



JUNOS® Software

Glossary

Release 9.3

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, California 94089
USA

408-745-2000

www.juniper.net

Part Number: 530-027188-01, Revision 1

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

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

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

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

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

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, ScreenOS, and Steel-Belted Radius are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

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

JUNOS® Software Glossary

Release 9.3

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Writing: Michael Scruggs, Merisha Wazna

Editing: Sonia Saruba, Nancy Kurahashi

Illustration: Faith Bradford

Cover Design: Edmonds Design

Revision History

10 October 2008—Revision 1

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux 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)).

Table of Contents

	About This Guide	xi
	Objectives	xi
	Audience	xi
	Supported Routing Platforms	xi
	Documentation Conventions	xi
	List of Technical Publications	xiii
	Documentation Feedback	xx
	Requesting Technical Support	xxi
Part 1	Glossary	
Chapter 1	Glossary	3

List of Tables

Table 1: Notice Icons	xii
Table 2: Text and Syntax Conventions	xii
Table 3: Technical Documentation for Supported Routing Platforms	xiii
Table 4: JUNOS Software Network Operations Guides	xviii
Table 5: JUNOS Software with Enhanced Services Documentation	xix
Table 6: Additional Books Available Through http://www.juniper.net/books	xx

About This Guide

This preface provides the following guidelines for using the *JUNOS® Software Glossary*:

- Objectives on page xi
- Audience on page xi
- Supported Routing Platforms on page xi
- Documentation Conventions on page xi
- List of Technical Publications on page xiii
- Documentation Feedback on page xx
- Requesting Technical Support on page xxi

Objectives

To define terms and acronyms used in networking.

Audience

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

Supported Routing Platforms

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

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

Documentation Conventions

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

Table 1: Notice Icons





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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the <code>configure</code> command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces important new terms. Identifies book names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>JUNOS System Basics Configuration Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Plain text like this	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"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric <i>metric</i> >;

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

Convention	Description	Examples
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (string1 string2 string3)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation 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.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none">■ In the Logical Interfaces box, select All Interfaces.■ To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select Protocols > Ospf .

List of Technical Publications

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

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

Table 3: Technical Documentation for Supported Routing Platforms

Book	Description
JUNOS Software for Supported Routing Platforms	

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

Book	Description
<i>Access Privilege</i>	Explains how to configure access privileges in user classes by using permission flags and regular expressions. Lists the permission flags along with their associated command-line interface (CLI) operational mode commands and configuration statements.
<i>Class of Service</i>	Provides an overview of the class-of-service (CoS) functions of the JUNOS software and describes how to configure CoS features, including configuring multiple forwarding classes for transmitting packets, defining which packets are placed into each output queue, scheduling the transmission service level for each queue, and managing congestion through the random early detection (RED) algorithm.
<i>CLI User Guide</i>	Describes how to use the JUNOS command-line interface (CLI) to configure, monitor, and manage Juniper Networks routing platforms. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>Feature Guide</i>	Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS software.
<i>High Availability</i>	Provides an overview of hardware and software resources that ensure a high level of continuous routing platform operation and describes how to configure high availability (HA) features such as nonstop active routing (NSR) and graceful Routing Engine switchover (GRES).
<i>MPLS Applications</i>	Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols.
<i>Multicast Protocols</i>	Provides an overview of multicast concepts and describes how to configure multicast routing protocols.
<i>Multiplay Solutions</i>	Describes how you can deploy IPTV and voice over IP (VoIP) services in your network.
<i>MX-series Layer 2 Configuration Guide</i>	Provides an overview of the Layer 2 functions of the MX-series routers, including configuring bridging domains, MAC address and VLAN learning and forwarding, and spanning-tree protocols. It also details the routing instance types used by Layer 2 applications. All of this material was formerly covered in the <i>JUNOS Routing Protocols Configuration Guide</i> .
<i>MX-series Layer 2 Solutions Guide</i>	Describes common configuration scenarios for the Layer 2 features supported on the MX-series routers, including basic bridged VLANs with normalized VLAN tags, aggregated Ethernet links, bridge domains, Multiple Spanning Tree Protocol (MSTP), and integrated routing and bridging (IRB).
<i>Network Interfaces</i>	Provides an overview of the network interface functions of the JUNOS software and describes how to configure the network interfaces on the routing platform.
<i>Network Management</i>	Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP and accounting options.

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

Book	Description
<i>Policy Framework</i>	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, and forwarding options.
<i>Protected System Domain</i>	Provides an overview of the JCS 1200 platform and the concept of Protected System Domains (PSDs). The JCS 1200 platform, which contains up to six redundant pairs of Routing Engines running JUNOS software, is connected to a T320 router or to a T640 or T1600 routing node. To configure a PSD, you assign any number of Flexible PIC concentrators (FPCs) in the T-series routing platform to a pair of Routing Engines on the JCS 1200 platform. Each PSD has the same capabilities and functionality as a physical router, with its own control plane, forwarding plane, and administration.
<i>Routing Protocols</i>	Provides an overview of routing concepts and describes how to configure routing instances, and unicast routing protocols.
<i>Secure Configuration Guide for Common Criteria and JUNOS-FIPS</i>	Provides an overview of secure Common Criteria and JUNOS-FIPS protocols for the JUNOS software and describes how to install and configure secure Common Criteria and JUNOS-FIPS on a routing platform.
<i>Services Interfaces</i>	Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the router.
<i>Software Installation and Upgrade Guide</i>	Describes the JUNOS software components and packaging and explains how to initially configure, reinstall, and upgrade the JUNOS system software. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>Subscriber Access</i>	Provides an overview of the subscriber access features of the JUNOS software and describes how to configure subscriber access support on the router, including dynamic profiles, class of service, AAA, and access methods.
<i>System Basics</i>	Describes Juniper Networks routing platforms and explains how to configure basic system parameters, supported protocols and software processes, authentication, and a variety of utilities for managing your router on the network.
<i>VPNs</i>	Provides an overview and describes how to configure Layer 2 and Layer 3 virtual private networks (VPNs), virtual private LAN service (VPLS), and Layer 2 circuits. Provides configuration examples.
JUNOS References	
<i>Hierarchy and RFC Reference</i>	Describes the JUNOS configuration mode commands. Provides a hierarchy reference that displays each level of a configuration hierarchy, and includes all possible configuration statements that can be used at that level. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>Interfaces Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot interfaces.

