | In the configuration editor hierarchy, select <b>Protocols &gt; Ospf &gt; Area &gt; 0.0.0.9</b> .                                                                                                                                                         | From the top of the configuration hierarchy, enter<br><br>edit protocols ospf area 0.0.0.9                                                                                                                                                |
| Configure each Services Router in area <b>0.0.0.9</b> as an NSSA router. | <ol style="list-style-type: none"> <li>1. In the Stub option list, select <b>Nssa</b> and click <b>OK</b>.</li> <li>2. Repeat Step 1 for every Services Router in the NSSA to configure them with the <b>nssa</b> parameter for the area.</li> </ol>      | <ol style="list-style-type: none"> <li>1. Set the nssa attribute:<br/><br/><b>set nssa</b></li> <li>2. Repeat Step 1 for every Services Router in the NSSA to configure them with the <b>nssa</b> parameter for the area.</li> </ol>      |

## Tuning an OSPF Network for Efficient Operation

To make your OSPF network operate more efficiently, you can change some default settings on the Services Router by performing the following tasks:

- Controlling Route Selection in the Forwarding Table on page 308
- Controlling the Cost of Individual Network Segments on page 308
- Enabling Authentication for OSPF Exchanges on page 309
- Controlling Designated Router Election on page 310

## Controlling Route Selection in the Forwarding Table

OSPF uses route preferences to select the route that is installed in the forwarding table when several routes have the same shortest path first (SPF) calculation. 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 Services Router is selected for the forwarding table any time multiple equal-cost paths to a destination exist.

To modify the default preferences on a Services Router:

1. Navigate to the top of the configuration hierarchy in either the J-Web or the CLI configuration editor.
2. Perform the configuration tasks described in Table 80.

**Table 80: Controlling Route Selection in the Forwarding Table by Setting Preferences**

| Task                                                              | J-Web Configuration Editor                                                                                                                                                                                            | CLI Configuration Editor                                                                                                                                                                  |
|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Navigate to the <b>Ospf</b> level in the configuration hierarchy. | In the configuration editor hierarchy, select <b>Protocols &gt; Ospf</b> .                                                                                                                                            | From the top of the configuration hierarchy, enter<br><br>edit protocols ospf                                                                                                             |
| Set the external and internal route preferences.                  | <ol style="list-style-type: none"> <li>1. In the External preference box, type <b>130</b>.</li> <li>2. In the Preference box, type the internal preference value of <b>7</b>.</li> <li>3. Click <b>OK</b>.</li> </ol> | <ol style="list-style-type: none"> <li>1. Set the external preference:<br/><br/>set external-preference 130</li> <li>2. Set the internal preference:<br/><br/>set preference 7</li> </ol> |

## Controlling the Cost of Individual Network Segments

When evaluating the cost of individual network segments, OSPF evaluates the reference bandwidth. For any link faster than 100 Mbps, the default cost metric is 1. When OSPF calculates the SPF algorithm, it sums the metrics of all interfaces along a path to determine the overall cost of the path. The path with the lowest metric is selected for the forwarding table.

To control the cost of the network segment, you can modify the metric value on an individual interface. Suppose all routers in the OSPF network use default metric values. If you increase the metric on an interface to 5, all paths through this interface have a calculated metric higher than the default and are *not* preferred.

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 in either the J-Web or the CLI configuration editor.
2. Perform the configuration tasks described in Table 81.

**Table 81: Controlling the Cost of Individual Network Segments by Modifying the Metric**

| Task                                                                    | J-Web Configuration Editor                                                                                                           | CLI Configuration Editor                                                                                           |
|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Navigate to the <b>fe-0/0/0.0</b> level in the configuration hierarchy. | In the configuration editor hierarchy, select <b>Protocols &gt; Ospf &gt; Area id 0.0.0.0 &gt; Interface name fe-0/0/0.0</b> .       | From the top of the configuration hierarchy, enter<br><br>edit protocols ospf area 0.0.0.0<br>interface fe-0/0/0.0 |
| Set the interface metric.                                               | <ol style="list-style-type: none"><li>1. In the Metric box, type the interface metric value 5.</li><li>2. Click <b>OK</b>.</li></ol> | Set the interface metric:<br><br>set metric 5                                                                      |

**Enabling Authentication for OSPF Exchanges**

All OSPFv2 protocol exchanges can be authenticated to guarantee that only trusted routers participate in the 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.

To enable OSPF authentication on the stub area:

1. Navigate to the top of the configuration hierarchy in either the J-Web or the CLI configuration editor.
2. Perform the configuration tasks described in Table 82.

**Table 82: Enabling OSPF Authentication**

| <b>Task</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <b>J-Web Configuration Editor</b>                                                                                                                                                                                                                                                                                   | <b>CLI Configuration Editor</b>                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Navigate to the <b>0.0.0.0</b> level in the configuration hierarchy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | In the configuration editor hierarchy, select <b>Protocols &gt; Ospf &gt; Area id 0.0.0.0</b> .                                                                                                                                                                                                                     | From the top of the configuration hierarchy, enter<br><br><code>edit protocols ospf area 0.0.0.0</code>                                                                                                                                                                                                          |
| Set the authentication type for the stub area to either simple or MD5—for example, MD5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <ol style="list-style-type: none"> <li>From the Authentication type list, select <b>md5</b>.</li> <li>Click <b>OK</b>.</li> </ol>                                                                                                                                                                                   | Set the authentication type:<br><br><code>set authentication-type md5</code>                                                                                                                                                                                                                                     |
| Navigate to the <i>interface-name</i> level in the configuration hierarchy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | In the configuration editor hierarchy under <b>Protocols &gt; Ospf &gt; Area &gt; 0.0.0.0 &gt; interface</b> , click an interface name.                                                                                                                                                                             | From the top of the configuration hierarchy, enter<br><br><code>edit protocols ospf area 0.0.0.0 interface interface-name</code>                                                                                                                                                                                 |
| Set the authentication password (key) and, for MD5 authentication only, the key identifier to associate with the MD5 password: <ul style="list-style-type: none"> <li>■ For simple authentication, set a password of from 1 through 8 ASCII characters—for example, <b>Chey3nne</b>.</li> <li>■ For MD5 authentication:               <ul style="list-style-type: none"> <li>■ Set a password of from 1 through 16 ASCII characters—for example, <b>Chey3nne</b>.</li> <li>■ Set a key identifier between 0 (the default) and 255—for example, 2.</li> </ul> </li> </ul> | <ol style="list-style-type: none"> <li>In the Key name box, type <b>Chey3nne</b>.</li> <li>For MD5 authentication only, in the Key ID box, type <b>2</b>.</li> <li>Click <b>OK</b>.</li> <li>Repeat Step 1 through Step 3 for each interface in the stub area for which you are enabling authentication.</li> </ol> | <ol style="list-style-type: none"> <li>Set the authentication password and, for MD5 authentication only, set the key identifier:<br/><br/><code>set authentication-key Chey3nne key-id 2</code></li> <li>Repeat Step 1 for each interface in the stub area for which you are enabling authentication.</li> </ol> |

## Controlling Designated Router Election

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**.

To change the priority of a Services Router to control designated router election:

- Navigate to the top of the configuration hierarchy in either the J-Web or the CLI configuration editor.
- Perform the configuration tasks described in Table 83.

**Table 83: Controlling Designated Router Election**

| Task                                                                                                                                                     | J-Web Configuration Editor                                                                                                   | CLI Configuration Editor                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Navigate to the OSPF interface address for the Services Router. For example, navigate to the <code>fe-0/0/1</code> level in the configuration hierarchy. | In the configuration editor hierarchy, select <b>Protocols &gt; Ospf &gt; area id 0.0.0.3 &gt; Interface name fe-0/0/1</b> . | From the top of the configuration hierarchy, enter<br><br><code>edit protocols ospf area 0.0.0.3 interface fe-0/0/1</code> |
| Set the Services Router priority to a value between 0 and 255—for example, 200. The default value is 128.                                                | 1. In the Priority box, type 200.<br>2. Click <b>OK</b> .                                                                    | Set the priority value:<br><br><code>set priority 200</code>                                                               |

## Verifying an OSPF Configuration

To verify an OSPF configuration, perform these tasks:

- Verifying OSPF-Enabled Interfaces on page 311
- Verifying OSPF Neighbors on page 312
- Verifying the Number of OSPF Routes on page 313
- Verifying Reachability of All Hosts in an OSPF Network on page 314

### Verifying OSPF-Enabled Interfaces

| <b>Purpose</b>       | Verify that OSPF is running on a particular interface and that the interface is in the desired area.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |         |              |              |       |        |      |            |        |         |         |         |   |            |    |         |              |              |   |       |    |         |              |         |   |            |      |         |         |         |   |            |        |         |         |         |   |            |      |         |         |         |   |            |        |         |         |         |   |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|--------------|--------------|-------|--------|------|------------|--------|---------|---------|---------|---|------------|----|---------|--------------|--------------|---|-------|----|---------|--------------|---------|---|------------|------|---------|---------|---------|---|------------|--------|---------|---------|---------|---|------------|------|---------|---------|---------|---|------------|--------|---------|---------|---------|---|
| <b>Action</b>        | From the CLI, enter the <code>show ospf interface</code> command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |         |              |              |       |        |      |            |        |         |         |         |   |            |    |         |              |              |   |       |    |         |              |         |   |            |      |         |         |         |   |            |        |         |         |         |   |            |      |         |         |         |   |            |        |         |         |         |   |
| <b>Sample Output</b> | <pre>user@host&gt; show ospf interface</pre> <table><tr><th>Intf</th><th>State</th><th>Area</th><th>DR ID</th><th>BDR ID</th><th>Nbrs</th></tr><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></table> | Intf    | State        | Area         | DR ID | BDR ID | Nbrs | at-5/1/0.0 | PtToPt | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 1 | ge-2/3/0.0 | DR | 0.0.0.0 | 192.168.4.16 | 192.168.4.15 | 1 | lo0.0 | DR | 0.0.0.0 | 192.168.4.16 | 0.0.0.0 | 0 | so-0/0/0.0 | Down | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 0 | so-6/0/1.0 | PtToPt | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 1 | so-6/0/2.0 | Down | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 0 | so-6/0/3.0 | PtToPt | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 1 |
| Intf                 | State                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Area    | DR ID        | BDR ID       | Nbrs  |        |      |            |        |         |         |         |   |            |    |         |              |              |   |       |    |         |              |         |   |            |      |         |         |         |   |            |        |         |         |         |   |            |      |         |         |         |   |            |        |         |         |         |   |
| at-5/1/0.0           | PtToPt                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 0.0.0.0 | 0.0.0.0      | 0.0.0.0      | 1     |        |      |            |        |         |         |         |   |            |    |         |              |              |   |       |    |         |              |         |   |            |      |         |         |         |   |            |        |         |         |         |   |            |      |         |         |         |   |            |        |         |         |         |   |
| ge-2/3/0.0           | DR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 0.0.0.0 | 192.168.4.16 | 192.168.4.15 | 1     |        |      |            |        |         |         |         |   |            |    |         |              |              |   |       |    |         |              |         |   |            |      |         |         |         |   |            |        |         |         |         |   |            |      |         |         |         |   |            |        |         |         |         |   |
| lo0.0                | DR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 0.0.0.0 | 192.168.4.16 | 0.0.0.0      | 0     |        |      |            |        |         |         |         |   |            |    |         |              |              |   |       |    |         |              |         |   |            |      |         |         |         |   |            |        |         |         |         |   |            |      |         |         |         |   |            |        |         |         |         |   |
| so-0/0/0.0           | Down                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 0.0.0.0 | 0.0.0.0      | 0.0.0.0      | 0     |        |      |            |        |         |         |         |   |            |    |         |              |              |   |       |    |         |              |         |   |            |      |         |         |         |   |            |        |         |         |         |   |            |      |         |         |         |   |            |        |         |         |         |   |
| so-6/0/1.0           | PtToPt                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 0.0.0.0 | 0.0.0.0      | 0.0.0.0      | 1     |        |      |            |        |         |         |         |   |            |    |         |              |              |   |       |    |         |              |         |   |            |      |         |         |         |   |            |        |         |         |         |   |            |      |         |         |         |   |            |        |         |         |         |   |
| so-6/0/2.0           | Down                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 0.0.0.0 | 0.0.0.0      | 0.0.0.0      | 0     |        |      |            |        |         |         |         |   |            |    |         |              |              |   |       |    |         |              |         |   |            |      |         |         |         |   |            |        |         |         |         |   |            |      |         |         |         |   |            |        |         |         |         |   |
| so-6/0/3.0           | PtToPt                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 0.0.0.0 | 0.0.0.0      | 0.0.0.0      | 1     |        |      |            |        |         |         |         |   |            |    |         |              |              |   |       |    |         |              |         |   |            |      |         |         |         |   |            |        |         |         |         |   |            |      |         |         |         |   |            |        |         |         |         |   |
| <b>What It Means</b> | <p>The output shows a list of the Services Router interfaces that are configured for OSPF. Verify the following information:</p> <ul style="list-style-type: none"><li>■ Each interface on which OSPF is enabled is listed.</li><li>■ Under Area, each interface shows the area for which it was configured.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |         |              |              |       |        |      |            |        |         |         |         |   |            |    |         |              |              |   |       |    |         |              |         |   |            |      |         |         |         |   |            |        |         |         |         |   |            |      |         |         |         |   |            |        |         |         |         |   |

- Under **Intf** and **State**, the Services Router 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**.

For more information about `show ospf interface`, see the *JUNOS Routing Protocols and Policies Command Reference*.

## Verifying OSPF Neighbors

**Purpose** OSPF neighbors are interfaces that have an immediate adjacency. On a point-to-point connection between the Services Router 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** `user@host> show ospf neighbor`

| Address         | Intf   | State | ID            | Pri | Dead |
|-----------------|--------|-------|---------------|-----|------|
| 192.168.254.225 | fxp3.0 | 2Way  | 10.250.240.32 | 128 | 36   |
| 192.168.254.230 | fxp3.0 | Full  | 10.250.240.8  | 128 | 38   |
| 192.168.254.229 | fxp3.0 | Full  | 10.250.240.35 | 128 | 33   |
| 10.1.1.129      | fxp2.0 | Full  | 10.250.240.12 | 128 | 37   |
| 10.1.1.131      | fxp2.0 | Full  | 10.250.240.11 | 128 | 38   |
| 10.1.2.1        | fxp1.0 | Full  | 10.250.240.9  | 128 | 32   |
| 10.1.2.81       | fxp0.0 | Full  | 10.250.240.10 | 128 | 33   |

**What It Means** The output shows a list of the Services Router'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 Services Router is listed.
- The Services Router's own loopback address and the loopback addresses of any routers with which the Services Router 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.

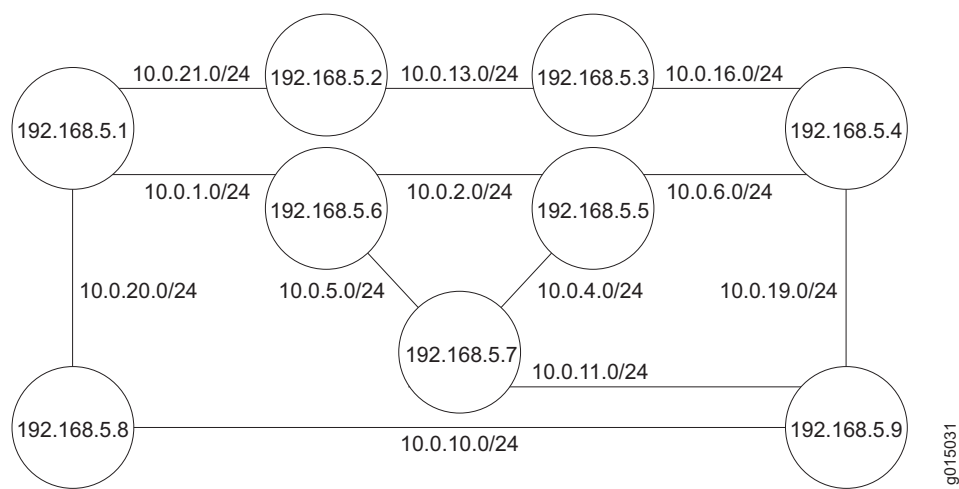
For more information about `show ospf neighbor`, see the *JUNOS Routing Protocols and Policies Command Reference*.

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 68 shows a sample network with an OSPF topology.

Figure 68: 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.

|                      |                                            |       |         |      |        |            |            |
|----------------------|--------------------------------------------|-------|---------|------|--------|------------|------------|
| <b>Sample Output</b> | <code>user@host&gt; show ospf route</code> |       |         |      |        |            |            |
|                      | Prefix                                     | Path  | Route   | NH   | Metric | NextHop    | Nexthop    |
|                      |                                            | Type  | Type    | Type |        | Interface  | addr/label |
|                      | 10.10.10.1/24                              | Intra | Network | IP   | 1      | fe-0/0/2.0 | 10.0.21.1  |
|                      | 10.10.10.2/24                              | Intra | Network | IP   | 1      | fe-0/0/2.0 | 10.0.21.1  |
|                      | 10.10.10.4/24                              | Intra | Network | IP   | 1      | fe-0/0/1.0 | 10.0.13.1  |
|                      | 10.10.10.5/24                              | Intra | Network | IP   | 1      | fe-0/0/2.0 | 10.0.21.1  |
|                      | 10.10.10.6/24                              | Intra | Network | IP   | 1      | fe-0/0/1.0 | 10.0.13.1  |
|                      | 10.10.10.10/24                             | Intra | Network | IP   | 1      | fe-0/0/2.0 | 10.0.21.1  |
|                      | 10.10.10.11/24                             | Intra | Network | IP   | 1      | fe-0/0/1.0 | 10.0.13.1  |
|                      | 10.10.10.13/24                             | Intra | Network | IP   | 1      | fe-0/0/1.0 | 10.0.13.1  |
|                      | 10.10.10.16/24                             | Intra | Network | IP   | 1      | fe-0/0/1.0 | 10.0.13.1  |
|                      | 10.10.10.19/24                             | Intra | Network | IP   | 1      | fe-0/0/1.0 | 10.0.13.1  |
|                      | 10.10.10.20/24                             | Intra | Network | IP   | 1      | fe-0/0/2.0 | 10.0.21.1  |
|                      | 10.10.10.21/24                             | Intra | Network | IP   | 1      | fe-0/0/2.0 | 10.0.21.1  |
|                      | 192.168.5.1                                | Intra | Router  | IP   | 1      | fe-0/0/2.0 | 10.0.21.1  |

|             |       |        |    |   |            |           |
|-------------|-------|--------|----|---|------------|-----------|
| 192.168.5.2 | Intra | Router | IP | 1 | lo0        |           |
| 192.168.5.3 | Intra | Router | IP | 1 | fe-0/0/1.0 | 10.0.13.1 |
| 192.168.5.4 | Intra | Router | IP | 1 | fe-0/0/1.0 | 10.0.13.1 |
| 192.168.5.5 | Intra | Router | IP | 1 | fe-0/0/1.0 | 10.0.13.1 |
| 192.168.5.6 | Intra | Router | IP | 1 | fe-0/0/2.0 | 10.0.21.1 |
| 192.168.5.7 | Intra | Router | IP | 1 | fe-0/0/2.0 | 10.0.21.1 |
| 192.168.5.8 | Intra | Router | IP | 1 | fe-0/0/2.0 | 10.0.21.1 |
| 192.168.5.9 | Intra | Router | IP | 1 | fe-0/0/1.0 | 10.0.13.1 |

**What It Means** 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 68, verify that the OSPF routing table has 21 entries, one for each network segment and one for each router's loopback address.

For more information about `show ospf route`, see the *JUNOS Routing Protocols and Policies Command Reference*.