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

Book	Description
<i>Routing Protocols and Policies Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot routing policies and protocols, including firewall filters.
<i>System Basics and Services Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot system basics, including commands for real-time monitoring and route (or path) tracing, system software management, and chassis management. Also describes commands for monitoring and troubleshooting services such as class of service (CoS), IP Security (IPsec), stateful firewalls, flow collection, and flow monitoring.
<i>System Log Messages Reference</i>	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
J-Web User Guide	
<i>J-Web Interface User Guide</i>	Describes how to use the J-Web graphical user interface (GUI) to configure, monitor, and manage Juniper Networks routing platforms.
JUNOS API and Scripting Documentation	
<i>JUNOScript API Guide</i>	Describes how to use the JUNOScript application programming interface (API) to monitor and configure Juniper Networks routing platforms.
<i>JUNOS XML API Configuration Reference</i>	Provides reference pages for the configuration tag elements in the JUNOS XML API.
<i>JUNOS XML API Operational Reference</i>	Provides reference pages for the operational tag elements in the JUNOS XML API.
<i>NETCONF API Guide</i>	Describes how to use the NETCONF API to monitor and configure Juniper Networks routing platforms.
<i>JUNOS Configuration and Diagnostic Automation Guide</i>	Describes how to use the commit script and self-diagnosis features of the JUNOS software. This guide explains how to enforce custom configuration rules defined in scripts, how to use commit script macros to provide simplified aliases for frequently used configuration statements, and how to configure diagnostic event policies.
Hardware Documentation	
<i>Hardware Guide</i>	Describes how to install, maintain, and troubleshoot routing platforms and components. Each platform has its own hardware guide.
<i>PIC Guide</i>	Describes the routing platform's Physical Interface Cards (PICs). Each platform has its own PIC guide.
<i>DPC Guide</i>	Describes the Dense Port Concentrators (DPCs) for all MX-series routers.
JUNOScope Documentation	

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

Book	Description
<i>JUNOScope Software User Guide</i>	Describes the JUNOScope software graphical user interface (GUI), how to install and administer the software, and how to use the software to manage routing platform configuration files and monitor routing platform operations.
Advanced Insight Solutions (AIS) Documentation	
<i>Advanced Insight Solutions Guide</i>	Describes the Advanced Insight Manager (AIM) application, which provides a gateway between JUNOS devices and Juniper Support Systems (JSS) for case management and intelligence updates. Explains how to run AI-Scripts on Juniper Networks devices.
J-series Routing Platform Documentation	
<i>Getting Started Guide</i>	Provides an overview, basic instructions, and specifications for J-series routing platforms. The guide explains how to prepare your site for installation, unpack and install the router and its components, install licenses, and establish basic connectivity. Use the <i>Getting Started Guide</i> for your router model.
<i>Basic LAN and WAN Access Configuration Guide</i>	Explains how to configure the interfaces on J-series Services Routers for basic IP routing with standard routing protocols, ISDN backup, and digital subscriber line (DSL) connections.
<i>Advanced WAN Access Configuration Guide</i>	Explains how to configure J-series Services Routers in virtual private networks (VPNs) and multicast networks, configure data link switching (DLSw) services, and apply routing techniques such as policies, stateless and stateful firewall filters, IP Security (IPsec) tunnels, and class-of-service (CoS) classification for safer, more efficient routing.
<i>Administration Guide</i>	Shows how to manage users and operations, monitor network performance, upgrade software, and diagnose common problems on J-series Services Routers.
Release Notes	
<i>JUNOS Release Notes</i>	Summarize new features and known problems for a particular software release, provide corrections and updates to published JUNOS, JUNOScript, and NETCONF manuals, provide information that might have been omitted from the manuals, and describe upgrade and downgrade procedures.
<i>Hardware Release Notes</i>	Describe the available documentation for the routing platform and summarize known problems with the hardware and accompanying software. Each platform has its own release notes.
<i>JUNOScope Release Notes</i>	Contain corrections and updates to the published JUNOScope manual, provide information that might have been omitted from the manual, and describe upgrade and downgrade procedures.
<i>AIS Release Notes</i>	Summarize AIS new features and guidelines, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide initial setup, upgrade, and downgrade procedures.

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

Book	Description
<i>AIS AI-Scripts Release Notes</i>	Summarize AI-Scripts new features, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide instructions for automatic and manual installation, including deleting and rolling back.
<i>J-series Services Router Release Notes</i>	Briefly describe Services Router features, identify known hardware problems, and provide upgrade and downgrade instructions.

Table 4: JUNOS Software Network Operations Guides

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

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

Table 5: JUNOS Software with Enhanced Services Documentation

Book	Description
All Platforms	
<i>JUNOS Software Interfaces and Routing Configuration Guide</i>	Explains how to configure J-series interfaces for basic IP routing with standard routing protocols, ISDN service, firewall filters (access control lists), and class-of-service (CoS) traffic classification.
<i>JUNOS Software Security Configuration Guide</i>	Explains how to configure and manage security services such as stateful firewall policies, IP Security (IPsec) virtual private networks (VPNs), firewall screens, Network Address Translation (NAT), Public Key Cryptography, and Application Layer Gateways (ALGs).
<i>JUNOS Software Administration Guide</i>	Shows how to monitor J-series devices and routing operations, firewall and security services, system alarms and events, and network performance. This guide also shows how to administer user authentication and access, upgrade software, and diagnose common problems.
<i>JUNOS Software CLI Reference</i>	Provides the complete JUNOS software with enhanced services configuration hierarchy and describes the configuration statements and operational mode commands not documented in the standard JUNOS manuals.
J-series Only	
<i>JUNOS Software with Enhanced Services Design and Implementation Guide</i>	Provides guidelines and examples for designing and implementing IPsec VPNs, firewalls, and routing on J-series Services Routers running JUNOS software with enhanced services.
<i>JUNOS Software with Enhanced Services Quick Start</i>	Explains how to quickly set up a J-series Services Router. This document contains router declarations of conformity.
<i>JUNOS Software with Enhanced Services J-series Services Router Hardware Guide</i>	Provides an overview, basic instructions, and specifications for J-series Services Routers. This guide explains how to prepare a site, unpack and install the router, replace router hardware, and establish basic router connectivity. This guide contains hardware descriptions and specifications.
<i>JUNOS Software with Enhanced Services Migration Guide</i>	Provides instructions for migrating an SSG device running ScreenOS software or a J-series Services Router running the JUNOS software to JUNOS software with enhanced services.
<i>WXC Integrated Services Module Installation and Configuration Guide</i>	Explains how to install and initially configure a WXC Integrated Services Module in a J-series Services Router for application acceleration.
<i>JUNOS Software with Enhanced Services Release Notes</i>	Summarizes new features and known problems for a particular release of JUNOS software with enhanced services on J-series Services Routers, including J-Web interface features and problems. The release notes also contain corrections and updates to the manuals and software upgrade and downgrade instructions for JUNOS software with enhanced services.

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

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

Documentation Feedback

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

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

Part 1

Glossary

Chapter 1

Glossary

In this glossary, we list terms that are unique to routing and JUNOS.

Numerics

- | | |
|----------------|---|
| 1X | First phase of third-generation (3G) mobile wireless technology for CDMA2000 networks. |
| 1XEV | Evolutionary phase of third-generation (3G) CDMA2000 networks, divided into two phases: 1XEV-DO (data only) and 1XEV-DV (data and voice). |
| 3DES | Triple Data Encryption Standard. A 168-bit encryption algorithm that encrypts data blocks with three different keys in succession, achieving a higher level of encryption than standard DES. 3DES is often implemented with cipher block chaining (CBC). 3DES is one of the strongest encryption algorithms available for use in virtual private networks (VPNs). Also called <i>triple DES</i> . |
| 3GPP | Third-generation Partnership Project. Created to expedite the development of open, globally accepted technical specifications for the Universal Mobile Telecommunications System (UMTS). |
| 802.1ad | The IEEE specification for “Q-in-Q” encapsulation and bridging of Ethernet frames. |
| 802.1ah | The IEEE specification for media access control (MAC) tunneling encapsulation and bridging of Ethernet frames across a provided backbone-managed bridge. |
| 802.1Q | The IEEE specification for adding virtual local area network (VLAN) tags to an Ethernet frame. |
| 802.3ah | The IEEE specification defining Ethernet between the subscriber and the immediate service provider. Also known as Ethernet in the first or last mile. |

A

AAL	ATM adaptation layer. A series of protocols enabling various types of traffic, including voice, data, image, and video, to run over an ATM network.
AAL5 mode	ATM adaption layer 5. One of four AALs recommended by the ITU-T. AAL5 is used predominantly for the transfer of classical IP over ATM. AAL5 is the least complex of the current AAL recommendations. It offers low bandwidth overhead and simpler processing requirements in exchange for reduced bandwidth capacity and error-recovery capability. It is a Layer 2 circuit transport mode that allows you to send ATM cells between ATM2 IQ interfaces across a Layer 2 circuit-enabled network. You use Layer 2 circuit AAL5 transport mode to tunnel a stream of AAL5-encoded ATM segmentation and reassembly protocol data units (SAR-PDUs) over an MPLS or IP backbone. <i>See also</i> cell-relay mode, Layer 2 circuits, standard AAL5 mode, trunk mode.
ABR	Area border router. Router that belongs to more than one area. Used in OSPF. <i>See also</i> OSPF.
access concentrator	Router that acts as a server in a Point-to-Point Protocol over Ethernet (PPPoE) session, for example, an E-series router.
accounting services	Method of collecting network data related to resource usage.
access point name	<i>See also</i> APN.
ACFC	Address and Control Field Compression. Enables routers to transmit packets without the two 1-byte address and control fields (0xff and 0x03) normal for PPP-encapsulated packets, thus transmitting less data and conserving bandwidth. ACFC is defined in RFC 1661, <i>The Point-to-Point Protocol (PPP)</i> . <i>See also</i> PFC.
active route	Route chosen from all routes in the routing table to reach a destination. Active routes are installed into the forwarding table.
adaptive services	Set of services or applications that you can configure on an Adaptive Services PIC (AS PIC). The services and applications include stateful firewall, Network Address Translation (NAT), intrusion detection service (IDS), Internet Protocol Security (IPsec), Layer 2 Tunneling Protocol (L2TP), and voice services. <i>See also</i> tunneling protocol.
add/drop multiplexer	<i>See</i> ADM.
Address and Control Field Compression	<i>See</i> ACFC.
address match conditions	Use of an IP address as a match criterion in a routing policy or a firewall filter.
Address Resolution Protocol	<i>See</i> ARP.

adjacency	Portion of the local routing information that pertains to the reachability of a single neighbor over a single circuit or interface.
Adjacency-RIB-In	Logical software table that contains BGP routes received from a specific neighbor.
Adjacency-RIB-Out	Logical software table that contains BGP routes to be sent to a specific neighbor.
ADM	Add/drop multiplexer. SONET functionality that allows lower-level signals to be dropped from a high-speed optical connection.
ADSL	Asymmetrical digital subscriber line. A technology that allows more data to be sent over existing copper telephone lines, using the public switched telephone network (PSTN). ADSL supports data rates from 1.5 to 9 Mbps when receiving data (downstream rate) and from 16 to 640 Kbps when sending data (upstream rate).
ADSL Annex A PIM	<i>See</i> ITU-T Rec. G.992.1.
ADSL Annex B PIM	<i>See</i> ITU-T Rec. G.992.1.
ADSL interface	Asymmetrical digital subscriber line interface. Physical WAN interface that connects a router to a digital subscriber line access multiplexer (DSLAM). An ADSL interface allocates line bandwidth asymmetrically. Downstream (provider-to-customer) data rates can be up to 8 Mbps for ADSL, 12 Mbps for ADSL2, and 25 Mbps for ADSL2 + . Upstream (customer-to-provider) rates can be up to 800 Kbps for ADSL and 1 Mbps for ADSL2 and ADSL2 + , depending on the implementation.
ADSL2 interface	ADSL interface that supports ITU-T Standard G.992.3 and ITU-T Standard G.992.4. ADSL2 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	ADSL interface that supports ITU-T Standard G.992.5. ADSL2 + allocates downstream (provider-to-customer) data rates of up to 25 Mbps and upstream (customer-to-provider) rates of up to 1 Mbps.
Advanced Encryption Standard	<i>See</i> AES.
AES	Advanced Encryption Standard. Defined in FIPS PUB 197. The AES algorithm uses keys of 128, 192, or 256 bits to encrypt and decrypt data in blocks of 128 bits.
aggregate route	Combination of groups of routes that have common addresses into a single entry in a routing table.

aggregated interface	Logical bundle of physical interfaces. The aggregated interface is managed as a single interface with one IP address. Network traffic is dynamically distributed across ports, so administration of data flowing across a given port is done automatically within the aggregated link. Using multiple ports in parallel provides redundancy and increases the link speed beyond the limits of any single port.
AH	Authentication header. A component of the IPsec protocol used to verify that the contents of a packet have not changed, and to validate the identity of the sender. <i>See also</i> ESP.
ALI	ATM line interface. Interface between ATM and 3G systems. <i>See also</i> ATM.
alternate priority queuing	<i>See</i> APQ.
ANSI	American National Standards Institute. The United States' representative to the ISO.
Any Source Multicast	<i>See</i> ASM.
APN	Access point name. When mobile stations connect to IP networks over a wireless network, the GGSN uses the APN to distinguish among the connected IP networks (known as APN networks). In addition to identifying these connected networks, an APN is also a configured entity that hosts the wireless sessions, which are called Packet Data Protocol (PDP) contexts.
application-specific integrated circuit	<i>See</i> ASIC.
APQ	Alternate priority queuing. Dequeuing method that has a special queue, similar to strict-priority queuing (SPQ), which is visited only 50 percent of the time. The packets in the special queue still have a predictable latency, although the upper limit of the delay is higher than that with SPQ. Since the other configured queues share the remaining 50 percent of the service time, queue starvation is usually avoided. <i>See also</i> SPQ.
APS	Automatic Protection Switching. Technology used by SONET ADMs to protect against circuit faults between the ADM and a router and to protect against failing routers.
area	Routing subdomain that maintains detailed routing information about its own internal composition as well as routing information that allows it to reach other routing subdomains. In IS-IS, an area corresponds to a Level 1 subdomain. In IS-IS and OSPF, a set of contiguous networks and hosts within an autonomous system that have been administratively grouped together.
area border router	<i>See</i> ABR.
ARP	Address Resolution Protocol. Protocol used for mapping IPv4 addresses to media access control (MAC) addresses. <i>See also</i> NDP.