## 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 Services Router.

**Action** For each Services Router in the OSPF network:

1. In the J-Web interface, select **Diagnose > Traceroute**.
2. In the Host Name box, type the name of a host for which you want to verify reachability from the Services Router.
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
```

**What It Means** Each numbered row in the output indicates a router (“hop”) in the path to the host. The three time increments indicate the round-trip time (RTT) between the Services Router 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 `ospf routeshow`, see “Verifying the Number of OSPF Routes” on page 313.

For information about the `traceroute` command and its output, see the *JUNOS System Basics and Services Command Reference*.



## Chapter 11

# Configuring the IS-IS Protocol

The Services Router supports the Intermediate System-to-Intermediate System (IS-IS) protocol.

You use either the J-Web configuration editor or CLI configuration editor to configure IS-IS.

This chapter contains the following topics. For more information about IS-IS, see the *JUNOS Routing Protocols Configuration Guide*.

- IS-IS Overview on page 315
- Before You Begin on page 316
- Configuring IS-IS with a Configuration Editor on page 317
- Verifying IS-IS on a Services Router on page 318

## IS-IS Overview

---

On the Services Router, Intermediate System-to-Intermediate System (IS-IS) protocol is an interior gateway routing protocol (IGP) that uses link-state information for routing network traffic. 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. The protocol was originally developed for routing International Organization for Standards (ISO) connectionless network protocol (CLNP) packets.

This overview contains the following topics:

- ISO Network Addresses on page 315
- System Identifier Mapping on page 316

## ISO Network Addresses

IS-IS uses ISO network address. Each address identifies a point of connection to the network, such as a router interface, which is called a 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
```

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.

---

## System Identifier Mapping

To provide assistance with debugging IS-IS, the Services Router 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.

## Before You Begin

---

Before you begin configuring IS-IS, complete the following tasks:

- Establish basic connectivity. See the *J-series Services Router Getting Started Guide*.

- If you do not already have an understanding of IS-IS, read “IS-IS Overview” on page 252 or the *JUNOS Routing Protocols Configuration Guide*.
- Obtain ISO addresses for participating routers in the AS.

## Configuring IS-IS with a Configuration Editor

To configure IS-IS with a configuration editor, you do the following:

- Enable IS-IS on the router.
- Configure a network entity title (NET) on one of the router interfaces, preferably the loopback interface, `lo0`.
- Configure the ISO family on all interfaces that are supporting the IS-IS protocol.

To configure IS-IS:

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 84.
3. Commit the configuration on the Services Router.
4. Repeat the configuration tasks on each Services Router in the IS-IS autonomous system (AS).

**Table 84: Configuring the IS-IS Protocol**

| Task                                                                    | J-Web Configuration Editor                                                                                                                                                                     | CLI Configuration Editor                                                   |
|-------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Navigate to the <b>Interfaces</b> level in the configuration hierarchy. | In the configuration editor hierarchy, select <b>Interfaces</b> .                                                                                                                              | From the top of the configuration hierarchy, enter<br><br>edit interfaces. |
| Configure the loopback interface <code>lo0</code> .                     | <ol style="list-style-type: none"> <li>1. Next to Interface, click <b>Add new entry</b>.</li> <li>2. In the Interface name box, type <code>lo0</code>.</li> <li>3. Click <b>OK</b>.</li> </ol> | Enter<br><br>edit interfaces lo0                                           |

**Table 84: Configuring the IS-IS Protocol (continued)**

| <b>Task</b>                                                                                             | <b>J-Web Configuration Editor</b>                                                                                                                                                                                                                                                                                                                                                                                                    | <b>CLI Configuration Editor</b>                                                                                          |
|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Configure the logical unit on the loopback interface—for example 0.                                     | 1. Next to lo0, click <b>Edit</b> under Encapsulation.                                                                                                                                                                                                                                                                                                                                                                               | 1. Enter<br>edit unit 0                                                                                                  |
| Add the NET address to the loopback interface—for example, 49.0001.00a0.c96b.c490.00.                   | 2. Next to Unit, click <b>Add new entry</b> .<br>3. In the Interface unit number box, type 0.<br>4. Under Family, select <b>Iso</b> .<br>5. Next to Address, click <b>Add new entry</b> .<br>6. In the Source box, type 49.0001.00a0.c96b.c490.00.<br>7. Click <b>OK</b> until you return to the Interfaces page.                                                                                                                    | 2. Enter<br>set family iso address<br>49.0001.00a0.c96b.c490.00                                                          |
| Configure a physical interface—for example, fe-0/0/1—with the NET address, and add the Family type iso. | 1. Next to fe-0/0/1, click <b>Edit</b> under Encapsulation.<br>2. Next to Unit, click <b>Add new entry</b> .<br>3. In the Interface unit number box, type 0.<br>4. Under Family, select <b>Iso</b> .<br>5. Next to Iso, click <b>Configure</b> .<br>6. Next to Address, click <b>Add new entry</b> .<br>7. In the Source box, type 49.0001.00a0.c96b.c490.00.<br>8. Click <b>OK</b> until you return to the Edit Configuration page. | Enter<br>edit interfaces fe-0/0/1<br>Enter<br>set unit 0<br>Enter<br>set family iso address<br>49.0001.00a0.c96b.c490.00 |
| Navigate to the <b>Protocols</b> level in the configuration hierarchy.                                  | In the configuration editor hierarchy, select <b>Protocols</b> .                                                                                                                                                                                                                                                                                                                                                                     | From the top of the configuration hierarchy, enter<br>edit protocols                                                     |
| Add the IS-IS protocol to all interfaces on the Services Router.                                        | 1. Next to Protocols, click <b>Edit</b> .<br>2. Next to Isis, click <b>Edit</b> .<br>3. In the Interface name box, type all.<br>4. Click <b>OK</b> .                                                                                                                                                                                                                                                                                 | Enter<br>set isis interface all                                                                                          |

## Verifying IS-IS on a Services Router

To verify IS-IS, perform these tasks:

- Displaying IS-IS Interface Configuration on page 319
- Displaying IS-IS Interface Configuration Detail on page 319
- Displaying IS-IS Adjacencies on page 320
- Displaying IS-IS Adjacencies in Detail on page 321

## Displaying IS-IS Interface Configuration

|                      |                                                                                                                                                                                                                                                                          |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>       | Verify the status of IS-IS-enabled interfaces.                                                                                                                                                                                                                           |
| <b>Action</b>        | From the CLI, enter the <code>show isis interface brief</code> command.                                                                                                                                                                                                  |
| <b>Sample Output</b> | <pre>user@host&gt; show isis interface brief  IS-IS interface database: Interface  L CirID Level 1 DR Level 2 DR lo0.0      3  0x1  router1 router.01 fe-0/0/1.0 2  0x9  Disabled router.03 fe-1/0/0.0 2  0x7  Disabled router.05</pre>                                  |
| <b>What It Means</b> | <p>Verify that the output shows the intended configuration of the interfaces on which IS-IS is enabled.</p> <p>For more information about the <code>show isis interface brief</code> command, see the <i>JUNOS Routing Protocols and Policies Command Reference</i>.</p> |

## Displaying IS-IS Interface Configuration Detail

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>       | Verify the details of IS-IS-enabled interfaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Action</b>        | From the CLI, enter the <code>show isis interface detail</code> command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Sample Output</b> | <pre>user@host&gt; 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 fe-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</pre> |
| <b>What It Means</b> | <p>Check the following output fields and verify that the output shows the intended configuration of IS-IS-enabled interfaces:</p> <ul style="list-style-type: none"> <li>■ <b>Interface</b>—Interface configured for IS-IS</li> <li>■ <b>State</b>—Internal implementation information</li> </ul>                                                                                                                                                                                                                                                                           |

- 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

For more information about the `show isis interface detail` command, see the *JUNOS Routing Protocols and Policies Command Reference*.

## Displaying 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
fe-0/0/0.0 1921.6800.5067 2 Up 13
fe-0/0/1.0 1921.6800.5067 2 Up 25
fe-0/0/2.0 1921.6800.5067 2 Up 19
```

**What It Means** Verify adjacent routers in the IS-IS database.

For more information about the `show isis adjacency brief` command, see the *JUNOS Routing Protocols and Policies Command Reference*.

## Displaying 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**

```

user@host> show isis adjacency extensive

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
  IP addresses: 10.1.26.2
  Transition log:
  When                State      Reason
  Tue Jul  5 18:03:45  Up        Seenself

```

**What It Means** Check the following fields and verify adjacency information about IS-IS neighbors:

- **Interface**—Interface through which the neighbor is reachable
- **L or Level**—Configured level of IS-IS:
  - 1—Level 1 only
  - 2—Level 2 only
  - 3—Level 1 and Level 2

An exclamation point before the level number indicates that the adjacency is missing an IP address.

- **State**—Status of the adjacency: Up, Down, New, One-way, Initializing, or Rejected

- Event—Message that identifies the cause of a state
- Down reason—Reason the adjacency is down
- Restart capable—Denotes a neighbor configured for graceful restart
- Transition log—List of transitions including When, State, and Reason

For more information about the `show isis adjacency extensive` command, see the *JUNOS Routing Protocols and Policies Command Reference*.



## Chapter 12

# Configuring BGP Sessions

Connections between peering networks are typically made through an exterior gateway protocol, most commonly the Border Gateway Protocol (BGP).

You can use either J-Web Quick Configuration or a configuration editor to configure BGP sessions.

This chapter contains the following topics. For more information about BGP, see the *JUNOS Routing Protocols Configuration Guide*.

- BGP Overview on page 323
- Before You Begin on page 325
- Configuring BGP Sessions with Quick Configuration on page 325
- Configuring BGP Sessions with a Configuration Editor on page 327
- Verifying a BGP Configuration on page 336

### BGP Overview

---

BGP is a heavy-duty, secure protocol that must be configured on a per-peer basis. Once a peering session has been configured, BGP uses a TCP connection to establish a session. After a BGP session is established, traffic is passed along the BGP-enabled link.

Although BGP requires a full-mesh topology to share route information, you can use route reflectors and confederations in a large autonomous system (AS) to reduce scaling problems.

### BGP Peering Sessions

Unlike RIP and OSPF links, BGP peering sessions must be explicitly configured at both ends. To establish a session between BGP peers, you must manually specify the interface address to which you are establishing a connection. Once this configuration is complete on both ends of a link, a TCP negotiation takes place and a BGP session is established.

The type of the BGP peering session depends on whether the peer is outside or inside the host's autonomous system (AS):

- Peering sessions established with hosts outside the local AS are external sessions. Traffic that passes along such links uses external BGP (EBGP) as its protocol.
- Peering sessions established with hosts within the local AS are internal sessions. Traffic that passes along such links uses internal BGP (IBGP) as its protocol.

### **IBGP Full Mesh Requirement**

By default, BGP does not readvertise routes that are learned from BGP. To share route information throughout the network, BGP requires a full mesh of internal peering sessions within an AS. 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`.

### **Route Reflectors and Clusters**

In larger networks, the overhead needed to implement the IBGP full-mesh requirement is prohibitive. Many networks use route reflectors to avoid having to configure an internal connection to each node for every new router.



**NOTE:** You must have an Advanced BGP Feature license installed on each Services Router that uses a route reflector. For license details, see the *J-series Services Router Administration Guide*.

---

A route reflector can readvertise routes learned through BGP to its BGP neighbors. If you define clusters of routers and configure a single router as a route reflector within each cluster, a full mesh is required only between the route reflectors and all their internal peers within the network. The route reflector is responsible for propagating BGP routes throughout the cluster.

For more information about route reflectors, see “Route Reflectors—for Added Hierarchy” on page 261

### **BGP Confederations**

Large ASs can be divided into smaller sub-ASs, which are groups of routers known as confederations. You configure EBGP peering sessions between confederations, and IBGP peering sessions within confederations. Within a confederation, the IBGP full mesh is required. For more information about confederations, see “Confederations—for Subdivision” on page 264

## Before You Begin

Before you begin configuring a BGP network, complete the following tasks:

- Establish basic connectivity. See the *J-series Services Router Getting Started Guide*.
- Configure network interfaces. See “Configuring Network Interfaces” on page 99.

## Configuring BGP Sessions with Quick Configuration

J-Web Quick Configuration allows you to create BGP peering sessions. Figure 69 shows the Quick Configuration Routing page for BGP.

**Figure 69: Quick Configuration Routing Page for BGP**

Juniper NETWORKS **ROUTER - J4300** Logged in as: **regress**  
[Help](#) [About](#) [Logout](#)

**Monitor Configuration Diagnose Manage**

**Quick Configuration**

Set Up  
SSL  
Interfaces  
Users  
SNMP

**Routing**

Firewall/NAT  
IPSec Tunnels  
Realtime Performance Monitoring

► **View and Edit**  
 ► **History**  
 ► **Rescue**

**Configuration > Quick Configuration > Routing**

**Quick Configuration**

**Routing**

**Router Identification**

\* **Router Identifier**  ?

**BGP**

**Enable BGP** ☐

**Autonomous System Number**  ?

**Peer Autonomous System Number**  ?

**Peer Address**

**Local Address**  ?

Copyright © 2004-2005, Juniper Networks, Inc. All Rights Reserved. [Trademark Notice](#).

To configure a BGP peering session with Quick Configuration:

1. In the J-Web user interface, select **Configuration > Routing > BGP Routing**.
2. Enter information into the Quick Configuration page for BGP, as described in Table 85.
3. From the main BGP routing Quick Configuration page, click one of the following buttons:
  - To apply the configuration and stay on the Quick Configuration Routing page for BGP, click **Apply**.
  - To apply the configuration and return to the Quick Configuration Routing page, click **OK**.
  - To cancel your entries and return to the Quick Configuration Routing page, click **Cancel**.
4. To check the configuration, see “Verifying a BGP Configuration” on page 336.

**Table 85: BGP Routing Quick Configuration Summary**

| Field                         | Function                                                                                                | Your Action                                                                                                                                                                                                                                        |
|-------------------------------|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Router Identification</b>  |                                                                                                         |                                                                                                                                                                                                                                                    |
| Router Identifier (required)  | Uniquely identifies the router                                                                          | Type the Services Router's 32-bit IP address, in dotted decimal notation.                                                                                                                                                                          |
| <b>BGP</b>                    |                                                                                                         |                                                                                                                                                                                                                                                    |
| Enable BGP                    | Enables or disables BGP.                                                                                | <ul style="list-style-type: none"> <li>■ To enable BGP, select the check box.</li> <li>■ To disable BGP, clear the check box.</li> </ul>                                                                                                           |
| Autonomous System Number      | Sets the unique numeric identifier of the AS in which the Services Router is configured.                | <p>Type the Services Router's 32-bit AS number, in dotted decimal notation.</p> <p>If you enter an integer, the value is converted to a 32-bit equivalent. For example, if you enter <b>3</b>, the value assigned to the AS is <b>0.0.0.3</b>.</p> |
| Peer Autonomous System Number | Sets the unique numeric identifier of the AS in which the peer host resides.                            | <p>Type the peer host's 32-bit AS number, in dotted decimal notation.</p> <p>If you enter an integer, the value is converted to a 32-bit equivalent. For example, if you enter <b>3</b>, the value assigned to the AS is <b>0.0.0.3</b>.</p>       |
| Peer Address                  | Specifies the IP address of the peer host's interface to which the BGP session is being established.    | Type the IP address of the peer host's adjacent interface, in dotted decimal notation.                                                                                                                                                             |
| Local Address                 | Specifies the IP address of the local host's interface from which the BGP session is being established. | Type the IP address of the local host's adjacent interface, in dotted decimal notation.                                                                                                                                                            |

## Configuring BGP Sessions with a Configuration Editor

---

To configure the Services Router as a node in a BGP network, you must perform the following tasks marked *(Required)*.

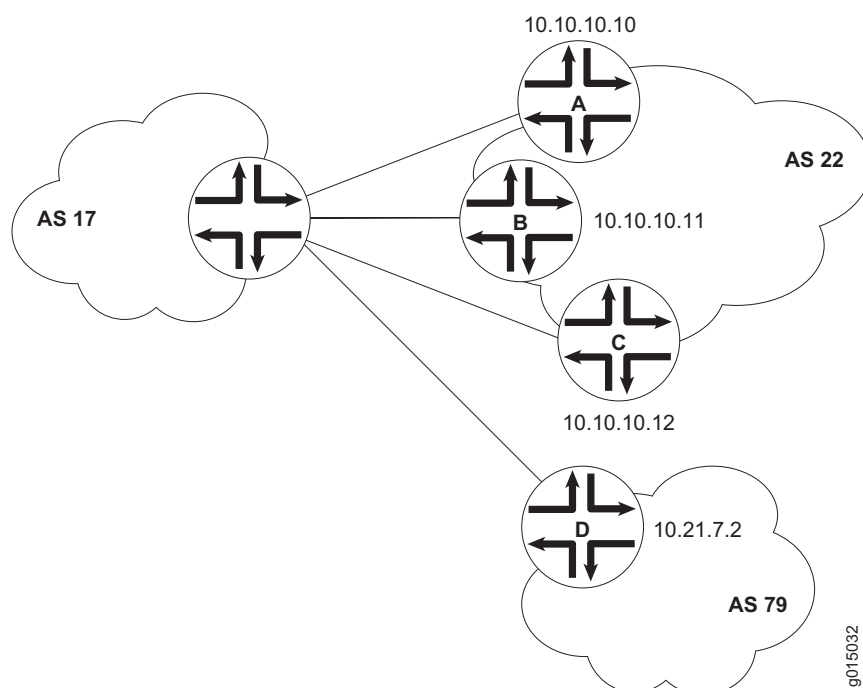
- Configuring a Point-to-Point Peering Session (Required) on page 327
- Configuring BGP Within a Network (Required) on page 330
- Configuring a Route Reflector (Optional) on page 331
- Configuring BGP Confederations (Optional) on page 334

For information about using the J-Web and CLI configuration editors, see “Using J-Web Configuration Tools” on page 3.

### Configuring a Point-to-Point Peering Session (Required)

To enable BGP traffic across one or more links, you must configure a BGP peering session with the adjacent host. Generally, such sessions are made at network exit points with neighboring hosts outside the autonomous system. Figure 70 shows a network with BGP peering sessions.

In the sample network, a Services Router 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 70: Typical Network with BGP Peering Sessions**

To configure the BGP peering sessions shown in Figure 70:

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 86.
3. If you are finished configuring the router, commit the configuration.
4. Go on to one of the following procedures:
  - To configure IBGP sessions between peers, see “Configuring BGP Within a Network (Required)” on page 330.
  - To configure route reflector clusters, see “Configuring a Route Reflector (Optional)” on page 331.
  - To subdivide autonomous systems (ASs), see “Configuring BGP Confederations (Optional)” on page 334.
  - To check the configuration, see “Verifying a BGP Configuration” on page 336.

**Table 86: Configuring BGP Peering Sessions**

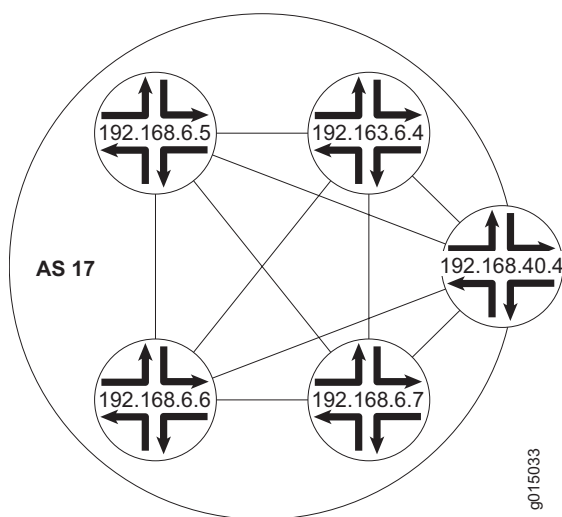
| <b>Task</b>                                                                                                                                                                                                                                                                       | <b>J-Web Configuration Editor</b>                                                                                                                                                                                                                                                                                                                                                                                                                                              | <b>CLI Configuration Editor</b>                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Navigate to the <b>Routing-options</b> level in the configuration hierarchy.                                                                                                                                                                                                      | In the configuration editor hierarchy, select <b>Routing-options</b> .                                                                                                                                                                                                                                                                                                                                                                                                         | From the top of the configuration hierarchy, enter<br><br>edit routing-options                                                                                                                                                                       |
| Set the network's AS number to <b>17</b> .                                                                                                                                                                                                                                        | 1. In the AS Number box, enter <b>17</b> .<br><br>2. Click <b>OK</b> .                                                                                                                                                                                                                                                                                                                                                                                                         | Set the AS number to <b>17</b> :<br><br>set autonomous-system 17                                                                                                                                                                                     |
| Navigate to the <b>Bgp</b> level in the configuration hierarchy.                                                                                                                                                                                                                  | In the configuration editor hierarchy, select <b>Protocols &gt; Bgp</b> .                                                                                                                                                                                                                                                                                                                                                                                                      | From the top of the configuration hierarchy, enter<br><br>edit protocols bgp                                                                                                                                                                         |
| Create the BGP group <b>external-peers</b> , and add the external neighbor addresses to the group.                                                                                                                                                                                | 1. In the Group box, click <b>Add new entry</b> .<br><br>2. In the Group name box, type the name of the group of external BGP peers— <b>external-peers</b> in this case.<br><br>3. In the Neighbor box, click <b>Add new entry</b> .<br><br>4. In the Address box, type the IP address of an external BGP peer, in dotted decimal notation, and click <b>OK</b> .<br><br>5. Repeat Step 3 and Step 4 for each BGP neighbor within the external group that you are configuring. | 1. Create the group <b>external-peers</b> , and add the address of an external neighbor:<br><br>set group external-peers neighbor 10.10.10.10<br><br>2. Repeat Step 1 for each BGP neighbor within the external peer group that you are configuring. |
| At the group level, set the AS number for the group <b>external-peers</b> to <b>22</b> .<br><br>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.                                                            | 1. In the Peer as box, type the number of the AS in which most peers in the <b>external-peers</b> group reside.<br><br>2. Click <b>OK</b> .                                                                                                                                                                                                                                                                                                                                    | From the [edit protocols bgp] hierarchy level:<br><br>set group external-peers peer-as 22                                                                                                                                                            |
| At the individual neighbor level, set the AS number for peer D to <b>79</b> .<br><br>Because peer D is a member of the group <b>external-peers</b> , it inherits the peer AS number configured at the group level. You must override this value at the individual neighbor level. | 1. Under Neighbor, in the Address column, click the IP address of peer D— <b>10.21.7.2</b> in this case.<br><br>2. In the Peer as box, type the AS number of the peer.<br><br>3. Click <b>OK</b> .                                                                                                                                                                                                                                                                             | From the [edit protocols bgp group external-peers] hierarchy level:<br><br>set neighbor 10.21.7.2 peer-as 79                                                                                                                                         |
| Set the group type to <b>external</b> .                                                                                                                                                                                                                                           | 1. From the Type list, select <b>external</b> .<br><br>2. Click <b>OK</b> .                                                                                                                                                                                                                                                                                                                                                                                                    | From the [edit protocols bgp group external-peers] hierarchy level:<br><br>set type external                                                                                                                                                         |

## Configuring BGP Within a Network (Required)

To configure BGP sessions between peering networks, you must configure point-to-point sessions between the external peers of the networks. Additionally, you must 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.

Figure 71 shows a typical network with external and internal peer sessions. In the sample network, the Services Router 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.

**Figure 71: Typical Network with EBGP External Sessions and IBGP Internal Sessions**



To configure IBGP in the network shown in Figure 71:

1. Configure all external peering sessions as described in “Configuring a Point-to-Point Peering Session (Required)” on page 327.
2. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
3. Perform the configuration tasks described in Table 87.
4. If you are finished configuring the router, commit the configuration.
5. Go on to one of the following procedures:
  - To configure route reflector clusters, see “Configuring a Route Reflector (Optional)” on page 331.
  - To subdivide autonomous systems (ASs), see “Configuring BGP Confederations (Optional)” on page 334.



- To check the configuration, see “Verifying a BGP Configuration” on page 336.

**Table 87: Configuring IBGP Peering Sessions**

| Task                                                                                                                                                                                                                                         | J-Web Configuration Editor                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | CLI Configuration Editor                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Navigate to the <b>Bgp</b> level in the configuration hierarchy.                                                                                                                                                                             | In the configuration editor hierarchy, select <b>Protocols &gt; Bgp</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                         | From the top of the configuration hierarchy, enter<br><br>edit protocols bgp                                                                                                                                                                                                         |
| Create the BGP group <b>internal-peers</b> , and add the internal neighbor addresses to the group.<br><br>You must configure a full IBGP mesh, which requires that each peer be configured with every other internal peer as a BGP neighbor. | <ol style="list-style-type: none"> <li>1. In the Group box, click <b>Add new entry</b>.</li> <li>2. In the Group name box, type the name of the group of internal BGP peers—<b>internal-peers</b> in this case.</li> <li>3. In the Neighbor box, click <b>Add new entry</b>.</li> <li>4. In the Address box, type the IP address of an internal BGP peer, in dotted decimal notation.</li> <li>5. Click <b>OK</b>.</li> <li>6. Repeat Step 3 and Step 4 for each internal BGP peer within the network.</li> </ol> | <ol style="list-style-type: none"> <li>1. Create the group <b>internal-peers</b>, and add the address of an internal neighbor:<br/><br/><b>set group internal-peers neighbor 192.168.6.4</b></li> <li>2. Repeat Step 1 for each internal BGP neighbor within the network.</li> </ol> |
| Set the group type to <b>internal</b> .                                                                                                                                                                                                      | <ol style="list-style-type: none"> <li>1. From the Type list, select <b>internal</b>.</li> <li>2. Click <b>OK</b>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                     | From the [edit protocols bgp group internal-peers] hierarchy level:<br><br>set type internal                                                                                                                                                                                         |
| Configure a routing policy to advertise BGP routes.                                                                                                                                                                                          | See the <i>J-series Services Router Advanced WAN Access Configuration Guide</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                      |

### Configuring a Route Reflector (Optional)

Because of the 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 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.

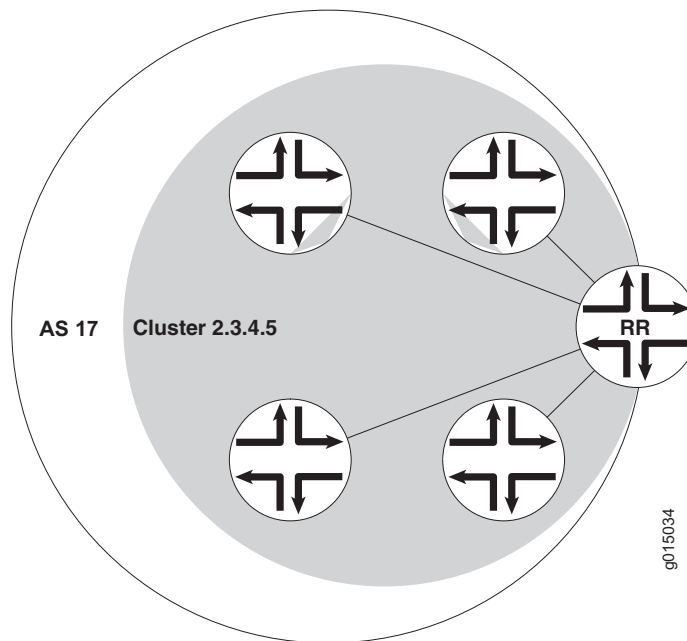


**NOTE:** You must have an Advanced BGP Feature license installed on each Services Router that uses a route reflector. For license details, see the *J-series Services Router Administration Guide*.

Figure 72 shows an IBGP network with a Services Router at IP address 192.168.40.4 acting as a route reflector. In the sample network, each router in cluster 2.3.4.5 has an internal client relationship to the route reflector. To configure the cluster:

- On the Services Router, create an internal group, configure an internal peer (neighbor) relationship to every other router in the cluster, and assign a cluster identifier.
- On each other router you are assigning to the cluster, create the cluster group and configure a client relationship to the route reflector.

**Figure 72: Typical IBGP Network Using a Route Reflector**



To configure IBGP in the network using the Services Router as a route reflector:

1. Configure all external peering sessions as described in “Configuring a Point-to-Point Peering Session (Required)” on page 327.
2. Navigate to the top of the configuration hierarchy in either the J-Web or CLI configuration editor.
3. Perform the configuration tasks described in Table 88.
4. If you are finished configuring the router, commit the configuration.
5. Go on to one of the following procedures:
  - To subdivide autonomous systems (ASs), see “Configuring BGP Confederations (Optional)” on page 334.

- To check the configuration, see “Verifying a BGP Configuration” on page 336.

**Table 88: Configuring a Route Reflector**

| <b>Task</b>                                                                                                                                                                                               | <b>J-Web Configuration Editor</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>CLI Configuration Editor</b>                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| On the Services Router that you are using as a route reflector, navigate to the <b>Bgp</b> level in the configuration hierarchy.                                                                          | In the configuration editor hierarchy, select <b>Protocols &gt; Bgp</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                | From the top of the configuration hierarchy, enter<br><br>edit protocols bgp                                                                                                                                                                                                                       |
| On the Services Router that you are using as a route reflector, create the BGP group <b>cluster-peers</b> , and add to the group the IP addresses of the internal neighbors that you want in the cluster. | <ol style="list-style-type: none"> <li>1. In the Group box, click <b>Add new entry</b>.</li> <li>2. In the Group name box, type the name of the group in which the BGP peer is configured—<b>cluster-peers</b> in this case.</li> <li>3. In the Neighbor box, click <b>Add new entry</b>.</li> <li>4. In the Address box, type the IP address of a BGP peer, in dotted decimal notation.</li> <li>5. Click <b>OK</b>.</li> <li>6. Repeat Step 3 and Step 4 for each BGP neighbor within the cluster that you are configuring.</li> </ol> | <ol style="list-style-type: none"> <li>1. Create the group <b>cluster-peers</b>, and add the address of an internal neighbor:<br/><br/><b>set group cluster-peers neighbor 192.168.6.4</b></li> <li>2. Repeat Step 1 for each BGP neighbor within the cluster that you are configuring.</li> </ol> |
| On the Services Router that you are using as a route reflector, set the group type to <b>internal</b> .                                                                                                   | From the Type list, select <b>internal</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | From the [edit protocols bgp group internal-peers] hierarchy level:<br><br><b>set type internal</b>                                                                                                                                                                                                |
| On the Services Router that you are using as a route reflector, configure the cluster identifier for the route reflector.                                                                                 | <ol style="list-style-type: none"> <li>1. In the Cluster box, enter the unique numeric cluster identifier.</li> <li>2. Click <b>OK</b>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                       | Set the cluster identifier:<br><br><b>set cluster 2.3.4.5</b>                                                                                                                                                                                                                                      |

**Table 88: Configuring a Route Reflector (continued)**

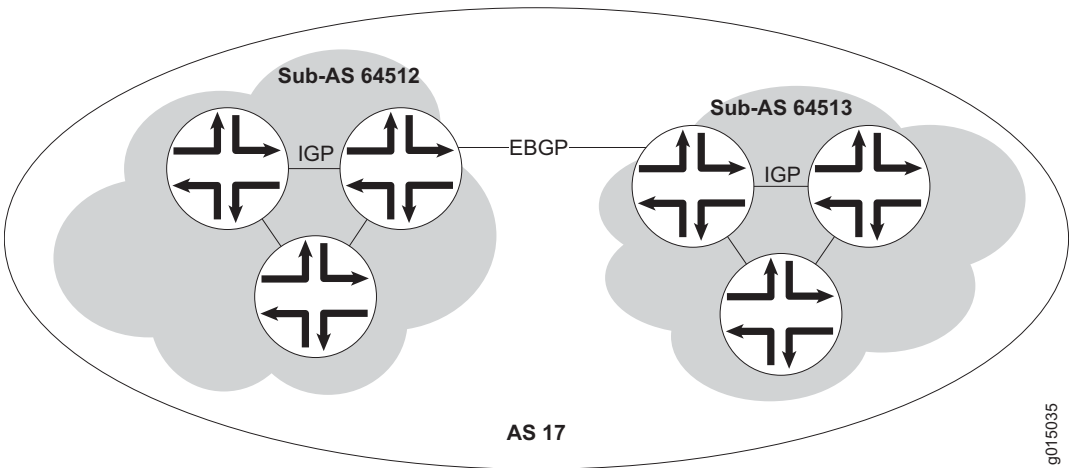
| <b>Task</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <b>J-Web Configuration Editor</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <b>CLI Configuration Editor</b>                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>On the other routers in the cluster, create the BGP group <b>cluster-peers</b>, and add the internal IP address of the route reflector.</p> <p>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.</p> <p><b>NOTE:</b> If the other routers in the network are Services Routers, follow the steps in this row. Otherwise, consult the router documentation for instructions.</p> | <p>On a client Services Router in the cluster:</p> <ol style="list-style-type: none"> <li>1. In the configuration editor hierarchy, select <b>Protocols &gt; Bgp</b>.</li> <li>2. In the Group box, click <b>Add new entry</b>.</li> <li>3. In the Group name box, type the name of the group in which the BGP peer is configured—<b>cluster-peers</b> in this case.</li> <li>4. In the Neighbor box, click <b>Add new entry</b>.</li> <li>5. In the Address box, type the IP address of the route reflector, in dotted decimal notation—in this case, <b>192.168.40.4</b>.</li> <li>6. Click <b>OK</b>.</li> </ol> | <p>On a client Services Router in the cluster:</p> <ol style="list-style-type: none"> <li>1. From the top of the configuration hierarchy, enter<br/><b>edit protocols bgp</b></li> <li>2. Create the group <b>cluster-peers</b>, and add only the route reflector address to the group:<br/><b>set group cluster-peers neighbor 192.168.40.4</b></li> </ol> |
| Configure a routing policy to advertise BGP routes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | See the <i>J-series Services Router Advanced WAN Access Configuration Guide</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                             |

## Configuring BGP Confederations (Optional)

To help solve BGP scaling problems caused by the IBGP full-mesh requirement, you can divide your AS into sub-ASs called confederations. As Figure 73 shows, the connections between the sub-ASs are made through EBGP sessions, and the internal connections are made through standard IBGP sessions.

In the sample network, 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.

Figure 73: Typical Network Using BGP Confederations



To configure the BGP confederations shown in Figure 73:

- 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 89.
- 3. If you are finished configuring the router, commit the configuration.
- 4. To check the configuration, see “Verifying a BGP Configuration” on page 336.

Table 89: Configuring BGP Confederations

| Task                                                                                                                                                                                                | J-Web Configuration Editor                                                                                                    | CLI Configuration Editor                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Navigate to the <b>Routing-options</b> level in the configuration hierarchy.                                                                                                                        | In the configuration editor hierarchy, select <b>Routing-options</b> .                                                        | From the top of the configuration hierarchy, enter<br><br>edit routing-options               |
| Set the AS number to the sub-AS number <b>64512</b> .<br><br>The sub-AS number is a unique AS number that is usually taken from the pool of private AS numbers— <b>64512</b> through <b>65535</b> . | <ul style="list-style-type: none"><li>1. In the AS Number box, enter the sub-AS number.</li><li>2. Click <b>OK</b>.</li></ul> | Set the sub-AS number:<br><br>set autonomous-system 64512                                    |
| Navigate to the <b>Confederation</b> level in the configuration hierarchy.                                                                                                                          | In the configuration editor hierarchy, select <b>Routing-options &gt; Confederation</b> .                                     | From the top of the configuration hierarchy, enter<br><br>edit routing-options confederation |
| Set the confederation number to the AS number <b>17</b> .                                                                                                                                           | In the Confederation as box, enter <b>17</b> .                                                                                | Set the confederation AS number:<br><br>set 17                                               |

**Table 89: Configuring BGP Confederations (continued)**

| <b>Task</b>                                                                                                                                                                                                                   | <b>J-Web Configuration Editor</b>                                                                                                                                                                                                                         | <b>CLI Configuration Editor</b>                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| Add the sub-ASs as members of the confederation. Every sub-AS within the AS must be added as a confederation member.                                                                                                          | <ol style="list-style-type: none"> <li>1. Next to Members, click <b>Add new entry</b>.</li> <li>2. In the Value box, enter the sub-ASs that are members of this confederation. Separate multiple sub-ASs with a space.</li> </ol>                         | Add members to the confederation:<br><br>set 17 members 64512 64513 |
| Using EBGp, configure the peering session between the confederations (from router A to router B in this example).<br><br>When setting the peer AS number for these sessions, use the sub-AS number rather than the AS number. | See “Configuring a Point-to-Point Peering Session (Required)” on page 327.                                                                                                                                                                                |                                                                     |
| Using IBGP, configure internal sessions within a sub-AS. You can configure an IBGP full mesh, or you can configure a route reflector.                                                                                         | <ul style="list-style-type: none"> <li>■ To configure an IBGP full mesh, see “Configuring BGP Within a Network (Required)” on page 330.</li> <li>■ To configure a route reflector, see “Configuring a Route Reflector (Optional)” on page 331.</li> </ul> |                                                                     |

## Verifying a BGP Configuration

To verify a BGP configuration, perform these tasks:

- Verifying BGP Neighbors on page 336
- Verifying BGP Groups on page 337
- Verifying BGP Summary Information on page 338
- Verifying Reachability of All Peers in a BGP Network on page 339

### 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
  Active prefixes: 0
  Received prefixes: 2
  Suppressed due to damping: 0
Last traffic (seconds): Received 3    Sent 3    Checked 3
Input messages: Total 9    Updates 6    Refreshes 0    Octets 403
Output messages: Total 7    Updates 3    Refreshes 0    Octets 365
Output Queue[0]: 0
Output Queue[1]: 0
Trace options: detail packets
Trace file: /var/log/bgppgr size 131072 files 10

```

**What It Means** The output shows a list of the BGP neighbors with detailed session information. Verify the following information:

- Each configured peering neighbor is listed.
- For **State**, each BGP session is Established.
- For **Type**, each peer is configured as the correct type (either internal or external).
- For **AS**, the AS number of the BGP neighbor is correct.

For more information about `show bgp neighbor`, see the *JUNOS Routing Protocols and Policies Command Reference*.

## Verifying BGP Groups

**Purpose** Verify that the BGP groups are configured correctly.

**Action** From the CLI, enter the `show bgp group` command.

**Sample Output** `user@host> show bgp group`

```

Group Type: Internal      AS: 10045      Local AS: 10045
Name: pe-to-asbr2        Flags: Export Eval
Export: [ match-all ]
Total peers: 1           Established: 1
4.4.4.4+179
bgp.l3vpn.0: 1/1/0
vpn-green.inet.0: 1/1/0

Groups: 1  Peers: 1  External: 0  Internal: 1  Down peers: 0  Flaps: 0
Table      Tot Paths  Act Paths Suppressed  History Damp State  Pending
bgp.l3vpn.0      1          1          0          0          0          0

```

**What It Means** 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.

For more information about `show bgp group`, see the *JUNOS Routing Protocols and Policies Command Reference*.

## 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
Peer      AS      InPkt    OutPkt    OutQ    Flaps Last Up/Dwn State|#Active/Rece
10.0.0.2   65002   88675    88652     0        2      42:38 2/4/0
10.0.0.3   65002   54528    54532     0        1     2w4d22h 0/0/0
10.0.0.4   65002   51597    51584     0        0     2w3d22h 2/2/0

```

**What It Means** 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.

For more information about `show bgp summary`, see the *JUNOS Routing Protocols and Policies Command Reference*.

## 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 Services Router.

**Action** For each Services Router in the BGP network:

1. In the J-Web interface, select **Diagnose > Ping Host**.
2. In the Remote Host box, type the name of a host for which you want to verify reachability from the Services Router.
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
```

**What It Means** 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. For more information about the ping output, see the *J-series Services Router Administration Guide*.

For more information about using the J-Web interface to ping a host, see the *J-series Services Router Administration Guide*.

For information about the `ping` command, see the *J-series Services Router Administration Guide* or the *JUNOS System Basics and Services Command Reference*.