AS	Autonomous system. Set of routers under a single technical administration. Each AS normally uses a single interior gateway protocol (IGP) and metrics to propagate routing information within the set of routers. Also called a routing domain.
AS external link advertisement	OSPF link-state advertisement sent by AS boundary routers to describe external routes that they have detected. These link-state advertisements are flooded throughout the AS (except for stub areas).
AS path	In BGP, the route to a destination. The path consists of the AS numbers of all routers that a packet must go through to reach a destination.
AS PIC	Adaptive Services PIC. <i>See</i> adaptive services.
ASBR	Autonomous system boundary router. In OSPF, a router that exchanges routing information with routers in other ASs.
ASBR Summary LSA	OSPF link-state advertisement (LSA) sent by an area border router (ABR) to advertise the router ID of an autonomous system boundary router (ASBR) across an area boundary. <i>See also</i> ASBR.
ASIC	Application-specific integrated circuit. Specialized processors that perform specific functions on the router.
ASM	The acronym ASM can be either of the following: <ol style="list-style-type: none"> 1. Adaptive Services Module. On a Juniper Networks M7i router, provides the same functionality as the AS PIC. 2. Any Source Multicast. Method of allowing a multicast receiver to listen to all traffic sent to a multicast group, regardless of its source.
asymmetrical digital subscriber line	<i>See</i> ADSL.
Asynchronous Transfer Mode	<i>See</i> ATM.
ATM	Asynchronous Transfer Mode. A high-speed multiplexing and switching method utilizing fixed-length cells of 53 octets to support multiple types of traffic.
ATM adaption layer	<i>See</i> AAL.
ATM line interface	<i>See</i> ALI.
ATM-over-ADSL interface	Asynchronous Transfer Mode (ATM) interface used to send network traffic through a point-to-point connection to a DSL access multiplexer (DSLAM). ATM-over-ADSL interfaces are intended for asymmetrical digital subscriber line (ADSL) connections only, not for direct ATM connections.

atomic	Smallest possible operation. An atomic operation is performed either entirely or not at all. For example, if machine failure prevents a transaction from finishing, the system is rolled back to the start of the transaction, with no changes taking place.
AUC	Authentication center. Part of the Home Location Register (HLR) in third-generation (3G) systems; performs computations to verify and authenticate a mobile phone user.
authentication center	<i>See</i> AUC.
authentication header	<i>See</i> AH.
auto-RP	Method of electing and announcing the rendezvous point-to-group address mapping in a multicast network. JUNOS software supports this vendor-proprietary specification. <i>See also</i> RP.
automatic policing	Policer that allows you to provide strict service guarantees for network traffic. Such guarantees are especially useful in the context of differentiated services for traffic engineered LSPs, providing better emulation for ATM wires over an MPLS network.
Automatic Protection Switching	<i>See</i> APS.
autonegotiation	Used by Ethernet devices to configure interfaces automatically. If interfaces support different speeds or different link modes (half duplex or full duplex), the devices attempt to settle on the lowest common denominator.
autonomous system	<i>See</i> AS.
autonomous system boundary router	<i>See</i> ASBR.
autonomous system external link advertisement	OSPF link-state advertisement sent by autonomous system boundary routers to describe external routes that they have detected. These link-state advertisements are flooded throughout the autonomous system (except for stub areas).
autonomous system path	In BGP, the route to a destination. The path consists of the autonomous system numbers of all the routers a packet must pass through to reach a destination.

B

B-channel	Bearer channel. A 64-Kbps channel used for voice or data transfer on an ISDN interface. <i>See also</i> D-channel.
B-MAC	Backbone source and destination MAC address fields found in the IEEE 802.1ah provider MAC encapsulation header.

B-TAG	Field defined in the IEEE 802.1ah provider MAC encapsulation header that carries the backbone VLAN identifier information. The format of the B-TAG field is the same as that of the IEEE 802.1ad S-TAG field. <i>See also</i> S-TAG.
B-VID	Specific VLAN identifier carried in a B-TAG.
BA classifier	Behavior aggregate classifier. A method of classification that operates on a packet as it enters the router. The packet header contents are examined, and this single field determines the class-of-service (CoS) settings applied to the packet. <i>See also</i> multifield classifier.
backbone area	In OSPF, an area that consists of all networks in area ID 0.0.0.0, their attached routers, and all area border routers.
backbone router	OSPF router with all operational interfaces within area 0.0.0.0.
backplane	<i>See</i> midplane.
backup designated router	OSPF router on a broadcast segment that monitors the operation of the designated router and takes over its functions if the designated router fails.
backward explicit congestion notification	<i>See</i> BECN.
bandwidth	Range of transmission frequencies a network can use, expressed as the difference between the highest and lowest frequencies of a transmission channel. In computer networks, greater bandwidth indicates a faster data transfer rate capacity.
bandwidth model	In Differentiated Services-aware traffic engineering, determines the value of the available bandwidth advertised by the interior gateway protocols (IGPs).
bandwidth on demand	Technique to temporarily provide additional capacity on a link to handle bursts in data, videoconferencing, or other variable bit rate applications. Also called <i>flexible bandwidth allocation</i> . On a Services Router, an ISDN cost-control feature defining the bandwidth threshold that must be reached on links before a Services Router initiates additional ISDN data connections to provide more bandwidth.
base station controller	<i>See</i> BSC.
base station subsystem	<i>See</i> BSS.
Base Station System GPRS Protocol	<i>See</i> BSSGP.

base transceiver station	<i>See</i> BTS.
Basic Rate Interface	<i>See</i> BRI.
BBD	<i>See</i> blade bay data.
bearer channel	<i>See</i> B-channel.
BECN	Backward explicit congestion notification. In a Frame Relay network, a header bit transmitted by the destination device requesting that the source device send data more slowly. BECN minimizes the possibility that packets will be discarded when more packets arrive than can be handled. <i>See also</i> FECN.
behavior aggregate classifier	<i>See</i> BA classifier.
Belcore	Bell Communications Research. A research and development organization created after the divestiture of the Bell System. It is supported by the regional Bell holding companies (RBHCs), which own the regional Bell operating companies (RBOCs).
Bellman-Ford algorithm	Algorithm used in distance-vector routing protocols to determine the best path to all routes in the network.
BERT	Bit error rate test. A test that can be run on the following interfaces to determine whether they are operating properly: E1, E3, T1, T3, and channelized (DS3, OC3, OC12, and STM1) interfaces.
BFD	Bidirectional forwarding detection. A simple hello mechanism that detects failures in a network. Used with routing protocols to speed up failure detection.
BGP	Border Gateway Protocol. Exterior gateway protocol used to exchange routing information among routers in different autonomous systems.
bidirectional forwarding detection	<i>See</i> BFD.
bit error rate test	<i>See</i> BERT.
bit field match conditions	Use of fields in the header of an IP packet as match criteria in a firewall filter.
bit rate	Number of bits transmitted per second.
BITS	Building Integrated Timing Source. Dedicated timing source that synchronizes all equipment in a particular building.