## **Part 4**

# **Index**



# Index

## Symbols

[ ], in configuration statements ..... xix  
 { }, in configuration statements ..... xx  
 ( ), in syntax descriptions ..... xix  
 < > , in syntax descriptions ..... xix  
 | (pipe), in syntax descriptions ..... xix  
 #, comments in configuration statements ..... xix  
 1-port four-wire mode, SHDSL *See* ATM-over-SHDSL interfaces  
 2-port two-wire mode, SHDSL *See* ATM-over-SHDSL interfaces

## A

AAL5 multiplex encapsulation ..... 153  
     ATM-over-ADSL for PPP-over-ATM (PPPoA) interfaces ..... 142  
     ATM-over-ADSL interfaces ..... 136  
     ATM-over-SHDSL interfaces ..... 147  
 ABM (Asynchronous Balance Mode), HDLC ..... 86  
 ABRs *See* area border routers  
 access concentrator  
     as a PPPoE server ..... 166  
     naming for PPPoE (configuration editor) ..... 176  
     naming for PPPoE (Quick Configuration) ..... 172  
 active routes, versus passive routes ..... 269  
 Add button ..... 8  
 Add new entry link ..... 11  
 addresses  
     BGP external peer address (configuration editor) ..... 329  
     BGP internal peer address (configuration editor) ..... 331  
     BGP local address (Quick Configuration) ..... 326  
     BGP peer address (Quick Configuration) ..... 326  
     IS-IS NETs ..... 253  
         *See also* NETs  
     IS-IS NSAP addresses ..... 315  
     physical, in data link layer ..... 48  
 adjacencies, IS-IS  
     hello PDUs for ..... 254  
         *See also* IS-IS  
     verifying ..... 320  
     verifying (detail) ..... 321  
 ADSL interfaces *See* ATM-over-ADSL interfaces

ADSL ports *See* ATM-over-ADSL interfaces  
 ADSL2+ operating mode ..... 138, 141  
 advertisements *See* LSAs; route advertisements  
 aggregation, route ..... 241  
 alternate mark inversion *See* AMI encoding  
 AMI (alternate mark inversion) encoding  
     E1 ..... 104  
     overview ..... 55  
     T1 ..... 114  
 Annex A PIMs  
     ATM-over-ADSL interfaces ..... 138  
         *See also* ATM-over-ADSL interfaces  
     ATM-over-SHDSL interfaces ..... 149  
         *See also* ATM-over-SHDSL interfaces  
     ATM-over-SHDSL modes ..... 144  
     G.SHDSL PIMs, setting annex type on ..... 148, 152  
     operating modes (configuration editor) ..... 141  
     operating modes (Quick Configuration) ..... 138  
     standards supported ..... 70  
 Annex B PIMs  
     ATM-over-ADSL interfaces ..... 138  
         *See also* ATM-over-ADSL interfaces  
     ATM-over-SDSL interfaces ..... 149  
         *See also* ATM-over-SHDSL interfaces  
     ATM-over-SHDSL modes ..... 144  
     G.SHDSL PIMs, setting annex type on ..... 148, 152  
     operating modes (configuration editor) ..... 141  
     operating modes (Quick Configuration) ..... 138  
     standards supported ..... 70  
 ANSI DMT operating mode ..... 138, 141  
 ANSI T1.413 Issue II operating mode ..... 138, 141  
 anycast IPv6 addresses ..... 91  
 Apply button ..... 8  
 area border routers  
     adding interfaces ..... 305  
     area ID (configuration editor) ..... 305  
     backbone area *See* backbone area  
     backbone area interface ..... 305  
     description ..... 249  
 areas *See* area border routers; backbone area; IS-IS, areas; NSSAs; stub areas  
 ARM (Asynchronous Response Mode), HDLC ..... 86  
 AS path  
     description ..... 259

|                                                                            |          |
|----------------------------------------------------------------------------|----------|
| forcing by MED .....                                                       | 260      |
| role in route selection .....                                              | 258      |
| ASs (autonomous systems)                                                   |          |
| area border routers .....                                                  | 249      |
| AS number (configuration editor) .....                                     | 329      |
| AS number (Quick Configuration) .....                                      | 326      |
| breaking into confederations .....                                         | 264      |
| description .....                                                          | 238      |
| group AS number (configuration editor) .....                               | 329      |
| individual AS number (configuration editor) .....                          | 329      |
| IS-IS networks .....                                                       | 253      |
| sample BGP confederation .....                                             | 335      |
| stub areas <i>See</i> stub areas                                           |          |
| sub-AS number .....                                                        | 335      |
| asymmetric digital subscriber line (ADSL)                                  |          |
| <i>See</i> ATM-over-ADSL interfaces                                        |          |
| Asynchronous Balance Mode (ABM), HDLC .....                                | 86       |
| asynchronous networks                                                      |          |
| data stream clocking .....                                                 | 77       |
| explicit clocking signal transmission .....                                | 77       |
| overview .....                                                             | 77       |
| Asynchronous Response Mode (ARM), HDLC .....                               | 86       |
| Asynchronous Transfer Mode (ATM) interfaces                                |          |
| <i>See</i> ATM-over-ADSL interfaces; ATM-over-SHDSL interfaces             |          |
| at-0/0/0 <i>See</i> ATM-over-ADSL interfaces;                              |          |
| ATM-over-SHDSL interfaces                                                  |          |
| ATM interfaces <i>See</i> ATM-over-ADSL interfaces;                        |          |
| ATM-over-SHDSL interfaces                                                  |          |
| ATM NLPID encapsulation                                                    |          |
| ATM-over-ADSL interfaces .....                                             | 136, 142 |
| ATM-over-SHDSL interfaces .....                                            | 147, 153 |
| ATM PPP over AAL5 LLC encapsulation                                        |          |
| ATM-over-ADSL for PPP-over-ATM (PPPoA) interfaces .....                    | 136, 142 |
| ATM-over-SHDSL interfaces .....                                            | 147, 153 |
| ATM PVC encapsulation                                                      |          |
| ATM-over-ADSL interfaces .....                                             | 137, 141 |
| ATM-over-SHDSL interfaces .....                                            | 148, 151 |
| ATM SNAP encapsulation                                                     |          |
| ATM-over-ADSL interfaces .....                                             | 136, 142 |
| ATM-over-SHDSL interfaces .....                                            | 147, 153 |
| ATM VC multiplex encapsulation                                             |          |
| ATM-over-ADSL interfaces .....                                             | 136, 142 |
| ATM-over-SHDSL interfaces .....                                            | 147, 153 |
| ATM-over-ADSL interfaces .....                                             | 138      |
| adding .....                                                               | 138      |
| ADSL overview .....                                                        | 69       |
| ADSL systems .....                                                         | 70       |
| ADSL topology .....                                                        | 71       |
| ADSL2 .....                                                                | 71       |
| ADSL2 + .....                                                              | 71       |
| ATM interface type .....                                                   | 71       |
| CHAP for PPPoA .....                                                       | 154      |
| CHAP for PPPoE .....                                                       | 178      |
| description .....                                                          | 133      |
| encapsulation types, logical (configuration editor) .....                  | 142      |
| encapsulation types, logical (Quick Configuration) .....                   | 136      |
| encapsulation types, physical (configuration editor) .....                 | 141      |
| encapsulation types, physical (Quick Configuration) .....                  | 137      |
| logical properties (configuration editor) .....                            | 142      |
| logical properties (Quick Configuration) .....                             | 135      |
| operating modes (configuration editor) .....                               | 141      |
| operating modes (Quick Configuration) .....                                | 138      |
| physical properties .....                                                  | 139      |
| PPPoE configuration .....                                                  | 175      |
| PPPoE encapsulation .....                                                  | 174      |
| PPPoE session on .....                                                     | 167      |
| preparation .....                                                          | 132      |
| Quick Configuration .....                                                  | 133      |
| statistics .....                                                           | 160      |
| VCI .....                                                                  | 136, 143 |
| verifying .....                                                            | 156      |
| verifying a PPPoA configuration .....                                      | 160      |
| verifying a PPPoE configuration .....                                      | 180–181  |
| VPI .....                                                                  | 137, 140 |
| <i>See also</i> PPPoE; PPPoE over ATM-over-ADSL; PPPoE over ATM-over-SHDSL |          |
| ATM-over-SHDSL interfaces .....                                            | 72       |
| 1-port four-wire mode .....                                                | 144      |
| 1-port four-wire mode, setting .....                                       | 148, 150 |
| 2-port two-wire mode, overview .....                                       | 144      |
| 2-port two-wire mode, setting .....                                        | 148, 150 |
| adding .....                                                               | 149      |
| annex type, setting .....                                                  | 148, 152 |
| ATM interface type .....                                                   | 71       |
| CHAP for PPPoA .....                                                       | 154      |
| CHAP for PPPoE .....                                                       | 178      |
| description .....                                                          | 143      |
| “dying gasp” .....                                                         | 163      |
| encapsulation types, logical (configuration editor) .....                  | 153      |
| encapsulation types, logical (Quick Configuration) .....                   | 147      |
| encapsulation types, physical .....                                        | 148      |
| encapsulation types, physical (configuration editor) .....                 | 151      |
| encapsulation types, physical (Quick Configuration) .....                  | 148      |
| line speed .....                                                           | 148      |
| logical properties (configuration editor) .....                            | 152      |
| logical properties (Quick Configuration) .....                             | 146      |
| loopback testing .....                                                     | 148      |
| overview .....                                                             | 72       |
| PPPoE configuration .....                                                  | 175      |
| PPPoE encapsulation .....                                                  | 174      |

- PPPoE session on ..... 167
  - preparation..... 132
  - Quick Configuration ..... 144
  - SNEXT threshold..... 149, 152
  - SNR margin ..... 149, 152
  - statistics ..... 163
  - status ..... 163
  - VCI ..... 147, 154
  - verifying ..... 161
  - verifying a PPPoE configuration ..... 180–181
  - VPI ..... 148, 151
  - See also* G.SHDSL PIMs
  - authentication
    - CHAP, for PPPoE interfaces ..... 169
    - OSPF, MD5 ..... 310
    - OSPF, plain-text passwords ..... 310
    - RIPv2, MD5 ..... 290
    - RIPv2, plain-text passwords ..... 289
  - auto operating mode ..... 138, 141
  - autonomous systems *See* ASs
- B**
- B-channels
    - description ..... 72
    - naming convention ..... 190
    - verifying ..... 224
  - B8ZS encoding ..... 56
  - backbone area
    - area ID (configuration editor) ..... 302
    - area ID (Quick Configuration) ..... 298
    - area type (Quick Configuration) ..... 299
    - configuring ..... 300
    - description ..... 250
    - interface ..... 305
  - backoff algorithm, collision detection ..... 51
  - backup connection, ISDN ..... 187
  - backward-explicit congestion notification (BECN)
    - bits ..... 80
  - bandwidth on demand, ISDN
    - dialer pool ..... 215
  - bandwidth-on-demand, ISDN
    - dialer interface (configuration editor) ..... 210
    - ISDN BRI interface (configuration editor) ..... 214
    - overview ..... 210
  - bc-0/0/0 ..... 190
  - BECN (backward-explicit congestion notification)
    - bits ..... 80
  - BERTs (bit error rate tests) ..... 76
  - BGP (Border Gateway Protocol)
    - AS number (Quick Configuration) ..... 326
    - See also* ASs (autonomous systems), AS number
    - AS path ..... 259
    - See also* AS path
    - confederations *See* BGP confederations
    - enabling (Quick Configuration) ..... 326
    - external ..... 257
    - See also* EBGp
    - external group type (configuration editor) ..... 329
    - external neighbor (peer) address (configuration editor) ..... 329
    - full mesh requirement ..... 257, 324
    - internal ..... 257
    - See also* IBGP
    - internal group type (configuration editor) ..... 331
    - internal neighbor (peer) address (configuration editor) ..... 331
    - local address (Quick Configuration) ..... 326
    - local preference ..... 258
    - MED metric ..... 260
    - origin value ..... 260
    - overview ..... 255, 323
    - peer address (Quick Configuration) ..... 326
    - peer AS number (Quick Configuration) ..... 326
    - peering sessions *See* BGP peers; BGP sessions
    - point-to-point internal peer session (configuration editor) ..... 330
    - point-to-point peer session (configuration editor) ..... 327
    - Quick Configuration ..... 325
    - requirements ..... 325
    - route reflectors *See* BGP route reflectors
    - route selection process ..... 258
    - See also* route selection
    - router ID (Quick Configuration) ..... 326
    - routing policy (configuration editor) ..... 331
    - See also* routing policies
    - sample BGP peer network ..... 328
    - sample confederation ..... 335
    - sample full mesh ..... 330
    - sample route reflector ..... 332
    - scaling techniques ..... 261
    - session establishment ..... 256
    - session maintenance ..... 257
    - verifying BGP configuration ..... 338
    - verifying BGP groups ..... 337
    - verifying BGP peers (neighbors) ..... 336
    - verifying peer reachability ..... 339
  - BGP confederations
    - confederation members ..... 336
    - confederation number ..... 335
    - creating (configuration editor) ..... 334
    - description ..... 264, 324
    - sample network ..... 335
    - sub-AS number ..... 335
  - BGP groups
    - cluster identifier (configuration editor) ..... 333
    - confederations (configuration editor) ..... 334
    - external group type (configuration editor) ..... 329
    - external, creating (configuration editor) ..... 329

|                                                                 |          |
|-----------------------------------------------------------------|----------|
| group AS number (configuration editor)                          | 329      |
| internal group type (configuration editor)                      | 331      |
| internal, creating (configuration editor)                       | 331      |
| internal, creating for a route reflector (configuration editor) | 333      |
| verifying                                                       | 337      |
| BGP messages                                                    |          |
| to establish sessions                                           | 256      |
| update, to maintain sessions                                    | 257      |
| BGP page                                                        | 325      |
| BGP peers                                                       |          |
| directing traffic by local preference                           | 258      |
| external (configuration editor)                                 | 327      |
| internal (configuration editor)                                 | 330      |
| internal, sample full mesh                                      | 330      |
| internal, sample route reflector                                | 332      |
| peer address (Quick Configuration)                              | 326      |
| peer AS number (Quick Configuration)                            | 326      |
| point-to-point connections                                      | 256      |
| routing policy (configuration editor)                           | 331      |
| <i>See also</i> routing policies                                |          |
| sample peer network                                             | 328      |
| sessions between peers                                          | 323      |
| verifying                                                       | 336, 338 |
| verifying reachability                                          | 339      |
| BGP route reflectors                                            |          |
| cluster (configuration editor)                                  | 333      |
| cluster identifier (configuration editor)                       | 333      |
| cluster of clusters                                             | 263      |
| creating (configuration editor)                                 | 331      |
| description                                                     | 261, 324 |
| group type (configuration editor)                               | 333      |
| multiple clusters                                               | 262      |
| sample IBGP network                                             | 332      |
| BGP sessions                                                    |          |
| configured at both ends                                         | 323      |
| establishment                                                   | 256      |
| maintenance                                                     | 257      |
| point-to-point external (configuration editor)                  | 327      |
| point-to-point internal (configuration editor)                  | 330      |
| sample peering session                                          | 256      |
| types                                                           | 324      |
| bipolar with 8-zero substitution (B8ZS) encoding                | 56       |
| bit error rate tests (BERTs)                                    | 76       |
| bit stuffing                                                    | 59       |
| Border Gateway Protocol <i>See</i> BGP                          |          |
| br-0/0/0                                                        | 190      |
| braces, in configuration statements                             | xx       |
| brackets                                                        |          |
| angle, in syntax descriptions                                   | xix      |
| square, in configuration statements                             | xix      |
| bridges, on LAN segments                                        | 52       |
| buttons                                                         | 12       |
| Add (Quick Configuration)                                       | 8        |
| Apply (Quick Configuration)                                     | 8        |

|                                      |    |
|--------------------------------------|----|
| Cancel (J-Web configuration editor)  | 12 |
| Cancel (Quick Configuration)         | 8  |
| Commit (J-Web configuration editor)  | 12 |
| CONFIG <i>See</i> CONFIG button      |    |
| Delete (Quick Configuration)         | 8  |
| Discard (J-Web configuration editor) | 12 |
| OK (J-Web configuration editor)      | 12 |
| OK (Quick Configuration)             | 8  |
| Refresh (J-Web configuration editor) | 12 |
| <i>See also</i> radio buttons        |    |

## C

|                                                                  |          |
|------------------------------------------------------------------|----------|
| C-bit parity frame format                                        |          |
| enable or disable on T3 ports                                    | 118      |
| overview                                                         | 61       |
| cables                                                           |          |
| T1 cable length                                                  | 115      |
| T3 cable length                                                  | 118      |
| call setup, ISDN                                                 | 74       |
| callback, ISDN                                                   |          |
| dialer interface (configuration editor)                          | 217      |
| encapsulation matching                                           | 216      |
| overview                                                         | 215      |
| rejecting incoming calls (configuration editor)                  | 220      |
| screening incoming calls (configuration editor)                  | 219      |
| voice not supported                                              | 215      |
| calling number, ISDN                                             | 193, 200 |
| Cancel button                                                    |          |
| J-Web configuration editor                                       | 12       |
| Quick Configuration                                              | 8        |
| canceled a commit                                                | 30–31    |
| carrier sense multiple access with collision detection (CSMA/CD) | 50       |
| ccc protocol family                                              | 87       |
| Challenge Handshake Authentication Protocol                      |          |
| <i>See</i> CHAP                                                  |          |
| channel number, in interface name                                | 47       |
| channel service unit (CSU) device                                | 83       |
| CHAP (Challenge Handshake Authentication Protocol)               |          |
| E1 local identity                                                | 103      |
| E3 local identity                                                | 106      |
| enabling for PPPoA                                               | 154      |
| enabling for PPPoE (configuration editor)                        | 178      |
| enabling for PPPoE (Quick Configuration)                         | 171      |
| enabling on ATM-over-ADSL interfaces                             | 154      |
| enabling on ATM-over-SHDSL interfaces                            | 154      |
| enabling on E1                                                   | 103      |
| enabling on E3                                                   | 106      |
| enabling on serial interfaces                                    | 120      |
| enabling on T1                                                   | 113      |
| enabling on T3                                                   | 117      |
| overview                                                         | 82       |
| PPP links                                                        | 82       |
| PPPoE                                                            | 169      |
| serial interface local identity                                  | 120      |



- T1 local identity.....113
  - T3 local identity.....117
- CHAP secret *See* CHAP, local identity
- checksum
  - E1 frame ..... 104
  - E3 frame ..... 108
  - overview .....78
  - T1 frame .....115
  - T3 frame .....118
- Cisco NLPID encapsulation
  - ATM-over-ADSL interfaces..... 136, 142
  - ATM-over-SHDSL interfaces ..... 147, 153
- classful addressing.....88
- clear system commit command .....31
- CLI configuration editor
  - activating a configuration .....30
  - ATM-over-ADSL interfaces..... 138
  - ATM-over-SHDSL interfaces ..... 149
  - BGP..... 327
  - CHAP on ATM-over-ADSL interfaces ..... 154
  - CHAP on ATM-over-SHDSL interfaces ..... 154
  - command summary..... 5
  - committing files .....29
  - confirming a configuration.....30
  - CRTP ..... 124
  - exiting.....21
  - IS-IS ..... 317
  - ISDN connections..... 198
  - managing files .....33
  - modifying a configuration.....24
  - network interfaces..... 122
  - network interfaces, adding..... 122
  - network interfaces, deleting..... 126
  - OSPF ..... 299
  - PPPoE ..... 172
  - PPPoE over ATM-over-ADSL ..... 172
  - PPPoE over ATM-over-SHDSL ..... 172
  - RIP..... 283
  - saving files .....36
  - starting .....21
  - static routes ..... 272
  - using show commands with .....33
  - verifying a configuration .....29
- clickable configuration..... 9
  - committing.....13
  - discarding changes .....12
  - viewing and editing..... 9
- See also* J-Web configuration editor
- clock rate, serial interface
  - DTE default reduction .....66
  - values ..... 121
- clocking
  - data stream clocking .....77
  - E1 ..... 103
  - E3 ..... 106
  - explicit clocking signal transmission .....77
  - overview .....76
  - serial interface ..... 121
  - serial interface, inverting the transmit clock .. 66, 121
  - serial interface, modes .....65
  - T1.....113
  - T3.....117
- clusters *See* BGP route reflectors
- collision detection
  - backoff algorithm.....51
  - overview .....51
- combined stations, HDLC .....85
- comments, in configuration statements ..... xix
- commit and-quit command .....30
- commit at command .....30
- Commit button.....12
- commit check command.....29
- commit command.....29
- commit confirmed command.....30
- committed configuration
  - activating (CLI configuration editor) .....30
  - canceling a commit (CLI configuration editor) .....31
  - comparing two configurations .....18
  - confirming (CLI configuration editor) .....30
  - description ..... 4
  - methods.....17
  - replacing (CLI configuration editor).....31
  - rescue configuration (CLI configuration editor) ....32
  - rescue configuration (J-Web) .....20
  - scheduling (CLI configuration editor) .....30
  - storage location..... 5
  - summaries .....17
  - verifying (CLI configuration editor) .....29
  - viewing previous (CLI configuration editor) .....32
- complete sequence number PDU (CSNP) ..... 255
- Compressed Real-Time Transport Protocol *See* CRTP
- confederations *See* BGP confederations
- CONFIG button
  - default behavior ..... 20, 32
  - disabling .....32
  - return to factory configuration ..... 20, 32
- config-button <no-rescue> <no-clear> statement ...32
- configuration
  - activating (CLI configuration editor) .....30
  - adding a statement (CLI configuration editor).....25
  - basic.....7
  - changing part of a file (CLI configuration editor)....34
  - CLI commands..... 5
  - CLI configuration mode .....21
  - committed ..... 4
  - committing (CLI configuration editor) .....29
  - committing (J-Web) .....13
  - committing as a text file, with caution (J-Web).....13
  - confirming (CLI configuration editor) .....30

|                                                                        |        |                                                                                                                                       |
|------------------------------------------------------------------------|--------|---------------------------------------------------------------------------------------------------------------------------------------|
| copying a statement .....                                              | 26     | <i>See also</i> CLI configuration editor; configuration;<br>configuration history; J-Web configuration<br>editor; Quick Configuration |
| deactivating a statement .....                                         | 28     | configure command .....                                                                                                               |
| deleting a statement .....                                             | 25     | configure exclusive command .....                                                                                                     |
| deleting with the CONFIG button .....                                  | 20, 32 | Configure link .....                                                                                                                  |
| disabling CONFIG button .....                                          | 32     | configure private command .....                                                                                                       |
| discarding changes (J-Web) .....                                       | 12     | confirming a configuration .....                                                                                                      |
| downloading (J-Web) .....                                              | 19     | congestion control                                                                                                                    |
| editing (J-Web) .....                                                  | 9      | for Frame Relay, with DE bits .....                                                                                                   |
| editing as a text file, with caution (J-Web) .....                     | 13     | connection process                                                                                                                    |
| history .....                                                          | 16     | ISDN BRI interfaces .....                                                                                                             |
| <i>See also</i> configuration history                                  |        | LCP, for PPP .....                                                                                                                    |
| inserting an identifier .....                                          | 27     | serial interfaces .....                                                                                                               |
| J-Web options .....                                                    | 5      | connectivity                                                                                                                          |
| loading new (CLI configuration editor) .....                           | 33     | bidirectional (BGP) .....                                                                                                             |
| loading previous (CLI configuration editor) .....                      | 31     | bidirectional (OSPF) .....                                                                                                            |
| loading previous (J-Web) .....                                         | 20     | unidirectional (RIP) .....                                                                                                            |
| locked, with the configure exclusive command .....                     | 22     | conventions                                                                                                                           |
| managing files (CLI configuration editor) .....                        | 33     | for interface names .....                                                                                                             |
| managing files (J-Web) .....                                           | 15     | notice icons .....                                                                                                                    |
| merging (CLI configuration editor) .....                               | 34     | text and syntax .....                                                                                                                 |
| modifying (CLI configuration editor) .....                             | 24     | copy command .....                                                                                                                    |
| modifying a statement (CLI configuration editor) .....                 | 25     | cost, of a network path <i>See</i> path cost metrics                                                                                  |
| overriding (CLI configuration editor) .....                            | 34     | CPE device, Services Router as, with PPPoE .....                                                                                      |
| renaming an identifier .....                                           | 26     | <i>See also</i> PPPoE                                                                                                                 |
| replacing configuration statements (CLI<br>configuration editor) ..... | 34     | CRC (cyclic redundancy check) .....                                                                                                   |
| requirements .....                                                     | 6      | CRTP (Compressed Real-Time Transport Protocol)                                                                                        |
| rescuing (CLI configuration editor) .....                              | 32     | E1 interfaces .....                                                                                                                   |
| rescuing (J-Web) .....                                                 | 20     | overview .....                                                                                                                        |
| rollback (CLI configuration editor) .....                              | 31     | T1 interfaces .....                                                                                                                   |
| rollback (J-Web) .....                                                 | 20     | CSMA/CD (carrier sense multiple access with collision<br>detection) .....                                                             |
| saving (CLI configuration editor) .....                                | 36     | CSNP (complete sequence number PDU) .....                                                                                             |
| uploading (J-Web) .....                                                | 14     | CSU (channel service unit) device .....                                                                                               |
| users-editors, viewing .....                                           | 18     | curly braces, in configuration statements .....                                                                                       |
| verifying (CLI configuration editor) .....                             | 29     | customer premises equipment (CPE) device, Services<br>Router as, with PPPoE .....                                                     |
| viewing as a text file (J-Web) .....                                   | 8      | <i>See also</i> PPPoE                                                                                                                 |
| configuration database, summary .....                                  | 16     | customer support .....                                                                                                                |
| configuration hierarchy, navigating .....                              | 23     | contacting JTAC .....                                                                                                                 |
| configuration history                                                  |        | cyclic redundancy check (CRC) .....                                                                                                   |
| comparing files .....                                                  | 18     |                                                                                                                                       |
| database summary .....                                                 | 16     | <b>D</b>                                                                                                                              |
| displaying .....                                                       | 16     | D-channel                                                                                                                             |
| downloading files .....                                                | 19     | description .....                                                                                                                     |
| summary .....                                                          | 17     | naming convention .....                                                                                                               |
| users-editors, viewing .....                                           | 18     | verifying .....                                                                                                                       |
| Configuration History page .....                                       | 16     | D4 framing .....                                                                                                                      |
| configuration mode                                                     |        | data communications equipment <i>See</i> DCE                                                                                          |
| entering and exiting .....                                             | 21     | data inversion                                                                                                                        |
| using show commands in .....                                           | 33     | E1 .....                                                                                                                              |
| configuration text                                                     |        | T1 .....                                                                                                                              |
| editing and committing, with caution .....                             | 13     | data link layer                                                                                                                       |
| viewing .....                                                          | 8      | error notification .....                                                                                                              |
| configuration tools .....                                              | 3      |                                                                                                                                       |

- flow control .....49
- frame sequencing.....48
- MAC addresses.....48
- network topology.....48
- physical addressing.....48
- purpose.....48
- sublayers.....49
- data service unit (DSU) device .....83
- data stream clocking.....77
- data terminal equipment *See* DTE
- data-link connection identifiers (DLCIs) .....80
- Database Information page .....16
- dc-0/0/0 .....190
- DCE (data communications equipment)
  - serial connection process .....64
  - serial device.....63
- DCE clocking mode.....65
- DDR *See* dial-on-demand routing backup, ISDN
- DE (discard eligibility) bits
  - BECN bits .....80
  - FECN bits .....80
- deactivate command .....28
- deactivating configuration statements or identifiers.....28
- default gateway, static routing.....271
- defaults
  - setting for static routes .....276
- Delete button .....8
- delete command.....25
- Delete Configuration Below This Point radio button ....12
- Delete link.....11
- deleting
  - current rescue configuration (CLI configuration editor).....32
  - current rescue configuration (J-Web) .....21
  - network interfaces.....126
- designated router, OSPF
  - controlling election .....310
  - description .....248
- destination prefix lengths .....90
- Deutsche Telekom UR-2 operating mode.....138, 141
- diagnosis
  - BERT .....76
  - displaying IS-IS-enabled interfaces .....319
  - displaying IS-IS-enabled interfaces (detail) .....319
  - displaying static routes in the routing table .....277
  - IS-IS adjacencies .....320
  - IS-IS adjacencies (detail).....321
  - IS-IS neighbors.....320
  - IS-IS neighbors (detail).....321
  - PPP magic numbers .....83
  - verifying B-channels.....224
  - verifying BGP configuration.....338
  - verifying BGP groups .....337
  - verifying BGP peer reachability.....339
  - verifying BGP peers (neighbors) .....336
  - verifying D-channels.....225
  - verifying dialer interfaces .....227
  - verifying ISDN call status.....226
  - verifying ISDN interfaces.....223
  - verifying ISDN status .....222
  - verifying OSPF host reachability.....314
  - verifying OSPF neighbors .....312
  - verifying OSPF routes .....313
  - verifying OSPF-enabled interfaces.....311
  - verifying PPPoA for ATM-over-ADSL
    - configuration .....160
  - verifying PPPoE interfaces .....182
  - verifying PPPoE over ATM-over-ADSL
    - configuration .....180–181
  - verifying PPPoE over ATM-over-SHDLS
    - configuration .....180–181
  - verifying PPPoE sessions.....183
  - verifying PPPoE statistics.....184
  - verifying PPPoE version information .....183
  - verifying RIP host reachability .....292
  - verifying RIP message exchange.....291
  - verifying RIP-enabled interfaces .....291
- dial backup
  - configuring (configuration editor).....204
  - configuring (Quick Configuration) .....197
  - interfaces to back up (configuration editor) .....204
  - interfaces to back up (Quick Configuration).....197
  - selecting (Quick Configuration) .....195
- dial-in, ISDN
  - dialer interface (configuration editor).....217
  - encapsulation matching .....216
  - overview .....215
  - rejecting incoming calls (configuration editor) ...220
  - screening incoming calls (configuration editor) ..219
  - voice not supported .....215
- dial-on-demand filter *See* dialer filter, ISDN
- dial-on-demand routing backup, ISDN
  - dialer filter .....205
    - See also* dialer filter, ISDN
  - dialer watch.....207
    - See also* dialer watch
  - OSPF support .....209
    - See also* dialer watch
- dialer filter, ISDN
  - applying to the dialer interface .....206
  - configuring.....205
  - overview .....205
- dialer interface, ISDN
  - adding.....201
  - bandwidth-on-demand (configuration editor)....210
  - callback (configuration editor) .....217
  - dial-in (configuration editor) .....217
  - dialer filter .....205
    - See also* dialer filter, ISDN
  - dialer profiles (configuration editor) .....220

|                                                                                                                 |         |
|-----------------------------------------------------------------------------------------------------------------|---------|
| dialer watch <i>See</i> dialer watch                                                                            |         |
| encapsulation matching for dial-in or callback                                                                  | 216     |
| limitations                                                                                                     | 190     |
| naming convention                                                                                               | 190     |
| Quick Configuration                                                                                             | 194     |
| rejecting incoming calls (configuration editor)                                                                 | 220     |
| restrictions                                                                                                    | 190     |
| screening incoming calls (configuration editor)                                                                 | 219     |
| secondary (backup) connection                                                                                   | 204     |
| verifying                                                                                                       | 227     |
| dialer options, Quick Configuration access                                                                      | 194     |
| dialer pools, ISDN                                                                                              |         |
| for bandwidth on demand (configuration editor)                                                                  | 215     |
| for dialer profiles (configuration editor)                                                                      | 221     |
| for dialer watch (configuration editor)                                                                         | 209     |
| ISDN BRI physical interface (configuration editor)                                                              | 199     |
| Quick Configuration                                                                                             | 193     |
| dialer profiles, ISDN                                                                                           | 220     |
| dialer watch                                                                                                    |         |
| adding a dialer watch interface (configuration editor)                                                          | 207     |
| configuring (Quick Configuration)                                                                               | 197     |
| dialer pool (configuration editor)                                                                              | 209     |
| ISDN interface for (configuration editor)                                                                       | 208     |
| overview                                                                                                        | 207     |
| selecting (Quick Configuration)                                                                                 | 196     |
| watch list (configuration editor)                                                                               | 208     |
| watch list (Quick Configuration)                                                                                | 198     |
| digital subscriber line (DSL) <i>See</i> ATM-over-ADSL interfaces; ATM-over-SHDSDL interfaces; DSLAM connection |         |
| Discard All Changes radio button                                                                                | 12      |
| Discard button                                                                                                  | 12      |
| Discard Changes Below This Point radio button                                                                   | 12      |
| discard eligibility bits <i>See</i> DE bits                                                                     |         |
| discard interface                                                                                               | 95      |
| discarding configuration changes                                                                                | 12      |
| discovery packets, PPPoE                                                                                        | 84, 168 |
| distance-vector routing protocols                                                                               | 243     |
| <i>See also</i> RIP                                                                                             |         |
| dl0                                                                                                             | 190     |
| DLCIs (data-link connection identifiers)                                                                        | 80      |
| documentation set                                                                                               |         |
| comments on                                                                                                     | xxii    |
| domains                                                                                                         |         |
| broadcast domains                                                                                               | 53      |
| collision domains                                                                                               | 52      |
| dotted decimal notation                                                                                         | 88      |
| downloading, configuration files (J-Web)                                                                        | 19      |
| DS1 ports <i>See</i> T1 ports                                                                                   |         |
| DS1 signals                                                                                                     |         |
| E1 and T1                                                                                                       | 55      |
| <i>See also</i> E1 interfaces; T1 interfaces                                                                    |         |
| multiplexing into DS2 signal                                                                                    | 58      |
| DS2 signals                                                                                                     |         |
| bit stuffing                                                                                                    | 59      |
| frame format                                                                                                    | 58      |
| DS3 ports <i>See</i> T3 ports                                                                                   |         |
| DS3 signals                                                                                                     |         |
| DS3 C-bit parity frame format                                                                                   | 61      |
| M13 frame format                                                                                                | 59      |
| dsc interface                                                                                                   | 95      |
| DSL <i>See</i> ATM-over-ADSL interfaces; ATM-over-SHDSDL interfaces; DSLAM connection                           |         |
| DSL access multiplexer (DSLAM) connection                                                                       |         |
| <i>See</i> DSLAM connection                                                                                     |         |
| DSLAM connection                                                                                                |         |
| ATM-over-ADSL interface for                                                                                     | 138     |
| ATM-over-SHDSDL interface for                                                                                   | 149     |
| PPPoE over ATM-over-ADSL topology                                                                               | 167     |
| DSU (data service unit) device                                                                                  | 83      |
| DTE (data terminal equipment)                                                                                   |         |
| default clock rate reduction                                                                                    | 66      |
| serial connection process                                                                                       | 64      |
| serial device                                                                                                   | 63      |
| DTE clocking mode                                                                                               | 65      |
| dying gasp message, SHDSL                                                                                       | 163     |
| dynamic routing                                                                                                 | 240     |
| <b>E</b>                                                                                                        |         |
| E1 interfaces                                                                                                   | 54      |
| AMI encoding                                                                                                    | 55      |
| data stream                                                                                                     | 55      |
| encoding                                                                                                        | 55      |
| framing                                                                                                         | 56      |
| HDB3 encoding                                                                                                   | 56      |
| loopback                                                                                                        | 57      |
| overview                                                                                                        | 55      |
| Quick Configuration                                                                                             | 101     |
| signals                                                                                                         | 55      |
| <i>See also</i> E1 ports                                                                                        |         |
| E1 ports                                                                                                        | 54      |
| adding CRTP                                                                                                     | 124     |
| CHAP                                                                                                            | 103     |
| clocking                                                                                                        | 103     |
| data inversion                                                                                                  | 104     |
| encapsulation type                                                                                              | 103     |
| fractional, channel number                                                                                      | 47      |
| frame checksum                                                                                                  | 104     |
| framing                                                                                                         | 104     |
| logical interfaces                                                                                              | 103     |
| MTU                                                                                                             | 103     |
| overview                                                                                                        | 55      |
| Quick Configuration                                                                                             | 101     |
| time slots                                                                                                      | 104     |
| <i>See also</i> E1 interfaces                                                                                   |         |
| E3 interfaces                                                                                                   | 58      |
| bit stuffing                                                                                                    | 59      |

- data stream .....58
  - DS3 framing .....59
  - multiplexing on .....59
  - overview .....58
  - Quick Configuration .....104
  - See also* E3 ports
  - E3 ports .....58
    - CHAP .....106
    - clocking .....106
    - encapsulation type .....106
    - frame checksum .....108
    - logical interfaces .....106
    - MTU .....106
    - overview .....58
    - Quick Configuration .....104
    - See also* E3 interfaces
  - EBGP (external BGP)
    - description .....257
    - sample network .....330
  - edit command .....23
  - Edit Configuration page .....10
  - Edit Configuration Text page .....14
  - Edit link .....11
  - EGPs (exterior gateway protocols) .....238
  - EIA-232 .....67
  - EIA-422 .....68
  - EIA-449 .....68
  - EIA-530 .....67
  - encapsulation type
    - ATM-over-ADSL logical interfaces .....136, 142
    - ATM-over-ADSL physical interfaces .....137, 141
    - ATM-over-SHDSL logical interfaces .....147, 153
    - ATM-over-SHDSL physical interfaces .....148, 151
    - E1 .....103
    - E3 .....106
    - Frame Relay .....79
    - HDLC .....85
    - ISDN dial-in and callback, monitoring .....216
    - overview .....79
    - PPP .....81
    - PPPoE .....165
    - PPPoE for Ethernet .....173
    - PPPoE, over ATM-over-ADSL .....174
    - PPPoE, over ATM-over-SHDSL .....174
    - PPPoE, overview .....83
    - serial interfaces .....120
    - T1 .....113
    - T3 .....117
  - encoding
    - AMI .....55
    - B8ZS .....56
    - HDB3 .....56
  - error notification, in the data link layer .....48
  - ESF (extended superframe) framing .....57
  - Ethernet interfaces .....50
    - access control .....50
    - broadcast domains .....53
    - collision detection .....51
    - collision domains .....52
    - CSMA/CD .....50
    - frame format .....53
    - IS-IS, NET address .....318
    - overview .....50
    - Quick Configuration .....109
    - See also* Fast Ethernet ports
  - Ethernet over ATM encapsulation .....141
    - ATM-over-ADSL interfaces .....136–137
    - ATM-over-SHDSL interfaces .....148, 151
    - for PPPoE .....175
  - Ethernet over ATM LLC encapsulation
    - ATM-over-ADSL interfaces .....142
    - ATM-over-SHDSL interfaces .....147, 153
  - Ethernet ports *See* Fast Ethernet ports
  - ETSI TS 101 388 V1.3.1 operating mode .....138, 141
  - EU-64 addresses .....49
  - exit command
    - to leave configuration mode .....22
    - to navigate the configuration hierarchy .....23
  - exit configuration-mode command .....22
  - explicit clocking signal transmission .....77
  - extended superframe (ESF) framing .....57
  - exterior gateway protocols .....238
  - external BGP *See* EBGp
- ## F
- failover connection, ISDN .....187
  - Fast Ethernet ports .....50
    - CHAP for PPPoA .....154
    - CHAP for PPPoE .....178
    - logical interfaces .....111
    - MTU .....111
    - overview .....50
    - PPPoE configuration .....175
    - PPPoE encapsulation .....173
    - PPPoE session on .....167
    - Quick Configuration .....109
    - See also* Ethernet interfaces
  - FCS (frame check sequence)
    - checksums .....78
    - CRCs .....78
    - overview .....78
    - two-dimensional parity .....78
  - fe-0/0/0, management interface .....96
  - FEAC C-bit condition indicators .....63
  - FECN (forward-explicit congestion notification) bits .....80
  - file management
    - configuration files (CLI configuration editor) .....33
    - configuration files (J-Web) .....15

|                                                          |          |
|----------------------------------------------------------|----------|
| flow control                                             |          |
| data link layer                                          | 49       |
| font conventions                                         | xix      |
| forward-explicit congestion notification (FECN) bits     | 80       |
| forwarding table                                         |          |
| controlling OSPF routes in                               | 308      |
| controlling static routes in                             | 268, 275 |
| description                                              | 239      |
| MED to determine routes in                               | 260      |
| four-wire mode (1 port), SHDSL <i>See</i> ATM-over-SHDSL |          |
| interfaces                                               |          |
| FPC (PIM slot on a Services Router) <i>See</i> PIMs      |          |
| frame check sequence <i>See</i> FCS                      |          |
| Frame Relay encapsulation                                |          |
| congestion control                                       | 80       |
| DLCIs                                                    | 80       |
| overview                                                 | 79       |
| PVCs                                                     | 80       |
| SVCs                                                     | 80       |
| virtual circuits                                         | 80       |
| Frame Relay network, typical                             | 79       |
| frames                                                   |          |
| DS2 M-frame format                                       | 58       |
| DS3 C-bit parity frame format                            | 61       |
| DS3 M13 frame format                                     | 59       |
| Ethernet frame format                                    | 53       |
| sequencing, data link layer                              | 48       |
| framing                                                  |          |
| E1                                                       | 104      |
| T1                                                       | 114      |
| T3                                                       | 118      |
| FRF.15 and FRF.16                                        | 97       |
| full mesh requirement                                    |          |
| description                                              | 257      |
| fulfilling with confederations                           | 264      |
| fulfilling with route reflectors                         | 261      |
| sample network                                           | 330      |
| fxp0 interface (not supported)                           | 93       |