blade	Routing Engine in the JCS chassis that runs JUNOS software. The JCS chassis holds up to 12 single Routing Engines (or 6 redundant Routing Engine pairs).
blade bay data (BBD)	60-byte text string stored in the JCS management module NVRAM that conveys configuration information to the Routing Engines (blades) in the JCS chassis.
Blowfish	Unpatented, symmetric cryptographic method developed by Bruce Schneier and used in many commercial and freeware software applications. Blowfish uses variable-length keys of up to 448 bits.
BOOTP	Bootstrap protocol. A UDP/IP-based protocol that allows a booting host to configure itself dynamically and without user supervision. BOOTP provides a means to notify a host of its assigned IP address, the IP address of a boot server host, and the name of a file to be loaded into memory and executed. Other configuration information, such as the local subnet mask, the local time offset, the addresses of default routers, and the addresses of various Internet servers, can also be communicated to a host using BOOTP.
bootstrap protocol	<i>See</i> BOOTP.
bootstrap router	Single router in a multicast network responsible for distributing candidate rendezvous point information to all PIM-enabled routers.
Border Gateway Protocol	<i>See</i> BGP.
BPDU	Bridge protocol data unit. A Spanning Tree Protocol hello packet that is sent out at intervals to exchange information across bridges and detect loops in a network topology.
BRI	Basic Rate Interface. ISDN interface intended for home and small enterprise applications. BRI consists of two 64-Kbps B-channels to carry voice or data, and one 16-Kbps D-channel for control and signaling. <i>See also</i> B-channel, D-channel.
bridge	Bridge can be either of the following: <ol style="list-style-type: none"> 1. Network component defined by the IEEE that forwards frames from one LAN segment or VLAN to another. The bridging function can be contained in a router, LAN switch, or other specialized device. A bridge operates at Layer 2 of the OSI reference model. <i>See also</i> switch. 2. Device that uses the same communications protocol to connect and pass packets between two network segments.
bridge domain	Set of logical ports that share the same flooding or broadcast characteristics. As in a virtual LAN, a bridge domain spans one or more ports of multiple devices. By default, each bridge domain maintains its own forwarding database of MAC addresses learned from packets received on ports belonging to that bridge domain. <i>See also</i> broadcast domain and VLAN.

bridge protocol data unit	<i>See</i> BPDU.
broadband services router	<i>See</i> BSR
broadcast	Operation of sending network traffic from one network node to all other network nodes.
broadcast domain	Logical division of a computer network, in which all nodes can reach each other by broadcast at the data link layer.
BSC	Base station controller. Key network node in third-generation (3G) systems that supervises the functioning and control of multiple base transceiver stations.
BSR	Broadband services router. A router used for subscriber management and edge routing.
BSS	Base station subsystem. Composed of the base transceiver station (BTS) and base station controller (BSC).
BSSGP	Base Station System GPRS Protocol. Processes routing and quality-of-service (QoS) information for the BSS.
BTS	Base transceiver station. Mobile telephony equipment housed in cabinets and colocated with antennas. (Also known as a <i>radio base station</i> .)
buffers	Memory space for handling data in transit. Buffers compensate for differences in processing speed between network devices and handle bursts of data until they can be processed by slower devices.
Building Integrated Timing Source	<i>See</i> BITS.
bundle	Multiple physical links of the same type, such as multiple asynchronous lines, or physical links of different types, such as leased synchronous lines and dial-up asynchronous lines. Collection of software that makes up a JUNOS software release.
bypass LSP	Carries traffic for an LSP whose link-protected interface has failed. A bypass LSP uses a different interface and path to reach the same destination.

C

CA	Certificate authority. A trusted third-party organization that creates, enrolls, validates, and revokes digital certificates. The CA guarantees a user's identity and issues public and private keys for message encryption and decryption (coding and decoding).
-----------	---

CAC	Call admission control. In Differentiated-Services-aware traffic engineering, checks for adequate bandwidth on the path before the LSP is established. If the bandwidth is insufficient, the LSP is not established and an error is reported.
CAIDA	Cooperative Association for Internet Data Analysis. An association that provides tools and analyses promoting the engineering and maintenance of a robust, scalable Internet infrastructure. One tool, cflowd, allows you to collect an aggregate of sampled flows and send the aggregate to a specified host that runs the cflowd application available from CAIDA.
call admission control	<i>See</i> CAC.
Call Detail Record	<i>See</i> CDR.
callback	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. <i>See also</i> dial-in.
caller ID	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 only from callers whose caller IDs are configured on it.
CAMEL	Customized Applications of Mobile Enhanced Logic. An ETSI standard for GSM networks that enhances the provision of Intelligent Network services.
candidate configuration	File maintained by the JUNOS software containing changes to the router's active configuration. This file becomes the active configuration when a user issues the commit command.
candidate RP advertisements	Information sent by routers in a multicast network when they are configured as a local rendezvous point. This information is unicast to the bootstrap router for the multicast domain.
carrier-of-carriers VPN	Virtual private network (VPN) service supplied to a network service provider that is supplying either Internet service or VPN service to an end customer. For a carrier-of-carriers VPN, the customer's sites are configured within the same autonomous system (AS).
CB	Control Board. On a T640 routing node, part of the host subsystem that provides control and monitoring functions for router components.
CBC	Cipher block chaining. A mode of encryption using 64 or 128 bits of fixed-length blocks in which each block of plain text is XORed with the previous cipher text block before being encrypted. <i>See also</i> XOR.

CBR	Constant bit rate. For ATM1 and ATM2 IQ interfaces, data that is serviced at a constant, repetitive rate. CBR is used for traffic that does not need to periodically burst to a higher rate, such as nonpacketized voice and audio.
CCC	Circuit cross-connect. A JUNOS software feature that allows you to configure transparent connections between two circuits. A circuit can be a Frame Relay DLCI, an ATM virtual channel (VC), a PPP interface, a Cisco HDLC interface, or an MPLS label-switched path (LSP).
CDMA	Code Division Multiple Access. Technology for digital transmission of radio signals between, for example, a mobile telephone and a base transceiver station (BTS).
CDMA2000	Radio transmission and backbone technology for the evolution to third-generation (3G) mobile networks.
CDR	Call Detail Record. A record containing data (such as origination, termination, length, and time of day) unique to a specific call.
CE	Customer edge. The customer router that is connected to the service provider network.
CE device	Customer edge device. Router or switch in the customer's network that is connected to a service provider's provider edge (PE) router and participates in a Layer 3 VPN.
cell relay	Data transmission technology based on the use of small, fixed-size packets (cells) that can be processed and switched in hardware at high speeds. Cell relay is the basis for many high-speed network protocols, including ATM and IEEE 802.6.
cell tax	Physical transmission capacity used by header information when sending data packets in an ATM network. Each ATM cell uses a 5-byte header.
cell-relay mode	Layer 2 circuit transport mode that sends ATM cells between ATM2 intelligent queuing (IQ) interfaces over an MPLS core network. You use Layer 2 circuit cell-relay transport mode to tunnel a stream of ATM cells over an MPLS or IP backbone. <i>See also</i> AAL5 mode, Layer 2 circuits, standard AAL5 mode, trunk mode.
central office	<i>See</i> CO.
certificate authority	<i>See</i> CA.
certificate revocation list	<i>See</i> CRL.
CFEB	Compact Forwarding Engine Board. In M7i and M10i routers, provides route lookup, filtering, and switching to the destination port.
cflowd	Application available from CAIDA that collects an aggregate of sampled flows and sends the aggregate to a specified host running the cflowd application.

CFM	Connectivity fault management. An end-to-end per-service-instance Ethernet layer operation, administration, and management (OAM) protocol. CFM includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks.
Challenge Handshake Authentication Protocol	<i>See</i> CHAP.
channel	Communication circuit linking two or more devices. A channel provides an input/output interface between a processor and a peripheral device, or between two systems. A single physical circuit can consist of one or many channels, or two systems carried on a physical wire or wireless medium. For example, the dedicated channel between a telephone and the central office (CO) is a twisted-pair copper wire. <i>See also</i> frequency-division multiplexed channel, time-division multiplexed channel.
channel group	Combination of DS0 interfaces partitioned from a channelized interface into a single logical bundle.
channel service unit	<i>See</i> CSU/DSU.
channelized E1	A 2.048-Mbps interface that can be configured as a single clear-channel E1 interface or channelized into as many as 31 discrete DS0 interfaces. On most channelized E1 interfaces, time slots are numbered from 1 through 32, and time slot 1 is reserved for framing. On some legacy channelized E1 interfaces, time slots are numbered from 0 through 31, and time slot 0 is reserved for framing.
channelized interface	Interface that is a subdivision of a larger interface, minimizing the number of Physical Interface Cards (PICs) or Physical Interface Modules (PIMs) that an installation requires. On a channelized PIC or PIM, each port can be configured as a single clear channel or partitioned into multiple discrete T3, T1, E1, and DS0 interfaces, depending on the size of the channelized PIC or PIM.
channelized T1	A 1.544-Mbps interface that can be configured as a single clear-channel T1 interface or channelized into as many as 24 discrete DS0 interfaces. Time slots are numbered from 1 through 24.
CHAP	Challenge Handshake Authentication Protocol. A protocol that authenticates remote users. CHAP is a server-driven, three-step authentication mechanism that depends on a shared secret password that resides on both the server and the client.
chassis daemon	<i>See</i> chassisd.
chassisd	Chassis daemon. A JUNOS software process responsible for managing the interaction of the router's physical components.

CIDR	Classless interdomain routing. A method of specifying Internet addresses in which you explicitly specify the bits of the address to represent the network address instead of determining this information from the first octet of the address.
CIP	Connector Interface Panel. On an M160 router, the panel that contains connectors for the Routing Engines, BITS interfaces, and alarm relay contacts.
cipher block chaining	<i>See</i> CBC.
CIR	Committed information rate. The CIR specifies the average rate at which packets are admitted to the network. As each packet enters the network, it is counted. Packets that do not exceed the CIR are marked green, which corresponds to low loss priority. Packets that exceed the CIR but are below the peak information rate (PIR) are marked yellow, which corresponds to medium loss priority. <i>See also</i> trTCM, PIR.
circuit cross-connect	<i>See</i> CCC.
Cisco-RP-Announce	Message advertised into a multicast network by a router configured as a local rendezvous point (RP) in an auto-RP network. A Cisco-RP-Announce message is advertised in dense-mode PIM to the 224.0.1.39 multicast group address.
Cisco-RP-Discovery	Message advertised by the mapping agent in an auto-RP network. A Cisco-RP-Discovery message contains the rendezvous point (RP) to multicast group address assignments for the domain. It is advertised in dense-mode PM to the 224.0.1.40 multicast group address.
CIST	Common and internal spanning tree. The single spanning tree calculated by the Spanning Tree Protocol (STP) and the Rapid Spanning Tree Protocol (RSTP) and the logical continuation of that connectivity through multiple spanning-tree (MST) bridges and regions, calculated to ensure that all LANs in the bridged LAN are simply and fully connected. <i>See also</i> MSTI.
class of service	<i>See</i> CoS.
Class Selector code point	<i>See</i> CSCP.
class type	In Differentiated Services-aware traffic engineering, a collection of traffic flows that are treated equivalently in a Differentiated Services domain. A class type maps to a queue and is much like a class-of-service (CoS) forwarding class in concept. It is also known as a <i>traffic class</i> .
class-of-service process	<i>See</i> cosd.
classification	In class of service (CoS), the examination of an incoming packet that associates the packet with a particular CoS servicing level. There are two kinds of classifiers, behavior aggregate and multifield. <i>See also</i> BA classifier, multifield classifier.

classifier	Method of reading a sequence of bits in a packet header or label and determining how the packet should be forwarded internally and scheduled (queued) for output.
classless interdomain routing	<i>See</i> CIDR.
clear channel	Interface configured on a channelized PIC or PIM that operates as a single channel, does not carry signaling, and uses the entire port bandwidth.
CLEC	(Pronounced “ <i>See-lek</i> ”) Competitive local exchange carrier. Company that competes with the already established local telecommunications business by providing its own network and switching.
CLEI	Common Language Equipment Identifier. Inventory code used to identify and track telecommunications equipment.
CLI	Command-line interface. Interface provided for configuring and monitoring the routing protocol software.
client peer	In a BGP route reflection, a member of a cluster that is not the route reflector. <i>See also</i> nonclient peer.
CLNP	Connectionless Network Protocol. An ISO-developed protocol for OSI connectionless network service. CLNP is the OSI equivalent of IP.
CLNS	Connectionless Network Service. A Layer 3 protocol, similar to Internet Protocol version 4 (IPv4). CLNS uses network service access points (NSAP) instead of the prefix addresses found in IPv4 to specify end systems and intermediate systems.
cluster	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.
CO	Central office. The local telephone company building that houses circuit switching equipment used for subscriber lines in a given area.
Code Division Multiple Access	<i>See</i> CDMA.
code-point alias	Name assigned to a pattern of code-point bits. This name is used, instead of the bit pattern, in the configuration of other class-of-service (CoS) components, such as classifiers, drop-profile maps, and rewrite rules.
command completion	Function of a router’s command-line interface (CLI) that allows a user to enter only the first few characters in any command. Users access this function through the Spacebar or Tab key.