## G

|                                              |          |
|----------------------------------------------|----------|
| G.992.1 Deutsche Telekom UR-2 operating mode | 138, 141 |
| G.992.1 Non-UR-2 operating mode              | 138, 141 |
| G.SHDSL PIMs                                 | 72       |
| Annex A or Annex B modes                     | 144      |
| configuring                                  | 143      |
| default mode                                 | 150      |
| standard supported                           | 72       |
| <i>See also</i> ATM-over-SHDSL interfaces    |          |
| global unicast IPv6 addresses                | 91       |
| glossary                                     |          |
| configuration                                | 3        |
| DSL                                          | 131      |
| interfaces                                   | 40       |
| ISDN                                         | 187      |

|                           |     |
|---------------------------|-----|
| ports                     | 40  |
| PPPoE                     | 165 |
| routing protocols         | 233 |
| gr-0/0/0 interface        | 93  |
| gre interface             | 93  |
| groups                    |     |
| BGP <i>See</i> BGP groups |     |
| OSPF areas                | 302 |
| RIP routers               | 283 |

## H

|                                              |     |
|----------------------------------------------|-----|
| HDB3 encoding                                | 56  |
| HDLC (High-Level Data Link Control)          |     |
| encapsulation                                | 85  |
| HDLC operational modes                       | 85  |
| HDLC stations                                | 85  |
| hello PDUs                                   | 254 |
| hierarchy, configuration                     | 23  |
| high-density bipolar 3 code (HDB3) encoding  | 56  |
| High-Level Data Link Control <i>See</i> HDLC |     |
| history <i>See</i> configuration history     |     |
| hold time, to maintain a session             | 257 |
| hop count, maximizing                        | 244 |
| <i>See also</i> RIP                          |     |
| host reachability                            |     |
| verifying for an OSPF network                | 314 |
| verifying for RIP network hosts              | 292 |
| hostname                                     |     |
| for PPPoA CHAP                               | 156 |
| for PPPoE CHAP (configuration editor)        | 179 |
| for PPPoE CHAP (Quick Configuration)         | 171 |
| IS-IS identifier-to-hostname mapping         | 316 |

## I

|                                   |     |
|-----------------------------------|-----|
| IBGP (internal BGP)               |     |
| description                       | 257 |
| full mesh (configuration editor)  | 330 |
| full mesh requirement             | 324 |
| sample network                    | 330 |
| sample route reflector            | 332 |
| identifier link                   | 11  |
| identifiers, configuration        |     |
| adding or modifying               | 25  |
| deactivating                      | 28  |
| deleting                          | 25  |
| inserting                         | 27  |
| renaming                          | 26  |
| IGPs (interior gateway protocols) | 238 |
| incoming calls                    |     |
| rejecting                         | 220 |
| screening                         | 219 |
| incoming metric (RIP)             |     |
| description                       | 280 |
| modifying                         | 287 |

- inet protocol family ..... 87
  - MTU value for PPPoE ..... 177
- inet6 protocol family ..... 87
  - MTU value for PPPoE ..... 177
- insert command ..... 27
- inserting configuration identifiers ..... 27
- Integrated Services Digital Network *See* ISDN
- interface naming conventions ..... 45
- interfaces ..... 39
  - ATM-over-ADSL interfaces ..... 69
  - ATM-over-SHDSDL interfaces ..... 72
  - clocking ..... 76
  - data link layer ..... 48
  - E1 interfaces ..... 54
  - E3 interfaces ..... 58
  - Ethernet interfaces ..... 50
  - FCS ..... 78
  - G.SHDSDL interfaces ..... 72
  - IPv4 addressing ..... 87
  - IPv6 addressing ..... 90
  - ISDN interfaces ..... 72
  - logical properties ..... 86
  - overview ..... 39
  - physical encapsulation ..... 79
    - See also* encapsulation type
  - physical properties ..... 75
  - protocol families ..... 86
  - Quick Configuration ..... 100
  - serial interfaces ..... 63
  - special interfaces ..... 93
  - T1 interfaces ..... 54
  - T3 interfaces ..... 58
  - VLANs ..... 92
  - See also* ATM-over-ADSL interfaces;  
ATM-over-SHDSDL interfaces; ISDN interfaces;  
loopback interface; management interfaces;  
network interfaces; services interfaces; special  
interfaces; ports
- Interfaces page ..... 100
  - for E1 ..... 102
  - for E3 ..... 105
  - for Fast Ethernet ..... 110
  - for serial interfaces ..... 119
  - for T1 ..... 112
  - for T3 (DS3) ..... 116
- interior gateway protocols ..... 238
- internal BGP *See* IBGP
- Internet routing, with BGP ..... 323
- invalid configuration, replacing
  - with J-Web ..... 20
  - with the CLI ..... 32
- inverting the transmit clock ..... 121
- IP addresses ..... 87
  - as IS-IS system identifiers ..... 316
  - See also* addresses; IPv4 addressing; IPv6  
addressing
- ip-0/0/0 interface ..... 94
- ip-ip interface ..... 94
- IPv4 addressing
  - assigning for PPPoE (configuration editor) ..... 178
  - assigning for PPPoE (Quick Configuration) ..... 171
  - classful addressing ..... 88
  - dotted decimal notation ..... 88
  - MAC-48 address format ..... 49
  - overview ..... 87
  - subnets ..... 89
  - VLSMs ..... 90
- IPv4 MTU value, PPPoE ..... 177
- IPv6 addressing
  - address format ..... 90
  - address scope ..... 91
  - address structure ..... 91
  - address types ..... 91
  - assigning for PPPoE ..... 178
  - overview ..... 90
- IPv6 MTU value, PPPoE ..... 177
- IPv6 support ..... 233
- IS-IS (Intermediate System-to-Intermediate System)
  - adjacency establishment with hello PDUs ..... 254
  - areas ..... 253
  - ASs ..... 253
  - CSNPs ..... 255
  - enabling on router interfaces ..... 317
  - hello PDUs ..... 254
  - LSPs ..... 254
  - NETs ..... 253
  - NSAP addresses ..... 315
  - overview ..... 252, 315
  - path selection ..... 254
  - preparation ..... 316
  - PSNPs ..... 255
  - system identifiers ..... 254
    - See also* system identifiers
  - verifying adjacencies ..... 320
  - verifying adjacencies (detail) ..... 321
  - verifying interface configuration ..... 319
  - verifying interface configuration (detail) ..... 319
  - verifying neighbors ..... 320
  - verifying neighbors (detail) ..... 321
- ISDN BRI interfaces ..... 72
  - adding an interface ..... 198
  - B-channel interface ..... 190
  - bandwidth-on-demand ..... 210
  - bandwidth-on-demand (configuration editor) ..... 214
  - call setup ..... 74
  - callback *See* callback
  - calling number ..... 193, 200
  - connection initialization ..... 74
  - D-channel interface ..... 190

|                                                    |          |
|----------------------------------------------------|----------|
| dial backup <i>See</i> dial backup                 |          |
| dial-in <i>See</i> dial-in                         |          |
| dial-on-demand routing backup, with OSPF           | 209      |
| dialer interface <i>See</i> dialer interface, ISDN |          |
| dialer profiles (configuration editor)             | 220      |
| dialer watch <i>See</i> dialer watch               |          |
| ISDN channels                                      | 72       |
| naming conventions                                 | 190      |
| NT1 devices                                        | 73       |
| overview                                           | 72       |
| PIMs supported                                     | 189      |
| Q.931 timer                                        | 194, 201 |
| Quick Configuration                                | 191      |
| requirements                                       | 190      |
| S/T interfaces                                     | 73, 189  |
| session establishment                              | 74       |
| SPID                                               | 193, 200 |
| static TEI                                         | 194, 200 |
| switch types                                       | 193, 200 |
| TEI option                                         | 194, 201 |
| typical network                                    | 73       |
| U interface                                        | 74, 189  |
| verifying B-channels                               | 224      |
| verifying call status                              | 226      |
| verifying D-channels                               | 225      |
| verifying dialer interfaces                        | 227      |
| verifying ISDN interfaces                          | 223      |
| verifying ISDN status                              | 222      |
| <i>See also</i> ISDN connections                   |          |
| ISDN connections                                   | 187      |
| adding an interface                                | 198      |
| bandwidth-on-demand                                | 210      |
| callback <i>See</i> callback                       |          |
| calling number                                     | 193, 200 |
| configuring                                        | 187      |
| dial backup <i>See</i> dial backup                 |          |
| dial-in <i>See</i> dial-in                         |          |
| dial-on-demand routing backup, with OSPF           | 209      |
| dialer filter <i>See</i> dialer filter             |          |
| dialer interface <i>See</i> dialer interface, ISDN |          |
| dialer profiles (configuration editor)             | 220      |
| dialer watch <i>See</i> dialer watch               |          |
| interface naming conventions                       | 189      |
| ISDN interface types                               | 189      |
| overview                                           | 189      |
| Q.931 timer                                        | 194, 201 |
| Quick Configuration                                | 191      |
| requirements                                       | 190      |
| SPID                                               | 193, 200 |
| static TEI                                         | 194, 200 |
| switch types                                       | 193, 200 |
| TEI option                                         | 194, 201 |
| verifying B-channels                               | 224      |
| verifying call status                              | 226      |
| verifying D-channels                               | 225      |
| verifying dialer interfaces                        | 227      |
| verifying ISDN interfaces                          | 223      |
| verifying ISDN status                              | 222      |
| <i>See also</i> ISDN BRI interfaces                |          |
| ISDN Dialer Logical Interface page                 | 196      |
| ISDN page                                          | 196      |
| ISDN Physical Interface page                       | 191      |
| ISO network addresses, for IS-IS routers           | 315      |
| ISO protocol family                                | 87       |
| ITU Annex B non-UR-2 operating mode                | 138, 141 |
| ITU Annex B UR-2 operating mode                    | 138, 141 |
| ITU DMT bis operating mode                         | 138, 141 |
| ITU DMT operating mode                             | 138, 141 |
| ITU G.992.1 operating mode                         | 138, 141 |
| ITU G.992.3 operating mode                         | 138      |
| ITU G.992.5 operating mode                         | 138, 141 |

## J

### J-series

|                            |      |
|----------------------------|------|
| BGP routing                | 323  |
| configuration tools        | 3    |
| DSL                        | 131  |
| interfaces overview        | 39   |
| IS-IS protocol             | 315  |
| ISDN connections           | 187  |
| network interfaces         | 99   |
| OSPF routing               | 295  |
| PPPoE                      | 165  |
| release notes, URL         | xvii |
| RIP routing                | 279  |
| routing protocols overview | 233  |
| static routing             | 267  |

### J-Web configuration editor

|                                             |     |
|---------------------------------------------|-----|
| ATM-over-ADSL interfaces                    | 138 |
| ATM-over-SHDSDL interfaces                  | 149 |
| BGP                                         | 327 |
| CHAP on ATM-over-ADSL interfaces            | 154 |
| CHAP on ATM-over-SHDSDL interfaces          | 154 |
| clickable configuration, committing         | 13  |
| clickable configuration, discarding changes | 12  |
| clickable configuration, editing            | 9   |
| committing a text file, with caution        | 13  |
| configuration text, viewing                 | 8   |
| CRTTP                                       | 124 |
| editing a text file, with caution           | 13  |
| IS-IS                                       | 317 |
| ISDN connections                            | 198 |
| managing files                              | 15  |
| network interfaces                          | 122 |
| network interfaces, adding                  | 122 |
| network interfaces, deleting                | 126 |
| OSPF                                        | 299 |
| PPPoE                                       | 172 |
| PPPoE over ATM-over-ADSL                    | 172 |
| PPPoE over ATM-over-SHDSDL                  | 172 |



|                                                     |      |
|-----------------------------------------------------|------|
| RIP                                                 | 283  |
| static routes                                       | 272  |
| uploading a file                                    | 14   |
| J-Web interface                                     | 5    |
| comparing configuration differences                 | 18   |
| configuration history                               | 16   |
| <i>See also</i> configuration history               |      |
| configuration options                               | 5    |
| <i>See also</i> J-Web configuration editor          |      |
| JTAC (Juniper Networks Technical Assistance Center) |      |
| <i>See</i> technical support                        |      |
| Juniper Networks Technical Assistance Center        |      |
| <i>See</i> technical support                        |      |
| JUNOS Internet software                             |      |
| ISDN connections                                    | 187  |
| release notes, URL                                  | xvii |

## K

|                                           |     |
|-------------------------------------------|-----|
| keepalive messages, for session hold time | 257 |
|-------------------------------------------|-----|

## L

|                                                 |     |
|-------------------------------------------------|-----|
| LANs                                            |     |
| bridges on LAN segments                         | 52  |
| collision domains                               | 52  |
| repeaters on LAN segments                       | 52  |
| topology                                        | 92  |
| LCP (Link Control Protocol), connection process | 81  |
| Level 1 areas, IS-IS                            | 253 |
| Level 2 areas, IS-IS                            | 253 |
| line buildout                                   |     |
| T1                                              | 115 |
| T3                                              | 118 |
| line speed                                      |     |
| ATM-over-SHDSDL interfaces                      | 148 |
| serial interfaces                               | 121 |
| line timing                                     | 65  |
| link services                                   | 97  |
| <i>See also</i> ls-0/0/0                        |     |
| link states, verifying                          | 127 |
| link-local unicast IPv6 addresses               | 91  |
| link-state advertisements <i>See</i> LSAs       |     |
| link-state PDUs <i>See</i> LSPs                 |     |
| lo0 interface functions                         | 96  |
| <i>See also</i> loopback interface              |     |
| lo0.16385, internal loopback address            | 94  |
| load command                                    | 34  |
| load merge command                              | 34  |
| load override command                           | 34  |
| load patch command                              | 34  |
| load replace command                            | 34  |
| loading a configuration file                    |     |
| CLI configuration editor                        | 33  |
| downloading (J-Web)                             | 19  |
| rollback (J-Web)                                | 20  |
| rollback command                                | 31  |

|                                                 |     |
|-------------------------------------------------|-----|
| uploading (J-Web)                               | 14  |
| without specifying full hierarchy               | 34  |
| local preference                                |     |
| description                                     | 258 |
| high value preferred                            | 259 |
| role in route selection                         | 258 |
| locked configuration                            | 22  |
| logical interfaces                              |     |
| adding (configuration editor)                   | 124 |
| ATM-over-ADSL (configuration editor)            | 142 |
| ATM-over-ADSL (Quick Configuration)             | 135 |
| ATM-over-SHDSDL                                 | 152 |
| ATM-over-SHDSDL (Quick Configuration)           | 146 |
| E1                                              | 103 |
| E3                                              | 106 |
| Fast Ethernet                                   | 111 |
| serial                                          | 120 |
| T1                                              | 113 |
| T3                                              | 117 |
| logical units                                   |     |
| adding (configuration editor)                   | 124 |
| ATM-over-ADSL interface (Quick Configuration)   | 135 |
| ATM-over-SHDSDL interface (Quick Configuration) | 146 |
| E1 interface                                    | 103 |
| E3 interface                                    | 106 |
| Fast Ethernet interface                         | 111 |
| number in interface name                        | 47  |
| pp0 interface                                   | 175 |
| PPPoE encapsulation                             | 173 |
| PPPoE over ATM-over-ADSL encapsulation          | 174 |
| PPPoE over ATM-over-SHDSDL encapsulation        | 174 |
| serial interface                                | 120 |
| T1 interface                                    | 113 |
| T3 interface                                    | 117 |
| long buildout <i>See</i> line buildout          |     |
| loop clocking mode                              | 65  |
| loopback address                                |     |
| internal, lo0.16385                             | 94  |
| loopback interface                              |     |
| functions                                       | 96  |
| NET on for IS-IS                                | 318 |
| loopback signals, E1 and T1                     | 57  |
| loopback testing, SHDSDL                        | 148 |
| ls-0/0/0                                        |     |
| adding CRTP                                     | 124 |
| interface description                           | 94  |
| LSAs (link-state advertisements)                |     |
| description                                     | 248 |
| three-way handshake                             | 248 |
| lsi interface                                   | 94  |
| LSPs (link-state PDUs)                          |     |
| CSNPs                                           | 255 |
| overview                                        | 254 |
| PSNPs                                           | 255 |

lt-0/0/0 interface .....94

## M

M13 frame format .....59

MAC (media access control) *See* MAC addresses

MAC addresses

- as IS-IS system identifiers ..... 316
- EUI-64 addresses .....49
- MAC-48 address format .....49
- overview .....49
- physical addressing .....48

MAC-48 addresses .....49

magic numbers, PPP .....83

management interfaces

- overview .....96

managing files *See* file management

manuals

- comments on ..... xxii

maximum hop count, RIP .....244

maximum transmission unit *See* MTU

MED (multiple exit discriminator)

- description .....260
- role in route selection .....258

media access control *See* MAC addresses

media types supported .....44

merging a configuration file .....34

- example .....36

metrics *See* path cost metrics

MLFR (Multilink Frame Relay) .....97

MLFR FRF.15 and FRF.16 .....97

mlfr-end-to-end protocol family .....87

mlfr-uni-nni protocol family .....87

MLPPP (Multilink Point-to-Point Protocol) .....97

mlppp protocol family .....87

MPLS protocol family .....87

- MTU value for PPPoE .....177

mt-0/0/0 interface .....94

MTU (maximum transmission unit)

- E1 .....103
- E3 .....106
- Fast Ethernet .....111
- T1 .....113
- T3 .....117, 120

mtun interface .....94

multiarea network, OSPF .....302

multicast IPv6 addresses .....91

Multilink Frame Relay (MLFR) .....97

Multilink Frame Relay Forum .....97

Multilink Point-to-Point Protocol (MLPPP) .....97

multilink services

- CRTP .....97
- MLFR .....97
- MLFR FRF.15 and FRF.16 .....97
- MLPPP .....97

multiple exit discriminator *See* MED

## N

n-selectors, in IS-IS NET addresses .....316

names, of network interfaces .....46

NCPs (Network Control Protocols) .....82

neighbors *See* adjacencies, IS-IS; BGP peers; OSPF neighbors; RIP neighbors

NETs (network entity titles)

- n-selectors .....316
- on an Ethernet interface .....318
- on the loopback interface .....318
- parts .....253
- system identifier .....254

Network Control Protocols (NCPs) .....82

network entity titles *See* NETs

network interfaces

- adding .....122
- ATM-over-ADSL configuration .....138
- ATM-over-ADSL interfaces .....69
- ATM-over-SHDSDL configuration .....149
- ATM-over-SHDSDL interfaces .....72
- clocking .....76
- deleting .....126
- DS3 configuration .....115
- E1 configuration .....101
- E1 interfaces .....54
- E3 configuration .....104
- E3 interfaces .....58
- enabling RIP on .....282
- Ethernet interfaces .....50
- Fast Ethernet configuration .....109
- FCS .....78
- G.SHDSDL interfaces .....72
- IPv4 addressing .....87
- IPv6 addressing .....90
- ISDN interfaces .....72
- logical properties .....86
- media types .....44
- names .....46
- naming conventions .....45
- output, understanding .....47
- physical encapsulation .....79
- See also* encapsulation type
- physical properties .....75
- preparation .....99
- protocol families .....86
- Quick Configuration .....100
- sample name .....47
- serial configuration .....118
- serial interfaces .....63
- supported .....43
- T1 configuration .....111
- T1 interfaces .....54
- T3 configuration .....115
- T3 interfaces .....58
- verifying ATM-over-ADSL properties .....156

- verifying ATM-over-SHDSL configuration ..... 161
- verifying link states ..... 127
- verifying properties ..... 128
- verifying RIP message exchange ..... 291
- verifying RIP on ..... 291
- VLANs ..... 92
- networks
  - description ..... 238
  - designated router *See* designated router, OSPF
  - IPv4 subnets ..... 89
  - path cost metrics *See* path cost metrics
  - PPPoE session on an ATM-over-ADSL loop ..... 168
  - PPPoE session on an Ethernet loop ..... 167
  - sample BGP AS path ..... 260
  - sample BGP confederation ..... 335
  - sample BGP confederations ..... 265
  - sample BGP external and internal links ..... 330
  - sample BGP local preference use ..... 259
  - sample BGP MED use ..... 261
  - sample BGP peer network ..... 328
  - sample BGP peer session ..... 256
  - sample BGP route reflector (one cluster) ... 262, 332
  - sample BGP route reflectors (cluster of clusters) .. 264
  - sample BGP route reflectors (multiple clusters) .. 263
  - sample distance-vector routing ..... 244
  - sample multiarea OSPF routing ..... 250
  - sample OSPF backbone area ..... 251
  - sample OSPF multiarea network ..... 302
  - sample OSPF network with stubs and NSSAs ... 252
  - sample OSPF single-area network ..... 301
  - sample OSPF stub areas and NSSAs ..... 306
  - sample OSPF topology ..... 313
  - sample poison reverse routing ..... 246
  - sample RIP network with incoming metric ..... 286
  - sample RIP network with outgoing metric ..... 288
  - sample RIP topology ..... 283
  - sample route advertisement ..... 241
  - sample route aggregation ..... 242
  - sample routing topology ..... 239
  - sample split horizon routing ..... 245
  - sample static route, preferred path ..... 274
  - sample stub network for static routes ..... 272
  - sample unidirectional routing ..... 247
  - static routing ..... 240
- next hop
  - address for static routes ..... 271
  - defining for static routes ..... 273
  - qualified, defining for static routes ..... 275
  - qualified, for static routes ..... 268
- non-UR-2 operating mode ..... 138, 141
- Normal Response Mode, HDLC ..... 85
- not-so-stubby areas *See* NSSAs
- notice icons ..... xviii
- NRM, HDLC ..... 85
- NSAPs (network service access points)
  - NSAP addresses for IS-IS routers ..... 315
- NSSAs (not-so-stubby areas)
  - area ID (configuration editor) ..... 304
  - area ID (Quick Configuration) ..... 298
  - area type (Quick Configuration) ..... 299
  - creating (configuration editor) ..... 305
  - description ..... 251
  - example ..... 252
  - sample topology ..... 306
- NT1 devices ..... 73
- O**
- OK button
  - J-Web configuration editor ..... 12
  - Quick Configuration ..... 8
- Open Shortest Path First protocol *See* OSPF
- operational mode, entering during configuration ..... 33
- origin, of BGP route ..... 260
- OSPF (Open Shortest Path First)
  - area border routers *See* area border routers
  - area type (Quick Configuration) ..... 299
  - areas ..... 249, 296
    - See also* area border routers; backbone area; NSSAs; stub areas
  - authenticating exchanges (OSPFv2 only) ..... 309
  - backbone area *See* backbone area
  - controlling designated router election ..... 310
  - controlling route cost ..... 308
  - designated router *See* designated router, OSPF
  - designating OSPF interfaces (configuration editor) ..... 302, 304
  - designating OSPF interfaces (Quick Configuration) ..... 299
  - dial-on-demand routing backup support, ISDN .. 209
  - enabling (Quick Configuration) ..... 298
  - enabling, description ..... 295
  - ensuring efficient operation ..... 307
  - ISDN dial-on-demand routing backup support ... 209
  - LSAs ..... 248
  - multiarea network (configuration editor) ..... 302
  - NSSAs *See* NSSAs
  - overview ..... 247, 295
  - path cost metrics *See* path cost metrics
  - Quick Configuration ..... 297
  - requirements ..... 297
  - route preferences ..... 308
  - router ID (configuration editor) ..... 300
  - router ID (Quick Configuration) ..... 298
  - sample multiarea network ..... 302
  - sample network topology ..... 313
  - sample NSSAs ..... 306
  - sample single-area network ..... 301
  - sample stub areas ..... 306
  - single-area network (configuration editor) ..... 300

- stub areas *See* stub areas
    - supported versions ..... 248
    - three-way handshake ..... 248
    - tuning an OSPF network ..... 307
    - verifying host reachability ..... 314
    - verifying neighbors ..... 312
    - verifying RIP-enabled interfaces ..... 311
    - verifying routes ..... 313
  - OSPF interfaces
    - enabling ..... 299
    - enabling (configuration editor) ..... 302, 304
    - enabling, for area border routers ..... 305
    - verifying ..... 311
  - OSPF neighbors, verifying ..... 312
  - OSPF page ..... 297
    - field summary ..... 298
  - outgoing metric (RIP)
    - description ..... 280
    - modifying ..... 289
  - overriding a configuration file ..... 34
    - example ..... 35
- P**
- packet encapsulation *See* encapsulation type
  - packets
    - PPPoE discovery ..... 84, 168
    - RIP, description ..... 245
  - PADI packets ..... 84
  - PADO packets ..... 84
  - PADR packets ..... 84
  - PADS packets ..... 84
  - PADT packets ..... 85
  - parentheses, in syntax descriptions ..... xix
  - partial sequence number PDU (PSNP) ..... 255
  - passive routes, rejection, in static routing ..... 269
  - password
    - for OSPFv2 authentication ..... 310
    - for RIPv2 authentication ..... 289
  - patching a configuration file ..... 34
  - path cost metrics
    - for OSPF routes, description ..... 249, 296
    - for OSPF routes, modifying ..... 308
    - for RIP routes, description ..... 279
    - for RIP routes, modifying ..... 286
  - path selection, IS-IS ..... 254
  - path-vector protocol *See* BGP
  - pd-0/0/0 interface ..... 95
  - PDUs (protocol data units)
    - CSNPs ..... 255
    - hello PDUs ..... 254
    - LSPs ..... 254
    - overview ..... 254
    - PSNPs ..... 255
  - pe-0/0/0 interface ..... 95
  - peering sessions *See* BGP peers; BGP sessions
  - permanent routes, adding ..... 267
  - permanent virtual circuits (PVCs) ..... 80
  - Physical Interface Module *See* PIMs
  - physical interface properties
    - BERT ..... 76
    - encapsulation ..... 79
    - FCS ..... 78
    - interface clocking ..... 76
    - key properties ..... 75
  - PIC (PIM on a Services Router) *See* PIMs
  - pimd interface ..... 95
  - pime interface ..... 95
  - PIMs (Physical Interface Modules)
    - G.SHDSL ..... 144
      - See also* G.SHDSL PIMs
    - output about, understanding ..... 47
    - PIM number, always 0 ..... 46
    - PIM slot number ..... 46
  - Ping Host page, output for BGP ..... 339
  - ping, verifying link states ..... 127
  - plesiochronous networks ..... 77
  - 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 ..... 245
  - polarity, signal ..... 65
  - policy *See* routing policies
  - ports
    - DS1 *See* T1 ports
    - DS3 *See* T3 ports
    - E1 *See* E1 ports
    - E3 *See* E3 ports
    - interfaces overview ..... 39
      - See also* ATM-over-ADSL interfaces;
      - ATM-over-SHDSL interfaces; ISDN
      - interfaces; loopback interface;
      - management interfaces; network
      - interfaces; services interfaces; special
      - interfaces
    - number in interface name ..... 47
    - T1 *See* T1 ports
    - T3 *See* T3 ports
  - pp0
    - creating ..... 175
    - enabling CHAP ..... 178
    - information about ..... 182
    - interface description ..... 95
    - logical Ethernet interface on (configuration editor) ..... 176
    - logical Ethernet interface on (Quick Configuration) ..... 171
  - PPP encapsulation
    - CHAP authentication ..... 82
    - CSU/DSU devices ..... 83
    - LCP connection process ..... 81

- magic numbers ..... 83
- NCPs ..... 82
- overview ..... 81
- PPP over ATM *See* PPPoA
- PPP over ATM-over-ADSL *See* PPPoA
- PPP over ATM-over-SHDSL *See* PPPoA
- PPP over Ethernet *See* PPPoE
- PPPoA (Point-to-Point Protocol over ATM)
  - CHAP ..... 154
  - logical encapsulation ..... 142
  - logical encapsulation (ATM-over-ADSL) ..... 142
  - logical encapsulation (ATM-over-SHDSL) ..... 153
  - physical encapsulation (ATM-over-ADSL) ..... 141
  - physical encapsulation (ATM-over-SHDSL) .. 148, 151
  - verifying ATM-over-ADSL configuration ..... 160
- PPPoE (Point-to-Point Protocol over Ethernet) ..... 167
  - address assignment (configuration editor) ..... 178
  - address assignment (Quick Configuration) ..... 171
  - CHAP (configuration editor) ..... 178
  - CHAP (Quick Configuration) ..... 171
  - CHAP local identity (Quick Configuration) ..... 171
  - CHAP, overview ..... 169
  - client and server ..... 166
  - creating the pp0 interface (configuration editor) ..... 175
  - discovery packets ..... 84, 168
  - encapsulation on an Ethernet interface ..... 83, 173
  - interfaces (Quick Configuration) ..... 169
  - interfaces, overview ..... 167
  - logical interfaces (Quick Configuration) ..... 171
  - MTU values ..... 177
  - overview ..... 166
  - preparation ..... 169
  - sample topology ..... 167
  - service type (configuration editor) ..... 177
  - service type (Quick Configuration) ..... 172
  - session limit (Quick Configuration) ..... 172
  - session overview ..... 84, 168
  - session reconnection time (configuration editor) ..... 176
  - session reconnection time (Quick Configuration) ..... 172
  - underlying interface (Quick Configuration) ..... 172
  - verifying interfaces ..... 182
  - verifying sessions ..... 183
  - verifying statistics ..... 184
  - verifying version information ..... 183
  - See also* PPPoE over ATM-over-ADSL; PPPoE over ATM-over-SHDSL
- PPPoE Active Discovery Initiation (PADI) packets ..... 84
- PPPoE Active Discovery Offer (PADO) packets ..... 84
- PPPoE Active Discovery Request (PADR) packets ..... 84
- PPPoE Active Discovery Session-Confirmation (PADS) packets ..... 84
- PPPoE Active Discovery Termination (PADT) packets .. 85
- PPPoE encapsulation *See* PPPoE
- PPPoE interfaces *See* PPPoE
- PPPoE Interfaces Quick Configuration page ..... 170
- PPPoE over ATM LLC encapsulation
  - ATM-over-ADSL interfaces ..... 136, 142
  - ATM-over-SHDSL interfaces ..... 147, 153
- PPPoE over ATM-over-ADSL ..... 167
  - CHAP ..... 178
  - creating the pp0 interface ..... 175
  - encapsulation ..... 174
  - preparation ..... 169
  - sample topology ..... 167
  - verifying configuration ..... 180–181
  - See also* PPPoE
- PPPoE over ATM-over-SHDSL ..... 167
  - CHAP ..... 178
  - creating the pp0 interface ..... 175
  - encapsulation ..... 174
  - preparation ..... 169
  - verifying configuration ..... 180–181
  - See also* PPPoE
- PPPoEoA *See* PPPoE over ATM-over-ADSL; PPPoE over ATM-over-SHDSL
- preferences
  - for OSPF routes ..... 308
  - for static routes ..... 268
  - setting for static routes ..... 275
- primary stations, HDLC ..... 85
- properties, verifying
  - for ATM-over-ADSL network interfaces ..... 156
  - for ATM-over-SHDSL network interfaces ..... 161
  - for network interfaces ..... 128
- protocol data units *See* PDUs
- protocol families
  - ccc ..... 87
  - common protocol suites ..... 87
  - inet ..... 87
  - inet6 ..... 87
  - ISO ..... 87
  - mlfr-end-to-end ..... 87
  - mlfr-uni-nni ..... 87
  - mlppp ..... 87
  - MPLS ..... 87
  - overview ..... 86
  - tcc ..... 87
  - tnp ..... 87
  - vpls ..... 87
- protocols
  - BGP *See* BGP
  - CRTP ..... 124
  - distance vector *See* RIP
  - EGPs ..... 238
  - EIA-530 ..... 67
  - IGPs ..... 238
  - IS-IS *See* IS-IS

|                                          |     |
|------------------------------------------|-----|
| OSPF <i>See</i> OSPF                     |     |
| overview .....                           | 233 |
| path vector <i>See</i> BGP               |     |
| PPPoE <i>See</i> PPPoE                   |     |
| RIP <i>See</i> RIP                       |     |
| RS-232 .....                             | 67  |
| RS-422/449 .....                         | 68  |
| serial .....                             | 66  |
| V.35 .....                               | 68  |
| X.21 .....                               | 69  |
| PSNP (partial sequence number PDU) ..... | 255 |
| PVCs (permanent virtual circuits) .....  | 80  |

## Q

|                                          |          |
|------------------------------------------|----------|
| Q.931 timer, ISDN .....                  | 194, 201 |
| Quick Configuration                      |          |
| ATM-over-ADSL Interfaces page .....      | 133      |
| ATM-over-SHDSL Interfaces page .....     | 144      |
| BGP page .....                           | 325      |
| buttons .....                            | 8        |
| E1 Interfaces page .....                 | 102      |
| E3 Interfaces page .....                 | 105      |
| Fast Ethernet Interfaces page .....      | 110      |
| Interfaces page .....                    | 100      |
| ISDN Dialer Logical Interface page ..... | 196      |
| ISDN Physical Interface page .....       | 191      |
| network interfaces .....                 | 100      |
| OSPF page .....                          | 297      |
| overview .....                           | 7        |
| PPPoE Interfaces page .....              | 170      |
| RIP page .....                           | 281      |
| serial Interfaces page .....             | 119      |
| Static Routes page .....                 | 270      |
| Summary page .....                       | 7        |
| T1 Interfaces page .....                 | 112      |
| T3 (DS3) Interfaces page .....           | 116      |

## R

|                                                     |      |
|-----------------------------------------------------|------|
| radio buttons                                       |      |
| Delete Configuration Below This Point .....         | 12   |
| Discard All Changes .....                           | 12   |
| Discard Changes Below This Point .....              | 12   |
| RADIUS authentication, of PPP sessions .....        | 169  |
| reachability                                        |      |
| verifying for a RIP network .....                   | 292  |
| verifying for BGP peers .....                       | 339  |
| verifying for OSPF network hosts .....              | 314  |
| reactivate command .....                            | 28   |
| Refresh button .....                                | 12   |
| rejecting incoming calls, ISDN .....                | 220  |
| relative option .....                               | 34   |
| release notes, URL .....                            | xvii |
| Remote Authentication Dial-In User Service (RADIUS) |      |
| authentication, of PPP sessions .....               | 169  |
| rename command .....                                | 26   |

|                                                           |          |
|-----------------------------------------------------------|----------|
| renaming configuration identifiers .....                  | 26       |
| repeaters, on LAN segments .....                          | 52       |
| replacing a configuration file .....                      | 34       |
| example .....                                             | 35       |
| request system configuration rescue delete                |          |
| command .....                                             | 32       |
| request system configuration rescue save command .....    | 32       |
| rescue configuration                                      |          |
| deleting (CLI configuration editor) .....                 | 32       |
| deleting (J-Web) .....                                    | 20–21    |
| disabling CONFIG button for .....                         | 32       |
| loading with the CONFIG button .....                      | 20, 32   |
| setting (CLI configuration editor) .....                  | 32       |
| setting (J-Web) .....                                     | 20       |
| viewing (CLI configuration editor) .....                  | 32       |
| viewing (J-Web) .....                                     | 20–21    |
| reset button, for return to factory configuration         |          |
| <i>See</i> CONFIG button                                  |          |
| RIP (Routing Information Protocol)                        |          |
| authentication (RIPv2 only) .....                         | 280      |
| authentication (RIPv2 only), configuring .....            | 289      |
| basic network (configuration editor) .....                | 283      |
| designating RIP interfaces .....                          | 282      |
| distance vector protocol .....                            | 243      |
| efficiency techniques .....                               | 245      |
| enabling (Quick Configuration) .....                      | 282      |
| maximum hop count .....                                   | 244      |
| overview .....                                            | 243, 279 |
| packets .....                                             | 245      |
| path cost metrics <i>See</i> path cost metrics            |          |
| poison reverse technique .....                            | 245      |
| Quick Configuration .....                                 | 280      |
| requirements .....                                        | 280      |
| routing policy (configuration editor) .....               | 283      |
| sample network with incoming metric .....                 | 286      |
| sample network with outgoing metric .....                 | 288      |
| sample topology .....                                     | 283      |
| split horizon technique .....                             | 245      |
| supported versions .....                                  | 243      |
| traffic control with metrics <i>See</i> path cost metrics |          |
| traffic control with metrics, configuring .....           | 286      |
| unidirectional limitations .....                          | 246      |
| verifying host reachability .....                         | 292      |
| verifying RIP message exchange .....                      | 291      |
| verifying RIP-enabled interfaces .....                    | 291      |
| RIP neighbors, verifying .....                            | 291      |
| RIP page .....                                            | 281      |
| field summary .....                                       | 282      |
| rollback ? command .....                                  | 32       |
| rollback command .....                                    | 31       |
| rollback rescue command .....                             | 31       |
| rolling back a configuration file                         |          |
| during configuration (CLI configuration editor) .....     | 31       |
| during configuration (J-Web) .....                        | 20       |

route advertisements  
     AS path in ..... 259  
     BGP, update messages..... 257  
     description ..... 241  
     external, EBGp ..... 257  
     internal, IBGP ..... 257  
     LSAs ..... 248  
     stub areas and NSSAs, to control ..... 251  
 route aggregation ..... 241  
 route reflectors *See* BGP route reflectors  
 route selection  
     BGP process..... 258  
     BGP, determining by AS path ..... 259  
     BGP, determining by local preference ..... 258  
     BGP, determining by MED metric..... 260  
     BGP, lowest origin value preferred ..... 260  
     static routes, defining ..... 273  
 router *See* Services Router  
 routing..... 233  
     advertisements ..... 241  
     aggregation ..... 241  
     BGP *See* BGP  
     configuring PPPoE..... 165  
     dynamic..... 240  
     forwarding tables ..... 239  
     in multiple ASs with BGP..... 323  
     in one AS with OSPF ..... 295  
     in one AS with RIP..... 279  
     IS-IS *See* IS-IS  
     neighbors *See* BGP peers; OSPF neighbors; RIP  
         neighbors  
     OSPF *See* OSPF  
     protocol overview..... 233  
     RIP *See* RIP  
     RIP statistics ..... 291  
     routing tables ..... 239  
     static *See* static routing  
     *See also* protocols; routing policies; routing  
         solutions  
 Routing Information Protocol *See* RIP  
 routing policies  
     BGP routing policy (configuration editor)..... 331  
     RIP routing policy (configuration editor) ..... 283  
 routing protocols *See* protocols  
 routing solutions  
     BGP confederations, for scaling problems..... 334  
     BGP route reflectors, for scaling problems ..... 331  
     BGP scaling techniques..... 261  
     controlling designated router election ..... 310  
     controlling OSPF route cost ..... 308  
     controlling OSPF route selection ..... 308  
     controlling RIP traffic with the incoming metric.. 286  
     controlling RIP traffic with the outgoing metric.. 287  
     designated router, to reduce flooding..... 248  
     directing BGP traffic by local preference ..... 258