command-line interface	<i>See</i> CLI.
commit	JUNOS software command-line interface (CLI) configuration-mode command that saves changes made to a router configuration, verifies the syntax, applies the changes to the configuration currently running on the router, and identifies the resulting file as the current operational configuration.
commit script	Script that enforces custom configuration rules. A script runs each time a new candidate configuration is committed and inspects the configuration. If a configuration breaks your custom rules, the script can generate actions for the JUNOS software.
commit script macro	Sequence of commands that allow you to create custom configuration syntax to simplify the task of configuring a routing platform. By itself, your custom syntax has no operational impact on the routing platform. A corresponding commit script macro uses your custom syntax as input data for generating standard JUNOS configuration statements that execute your intended operation.
committed information rate	<i>See</i> CIR.
common and internal spanning tree	<i>See</i> CIST.
Common Criteria	International standard (ISO/IEC 15408) for computer security. <i>See also</i> EAL3
Common Criteria Evaluation Assurance Level 3	<i>See</i> EAL3.
Common Language Equipment Identifier	<i>See</i> CLEI.
community	<p>In BGP, a group of destinations that share a common property. Community information is included as one of the path attributes in BGP update messages.</p> <p>In SNMP, an authentication scheme that authorizes SNMP clients based on the source IP address of incoming SNMP packets, defines which MIB objects are available, and specifies the operations (read-only or read-write) allowed on those objects.</p>
Compact Forwarding Engine Board	<i>See</i> CFEB.
CompactFlash drive	Nonvolatile memory card in Juniper Networks M-series, MX-series, T-series, and J-series routing platforms used for storing a copy of the JUNOS software and the current and most recent router configurations. It also typically acts as the primary boot device.
competitive local exchange carrier	<i>See</i> CLEC.

complete sequence number PDU	<i>See</i> CSNP.
Compressed Real-Time Transport Protocol	<i>See</i> CRTP.
Concurrent Versions System	<i>See</i> CVS.
confederation	In BGP, a group of systems that appears to external autonomous systems as a single autonomous system.
configuration management server	When using NETCONF or JUNOScript, a remote server used to configure JUNOS routers.
configuration mode	JUNOS software mode that allows a user to alter the router's current configuration.
Connect	BGP neighbor state in which the local router has initiated the TCP session and is waiting for the remote peer to complete the TCP connection.
Connectionless Network Protocol	<i>See</i> CLNP.
Connectionless Network Service	<i>See</i> CLNS.
connectivity fault management	<i>See</i> CFM.
Connector Interface Panel	<i>See</i> CIP.
constant bit rate	<i>See</i> CBR.
constrained path	In traffic engineering, a path determined using the CSPF algorithm. The ERO carried in the RSVP packets contains the constrained path information. <i>See also</i> ERO.
Constrained Shortest Path First	<i>See</i> CSPF.
context node	Node that the Extensible Stylesheet Language for Transformations (XSLT) processor is currently examining. XSLT changes the context as it traverses the XML document's hierarchy. <i>See also</i> XSLT.
context-sensitive help	Function of the router's command-line interface (CLI) that allows a user to request information on the JUNOS software hierarchy. You can access context-sensitive help in both operational and configuration mode.
contributing routes	Active IP routes in the routing table that share the same most-significant bits and are more specific than an aggregate or generate route.

Control Board	<i>See</i> CB.
control plane	Virtual network path used to set up, maintain, and terminate data plane connections. <i>See also</i> data plane.
Cooperative Association for Internet Data Analysis	<i>See</i> CAIDA.
core	Central backbone of the network.
CoS	Class of service. Method of classifying traffic on a packet-by-packet basis using information in the type-of-service (ToS) byte to provide different service levels to different traffic.
cosd	Class-of-service process that enables the routing platform to provide different levels of service to applications based on packet classifications.
CPE	Customer premises equipment. Telephone, modem, router, or other service provider equipment located at a customer site.
craft interface	Mechanisms used by a Communication Workers of America craftsperson to operate, administer, and maintain equipment or provision data communications. On a Juniper Networks router, the craft interface allows you to view status and troubleshooting information and perform system control functions.
Critical Security Parameter	<i>See</i> CSP.
CRL	Certificate revocation list. A list of digital certificates that have been invalidated, including the reasons for revocation and the names of the entities that issued them. A CRL prevents usage of digital certificates and signatures that have been compromised.
C RTP	Compressed Real-Time Transport Protocol. Protocol that decreases the size of the IP, UDP, and RTP headers and works with reliable and fast point-to-point links for voice over IP (VoIP) traffic. CRTP is defined in RFC 2508.
Crypto Accelerator Module	Processor card that speeds up certain cryptographic IP Security (IPsec) services on some J-series Services Routers. For the supported cryptographic algorithms, see the J-series documentation.
Crypto Officer	Superuser responsible for the proper operation of a router running JUNOS-FIPS software.
CSCP	Class Selector code point. Eight Differentiated Services code point (DSCP) values of the form xxx000 (where x can be 0 or 1). Defined in RFC 2474.

CSNP	Complete sequence number PDU. Packet that contains a complete list of all the LSPs in the IS-IS database.
CSP	Critical Security Parameter. On routers running JUNOS-FIPS software, a collection of cryptographic keys and passwords that must be protected at all times.
CSPF	Constrained Shortest Path First. An MPLS algorithm that has been modified to take into account specific restrictions when calculating the shortest path across the network.
CSU/DSU	Channel service unit/data service unit. A channel service unit connects a digital phone line to a multiplexer or other digital signal device. A data service unit connects a DTE to a digital phone line.
customer edge	<i>See</i> CE.
customer edge device	<i>See</i> CE device.
customer premises equipment	<i>See</i> CPE.
Customized Applications of Mobile Enhanced Logic	<i>See</i> CAMEL.
CVS	Concurrent Versions System. A widely used version control system for software development or data archives.

D

D-channel	Delta channel. A circuit-switched channel that carries signaling and control for B-channels. In Basic Rate Interface (BRI) applications, it can also support customer packet data traffic at speeds up to 9.6 Kbps. <i>See also</i> B-channel, BRI.
daemon	Background process that performs operations for the system software and hardware. Daemons normally start when the system software is booted, and run as long as the software is running. In the JUNOS software, daemons are also referred to as processes.
damping	Method of reducing the number of update messages sent between BGP peers, thereby reducing the load on these peers without adversely affecting the route convergence time for stable routes.
data circuit-terminating equipment	<i>See</i> DCE.
Data Encryption Standard	<i>See</i> DES.

data link switching	<i>See</i> DLSw.
data packet	Chunk of data transiting the router from the source to a destination.
data plane	Virtual network path used to distribute data between nodes. <i>See also</i> control plane.
data service unit	<i>See</i> CSU/DSU.
data terminal equipment	<i>See</i> DTE.
data-driven multicast distribution tree tunnel	<i>See</i> data-MDT.
data-link connection identifier	<i>See</i> DLCI.
data-MDT	Data-driven multicast distribution tree tunnel. A multicast tunnel created and deleted based on defined traffic loads and designed to ease loading on the default MDT tunnel.
database description packet	OSPF packet type used in the formation of an adjacency. The packet sends summary information about the local router's database to the neighboring router.
dcd	Device control process. A JUNOS software interface process (daemon).
DCE	Data circuit-terminating equipment. An RS-232-C device, typically used for a modem or printer, or a network access and packet switching node.
DCU	Destination class usage. A means of tracking traffic originating from specific prefixes on the customer edge router and destined for specific prefixes on the provider core router, based on the IP source and destination addresses.
DE	Discard-eligible bit. In a Frame Relay network, a header bit notifying devices on the network that traffic can be dropped during congestion to ensure the delivery of higher priority traffic.
deactivate	Method of modifying the router's active configuration. Portions of the hierarchy marked as inactive using this command are ignored during the router's commit process as if they were not configured at all.
dead interval	Amount of time that an OSPF router maintains a neighbor relationship before declaring that neighbor as no longer operational. The JUNOS software uses a default value of 40 seconds for this timer.
dead peer detection	<i>See</i> DPD.