NSSAs, to control route advertisement ..... 251  
 path cost metrics, for packet flow control *See* path  
     cost metrics  
 point-to-point sessions over Ethernet..... 165  
 poison reverse, for traffic reduction ..... 245  
 securing OSPF routing (OSPFv2 only) ..... 309  
 split horizon, for traffic reduction..... 245  
 static route control techniques ..... 268  
 stub areas, to control route advertisement ..... 251  
 routing table  
     controlling static routes in..... 268, 275  
     description ..... 239  
     displaying static routes in ..... 277  
     sample distance-vector routing ..... 244  
     updates, limitations in RIP ..... 246  
     verifying OSPF routes ..... 313  
 RS-232..... 67  
 RS-422/449..... 68  
 RS-530..... 67  
 run command..... 33

## S

S/T interface  
     overview ..... 73  
     PIMs ..... 189  
 samples ..... 160, 180–181  
     PPPoA for ATM-over-ADSL configuration ..... 160  
     PPPoE over ATM-over-ADSL configuration ..... 181  
     PPPoE over ATM-over-SHDSL configuration ..... 181  
     PPPoE over Ethernet configuration ..... 180  
     *See also* networks; topology  
 saving, configuration files ..... 36  
 scaling BGP *See* BGP confederations; BGP route  
     reflectors  
 scheduling a commit ..... 30  
 scope, IPv6 addresses  
     global unicast ..... 91  
     link-local unicast..... 91  
     multicast types..... 91  
     site-local unicast ..... 91  
 screening incoming calls, ISDN ..... 219  
 secondary stations, HDLC ..... 85  
 secret, CHAP *See* CHAP, local identity  
 security  
     MD5 authentication for OSPF..... 310  
     MD5 authentication for RIPv2 ..... 290  
     password authentication for OSPFv2 ..... 310  
     password authentication for RIPv2 ..... 289  
 self-near-end crosstalk *See* SNEXT  
 serial interfaces ..... 63  
     clocking modes ..... 65  
     connection process ..... 64  
     DTE default clock rate reduction ..... 66  
     EIA-530..... 67  
     inverting the transmit clock..... 66

|                                                       |         |                                                  |              |
|-------------------------------------------------------|---------|--------------------------------------------------|--------------|
| line protocols .....                                  | 66      | SHDSL page .....                                 | 145          |
| Quick Configuration .....                             | 118     | SHDSL ports <i>See</i> ATM-over-SHDSL interfaces |              |
| RS-232 .....                                          | 67      | shortest path first algorithm .....              | 247          |
| RS-422/449 .....                                      | 68      | show access command .....                        | 160          |
| signal polarity .....                                 | 65      | show bgp group command .....                     | 337          |
| transmission signals .....                            | 64      | explanation .....                                | 338          |
| V.35 .....                                            | 68      | show bgp neighbor command .....                  | 336          |
| X.21 .....                                            | 69      | explanation .....                                | 337          |
| <i>See also</i> serial ports                          |         | show bgp summary command .....                   | 338          |
| serial numbers, in MAC addresses .....                | 49      | explanation .....                                | 338          |
| serial ports .....                                    | 63      | show chassis hardware command .....              | 47           |
| CHAP .....                                            | 120     | show cli history command .....                   | 33           |
| clock rate .....                                      | 121     | show command .....                               | 24           |
| clocking .....                                        | 121     | show interfaces bc-0/0/4 extensive command ..... | 224          |
| clocking, inverting the transmit clock .....          | 121     | show interfaces br-6/0/0 extensive command ..... | 223          |
| encapsulation type .....                              | 120     | show interfaces command .....                    | 160, 180–181 |
| line speed .....                                      | 121     | show interfaces dc-0/0/4 extensive command ..... | 225          |
| logical interfaces .....                              | 120     | show interfaces detail command .....             | 128          |
| Quick Configuration .....                             | 118     | show interfaces dl0 extensive command .....      | 227          |
| <i>See also</i> serial interfaces                     |         | show interfaces extensive command .....          | 156          |
| service provider ID <i>See</i> SPID                   |         | explanation, for ATM-over-ADSL interfaces .....  | 159          |
| service types, naming for PPPoE .....                 | 177     | explanation, for ATM-over-SHDSL                  |              |
| services interfaces                                   |         | interfaces .....                                 | 161–162      |
| CRTP .....                                            | 97      | explanation, for ISDN interfaces .....           | 223, 225–226 |
| MLFR .....                                            | 97      | show interfaces ppo command .....                | 182          |
| MLFR FRF.15 and FRF.16 .....                          | 97      | show isdn calls command .....                    | 226          |
| MLPPP .....                                           | 97      | show isdn status command .....                   | 222          |
| overview .....                                        | 97      | show isis adjacency brief command .....          | 320          |
| Services Router                                       |         | show isis adjacency extensive command .....      | 321          |
| as a PPPoE client .....                               | 166     | explanation .....                                | 321          |
| BGP routing .....                                     | 323     | show isis interface brief command .....          | 319          |
| configuration tools .....                             | 3       | show isis interface detail command .....         | 319          |
| CPE, with PPPoE .....                                 | 165     | explanation .....                                | 319          |
| <i>See also</i> PPPoE                                 |         | show ospf interface command .....                | 311          |
| DSL .....                                             | 131     | explanation .....                                | 311          |
| interfaces overview .....                             | 39      | show ospf neighbor command .....                 | 312          |
| IS-IS protocol .....                                  | 315     | explanation .....                                | 312          |
| ISDN connections .....                                | 187     | show ospf route command .....                    | 313          |
| network interfaces .....                              | 99      | explanation .....                                | 314          |
| OSPF routing .....                                    | 295     | show pppoe interfaces command .....              | 183          |
| PPPoE .....                                           | 165     | show pppoe statistics command .....              | 184          |
| RIP routing .....                                     | 279     | show pppoe version command .....                 | 184          |
| routing protocols overview .....                      | 233     | show rip neighbor command .....                  | 291          |
| static routing .....                                  | 267     | explanation .....                                | 291          |
| sessions                                              |         | show rip statistics command .....                | 291          |
| BGP session establishment .....                       | 256     | show route terse command .....                   | 277          |
| BGP session maintenance .....                         | 257     | explanation .....                                | 278          |
| ISDN session establishment .....                      | 74      | show system reboot command .....                 | 33           |
| limit on PPPoE sessions .....                         | 168     | signal-to-noise ratio <i>See</i> SNR             |              |
| PPPoE .....                                           | 84, 168 | signals                                          |              |
| PPPoE, reconnection time (configuration               |         | DS1 .....                                        | 55           |
| editor) .....                                         | 176     | E1 loopback (control) .....                      | 57           |
| PPPoE, reconnection time (Quick                       |         | explicit clocking signal transmission .....      | 77           |
| Configuration) .....                                  | 172     | multiplexing DS1 into DS2 signal .....           | 58           |
| SHDSL interfaces <i>See</i> ATM-over-SHDSL interfaces |         | serial polarity .....                            | 65           |



- serial transmission ..... 64
- T1 loopback (control) ..... 57
- V.35 ..... 68
- X.21 ..... 69
- single-area network, OSPF ..... 300
- site-local unicast IPv6 addresses ..... 91
- SNEXT (self-near-end crosstalk) threshold,
  - SHDSL ..... 149, 152
- SNR (signal-to-noise ratio) margin, SHDSL ..... 149, 152
- sp-0/0/0 interface ..... 95
- special interfaces
  - CRTP ..... 97
  - dsc interface ..... 95
  - IPv4 addressing ..... 87
  - IPv6 addressing ..... 90
  - logical properties ..... 86
  - loopback interface ..... 96
  - management interface ..... 96
  - MLFR ..... 97
  - MLFR FRF.15 and FRF.16 ..... 97
  - MLPPP ..... 97
  - names ..... 46
  - naming conventions ..... 45
  - output, understanding ..... 47
  - overview ..... 93
  - physical properties ..... 75
  - protocol families ..... 86
  - services interfaces ..... 97
  - summary ..... 93
- SPF (shortest path first) algorithm ..... 247
- SPID (service provider ID), ISDN ..... 193, 200
- split horizon technique ..... 245
- statements
  - adding or modifying ..... 25
  - copying ..... 26
  - deactivating ..... 28
  - deleting ..... 25
  - replacing ..... 34
- static routes
  - configuring basic routes (configuration editor) ..... 272
  - controlling ..... 268
  - controlling in routing and forwarding tables ..... 275
  - default properties ..... 269
  - default properties, setting ..... 276
  - defining route selection ..... 273
  - preferences ..... 268
  - preventing readvertisement ..... 269
  - qualified next hops ..... 268
  - Quick Configuration ..... 270
  - rejecting passive traffic ..... 269
  - requirements ..... 270
  - route retention ..... 269
  - sample preferred path ..... 274
  - sample stub network ..... 272
  - verifying ..... 277
- Static Routes page ..... 270
  - field summary ..... 271
- static routing
  - default gateway ..... 271
  - description ..... 240
  - overview ..... 267
    - See also* static routes
- static TEI (terminal endpoint identifier), ISDN .. 194, 200
- statistics
  - ATM-over-ADSL interfaces ..... 160
  - ATM-over-SHDSL interfaces ..... 163
  - ISDN B-channel interfaces ..... 224
  - ISDN D-channel interfaces ..... 225
  - PPPoE ..... 184
  - RIP ..... 291
- status
  - ATM-over-SHDSL interfaces, verifying ..... 163
  - ISDN calls, verifying ..... 226
  - ISDN interfaces, verifying ..... 222
  - link states, verifying ..... 127
- status command ..... 21
- stub areas
  - area ID (configuration editor) ..... 304
  - area ID (Quick Configuration) ..... 298
  - area type (Quick Configuration) ..... 299
  - controlling OSPF route cost ..... 309
  - creating (configuration editor) ..... 305
  - description ..... 251
  - example ..... 252
  - sample topology ..... 306
- sub-ASs, BGP ..... 264
- subautonomous systems, BGP ..... 264
- subnet masks ..... 90
- subnets *See* subnetworks
- subnetworks
  - description ..... 238
  - IPv4 subnets ..... 89
  - route aggregation ..... 242
- Summary Quick Configuration page ..... 7
- superframe framing ..... 56
- support, technical *See* technical support
- SVCs (switched virtual circuits) ..... 80
- switch types, ISDN ..... 193, 200
- switched virtual circuits (SVCs) ..... 80
- switches, on LAN segments ..... 52
- symmetric high-speed digital subscriber line (SHDSL)
  - See* ATM-over-SHDSL interfaces
- synchronous networks ..... 76
- syntax conventions ..... xix
- system clock *See* clocking
- system identifier, IS-IS
  - all zeros not supported ..... 316
  - formats, MAC or IP address ..... 316
  - identifier-to-hostname mapping ..... 316
  - overview ..... 254

**T**

|                                  |          |                                                                |          |
|----------------------------------|----------|----------------------------------------------------------------|----------|
| T1 interfaces .....              | 54       | technical support .....                                        |          |
| AMI encoding .....               | 55       | contacting JTAC .....                                          | xxii     |
| B8ZS encoding .....              | 56       | TEI option, ISDN .....                                         | 194, 201 |
| D4 framing .....                 | 56       | telephone calls .....                                          |          |
| data stream .....                | 54       | rejecting incoming ISDN .....                                  | 220      |
| encoding .....                   | 55       | screening incoming ISDN .....                                  | 219      |
| ESF framing .....                | 57       | verifying status .....                                         | 226      |
| framing .....                    | 56       | terminal endpoint identifier <i>See</i> static TEI; TEI option |          |
| loopback .....                   | 57       | terminology .....                                              |          |
| overview .....                   | 54       | configuration .....                                            | 3        |
| Quick Configuration .....        | 111      | DSL .....                                                      | 131      |
| signals .....                    | 55       | interfaces .....                                               | 40       |
| superframe framing .....         | 56       | ISDN .....                                                     | 187      |
| <i>See also</i> T1 ports         |          | ports .....                                                    | 40       |
| T1 ports .....                   | 54       | PPPoE .....                                                    | 165      |
| adding CRTP .....                | 124      | routing protocols .....                                        | 233      |
| cable length .....               | 115      | three-way handshake .....                                      | 248      |
| CHAP .....                       | 113      | time slots .....                                               |          |
| clocking .....                   | 113      | E1 .....                                                       | 104      |
| data inversion .....             | 114      | number in interface name .....                                 | 47       |
| encapsulation type .....         | 113      | T1 .....                                                       | 114      |
| fractional, channel number ..... | 47       | tnp protocol family .....                                      | 87       |
| frame checksum .....             | 115      | top command .....                                              | 24       |
| framing .....                    | 114      | topology .....                                                 |          |
| logical interfaces .....         | 113      | data link layer .....                                          | 48       |
| MTU .....                        | 113      | IPv4 subnets .....                                             | 89       |
| overview .....                   | 54       | PPPoE session on an ATM-over-ADSL loop .....                   | 168      |
| Quick Configuration .....        | 111      | PPPoE session on an Ethernet loop .....                        | 167      |
| time slots .....                 | 114      | sample ATM-over-ADSL .....                                     | 71       |
| <i>See also</i> T1 interfaces    |          | sample BGP AS path .....                                       | 260      |
| T3 interfaces .....              | 58       | sample BGP confederation .....                                 | 335      |
| bit stuffing .....               | 59       | sample BGP confederations .....                                | 265      |
| data stream .....                | 58       | sample BGP external and internal links .....                   | 330      |
| DS3 framing .....                | 59       | sample BGP local preference use .....                          | 259      |
| multiplexing on .....            | 59       | sample BGP MED use .....                                       | 261      |
| overview .....                   | 58       | sample BGP peer network .....                                  | 328      |
| Quick Configuration .....        | 115      | sample BGP peer session .....                                  | 256      |
| <i>See also</i> T3 ports         |          | sample BGP route reflector (one cluster) ..                    | 262, 332 |
| T3 ports .....                   | 58       | sample BGP route reflectors (cluster of clusters) ..           | 264      |
| C-bit parity .....               | 118      | sample BGP route reflectors (multiple clusters) ..             | 263      |
| cable length .....               | 118      | sample distance-vector routing .....                           | 244      |
| CHAP .....                       | 117      | sample Frame Relay network .....                               | 79       |
| clocking .....                   | 117      | sample ISDN network .....                                      | 73       |
| encapsulation type .....         | 117      | sample LAN .....                                               | 92       |
| frame checksum .....             | 118      | sample multiarea OSPF routing .....                            | 250      |
| framing .....                    | 118      | sample OSPF backbone area .....                                | 251      |
| logical interfaces .....         | 117      | sample OSPF multiarea network .....                            | 302      |
| MTU .....                        | 117, 120 | sample OSPF network .....                                      | 313      |
| overview .....                   | 58       | sample OSPF network with stubs and NSSAs ..                    | 252      |
| Quick Configuration .....        | 115      | sample OSPF single-area network .....                          | 301      |
| <i>See also</i> T3 interfaces    |          | sample OSPF stub areas and NSSAs .....                         | 306      |
| tap interface .....              | 95       | sample poison reverse routing .....                            | 246      |
| tcc protocol family .....        | 87       | sample RIP network .....                                       | 283      |
|                                  |          | sample RIP network with incoming metric .....                  | 286      |
|                                  |          | sample RIP network with outgoing metric .....                  | 288      |

|                                                          |     |
|----------------------------------------------------------|-----|
| sample route advertisement                               | 241 |
| sample route aggregation                                 | 242 |
| sample router network                                    | 239 |
| sample split horizon routing                             | 245 |
| sample static route                                      | 240 |
| sample static route, preferred path                      | 274 |
| sample stub network for static routes                    | 272 |
| sample unidirectional routing                            | 247 |
| sample VLAN                                              | 93  |
| topology database, OSPF                                  | 295 |
| Traceroute page                                          |     |
| results for OSPF                                         | 314 |
| results for RIP                                          | 293 |
| traffic                                                  |     |
| controlling with incoming RIP metric                     | 286 |
| controlling with outgoing RIP metric                     | 287 |
| transmit clock source <i>See</i> clocking                |     |
| two-dimensional parity                                   | 78  |
| two-wire mode (2 ports), SHDSL <i>See</i> ATM-over-SHDSL |     |
| interfaces                                               |     |
| types of interfaces                                      | 46  |

## U

|                                |          |
|--------------------------------|----------|
| U interface                    |          |
| overview                       | 74       |
| PIMs                           | 189      |
| unicast IPv6 addresses         | 91       |
| up command                     | 23       |
| uploading a configuration file | 14       |
| UR-2 operating mode            | 138, 141 |
| URLs                           |          |
| release notes                  | xvii     |

## V

|                                        |          |
|----------------------------------------|----------|
| V.35                                   | 68       |
| variable-length subnet masks (VLSMs)   | 90       |
| VCI (virtual channel identifier)       |          |
| ATM-over-ADSL interfaces               | 136, 143 |
| ATM-over-SHDSL interfaces              | 147, 154 |
| PPPoE over ATM-over-ADSL interfaces    | 175      |
| PPPoE over ATM-over-SHDSL interfaces   | 175      |
| verification                           |          |
| ATM-over-ADSL interface properties     | 156      |
| ATM-over-SHDSL interface configuration | 161      |
| B-channels                             | 224      |
| BGP configuration                      | 338      |
| BGP groups                             | 337      |
| BGP peer reachability                  | 339      |
| BGP peers (neighbors)                  | 336      |
| configuration syntax                   | 29       |
| D-channels                             | 225      |
| dialer interfaces                      | 227      |
| IS-IS adjacencies                      | 320      |
| IS-IS adjacencies (detail)             | 321      |
| IS-IS interface configuration          | 319      |

|                                                   |          |
|---------------------------------------------------|----------|
| IS-IS interface configuration (detail)            | 319      |
| IS-IS neighbors                                   | 320      |
| IS-IS neighbors (detail)                          | 321      |
| ISDN call status                                  | 226      |
| ISDN interfaces                                   | 223      |
| ISDN status                                       | 222      |
| network interfaces                                | 127      |
| OSPF host reachability                            | 314      |
| OSPF neighbors                                    | 312      |
| OSPF routes                                       | 313      |
| OSPF-enabled interfaces                           | 311      |
| PPPoA for ATM-over-ADSL configuration             | 160      |
| PPPoE interfaces                                  | 182      |
| PPPoE over ATM-over-ADSL configuration            | 180–181  |
| PPPoE over ATM-over-SHDSL                         |          |
| configuration                                     | 180–181  |
| PPPoE sessions                                    | 183      |
| PPPoE statistics                                  | 184      |
| PPPoE version                                     | 183      |
| RIP host reachability                             | 292      |
| RIP message exchange                              | 291      |
| RIP-enabled interfaces                            | 291      |
| static routes in the routing table                | 277      |
| version                                           |          |
| OSPF, supported                                   | 248      |
| PPPoE, verifying                                  | 183      |
| RIP, supported                                    | 243      |
| View Configuration Text page                      | 9        |
| virtual channel identifier <i>See</i> VCI         |          |
| virtual circuits                                  |          |
| DLCIs                                             | 80       |
| overview                                          | 80       |
| PVCs                                              | 80       |
| SVCs                                              | 80       |
| virtual LANs <i>See</i> VLANs                     |          |
| virtual link, through the backbone area           | 250      |
| virtual path identifier <i>See</i> VPI            |          |
| VLANs (virtual LANs)                              |          |
| LAN comparison                                    | 93       |
| overview                                          | 92       |
| topology                                          | 93       |
| VLSMs (variable-length subnet masks)              | 90       |
| voice calls, not supported in dial-in or callback | 215      |
| VPI (virtual path identifier)                     |          |
| ATM-over-ADSL interfaces                          | 137, 140 |
| ATM-over-SHDSL interfaces                         | 148, 151 |
| PPPoE over ATM-over-ADSL interfaces               |          |
| (configuration editor)                            | 174      |
| PPPoE over ATM-over-SHDSL interfaces              |          |
| (configuration editor)                            | 174      |
| vpls protocol family                              | 87       |

## W

|                             |          |
|-----------------------------|----------|
| watch list, for ISDN backup | 198, 208 |
|-----------------------------|----------|

**X**  
X.21 .....69