default address	Router address that is used as the source address on unnumbered interfaces.
default route	Route used to forward IP packets when a more specific route is not present in the routing table. Often represented as 0.0.0.0/0, the default route is sometimes referred to as the route of last resort.
delta channel	<i>See</i> D-channel.
demand circuit	Network segment whose cost varies with usage, according to a service level agreement with a service provider. Demand circuits limit traffic based on either bandwidth (bits or packets transmitted) or access time. <i>See also</i> multicast.
denial of service	<i>See</i> DoS.
dense mode	Method of forwarding multicast traffic to interested listeners. Dense mode forwarding assumes that most of the hosts on the network will receive the multicast data. Routers flood packets and prune unwanted traffic every 3 minutes.
dense wavelength-division multiplexing	<i>See</i> DWDM.
DES	Data Encryption Standard. A method for encrypting information using a 56-bit key. Considered to be a legacy method and insecure for many applications. <i>See also</i> 3DES.
designated router	In OSPF, a router selected by other routers that is responsible for sending link-state advertisements (LSAs) that describe the network, thereby reducing the amount of network traffic and the size of the routers' topological databases.
destination class usage	<i>See</i> DCU.
destination prefix length	Number of bits of the network address used for the host portion of a CIDR IP address.
destination service access point	<i>See</i> DSAP.
device control process	<i>See</i> dcd.
DFC	Dynamic flow capture. Process of collecting packet flows that match a particular filter list to one or more content destinations using an on-demand control protocol that relays requests from one or more control sources.
DHCP	Dynamic Host Configuration Protocol. Allocates IP addresses dynamically so that they can be reused when no longer needed.

dial backup	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.
dial-in	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. <i>See also</i> callback.
dial-on-demand routing (DDR) backup	Feature that provides a J-series Services Router with full-time connectivity across an ISDN line. 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. <i>See also</i> dialer filter, dialer watch.
dialer filter	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. <i>See also</i> dial-on-demand routing (DDR) backup, floating static route.
dialer interface (di)	Logical interface for configuring dialing properties and the control interface for a backup ISDN connection.
dialer profile	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.
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. <i>See also</i> dial-on-demand routing (DDR) backup.
Differentiated Services	<i>See</i> DiffServ.
Differentiated Services aware	<i>See</i> DiffServ-aware.
Differentiated Services code point	<i>See</i> DSCP.

Differentiated Services domain	Routers in a network that have Differentiated Services enabled.
Differentiated Services-aware traffic engineering	Type of constraint-based routing that can enforce different bandwidth constraints for different classes of traffic. It can also do call admission control (CAC) on each traffic engineering class when a label-switched path (LSP) is established.
Diffie-Hellman	Method of key exchange across a nonsecure environment, such as the Internet. The Diffie-Hellman algorithm negotiates a session key without sending the key itself across the network by allowing each party to pick a partial key independently and send part of it to each other. Each side then calculates a common key value. This is a symmetrical method and keys are typically used only for a short time, then discarded and regenerated.
DiffServ	Differentiated Services (based on RFC 2474). DiffServ uses the type-of-service (ToS) byte to identify different packet flows on a packet-by-packet basis. DiffServ adds a Class Selector code point (CSCP) and a Differentiated Services code point (DSCP).
DiffServ-aware	Paradigm that gives different treatment to traffic based on the experimental (EXP) bits in the MPLS label header and allows you to provide multiple classes of service.
digital certificate	Electronic file based on private and public key technology that verifies the identity of the certificate's holder to protect data exchanged online. Digital certificates are issued by a certificate authority (CA).
Dijkstra algorithm	<i>See</i> SPF.
DIMM	Dual inline memory module. A 168-pin memory module that supports 64-bit data transfer.
direct routes	<i>See</i> interface routes.
disable	Method of modifying the router's active configuration. When portions of the hierarchy are marked as disabled (mainly router interfaces), the router uses the configuration but ignores the disabled portions.
discard	JUNOS software syntax command used in a routing policy or a firewall filter. The command halts the logical processing of the policy or filter when a set of match conditions is met. The specific route or IP packet is dropped from the network silently. It can also be a next-hop attribute assigned to a route in the routing table.
discard-eligible bit	<i>See</i> DE.
distance-vector	Method used in Bellman-Ford routing protocols to determine the best path to all routers in the network. Each router determines the distance (metric) to the destination and the vector (next hop) to follow.

Distributed Buffer Manager ASIC	Juniper Networks ASIC responsible for managing the router's packet storage memory.
DLCI	Data-link connection identifier. Identifier for a Frame Relay virtual connection (also called a logical interface).
DLSw	Data link switching. Method of tunneling IBM System Network Architecture (SNA) and NetBIOS traffic over an Internet Protocol (IP) network. (The JUNOS software does not support NetBIOS.) <i>See also</i> tunneling protocol.
DLSw circuit	Path formed by establishing data link control (DLC) connections between an end system and a local router configured for DLSw. Each DLSw circuit is identified by the circuit ID that includes the end system method authenticity check (MAC) address, local service access point (LSAP), and DLC port ID. Multiple DLSw circuits can operate over the same DLSw connection.
DLSw connection	Set of TCP connections between two DLSw peers that is established after the initial handshake and successful capabilities exchange.
DNS	Domain Name System. A system that stores information about hostnames and domain names. DNS provides an IP address for each hostname, and lists the e-mail exchange servers accepting e-mail addresses for each domain.
document type definition	<i>See</i> DTD.
Domain Name System	<i>See</i> DNS.
DoS	Denial of service. A system security breach in which network services become unavailable to users.
DPD	Dead peer detection. Protocol that recognizes the loss of the primary IPsec IKE peer and establishes a secondary IPsec tunnel to a backup peer.
DRAM	Dynamic random-access memory. Storage source on the router that can be accessed quickly by a process.
drop probability	Percentage value expresses the likelihood that an individual packet will be dropped from the network. <i>See also</i> drop profile.
drop profile	Mechanism of random early detection (RED) that defines parameters that allow packets to be dropped from the network. When you configure drop profiles, there are two important values: the queue fullness and the drop probability. <i>See also</i> drop probability, queue fullness, RED.
DS0	Digital signal level 0. In T-carrier systems, a basic digital signaling rate of 64 Kbps. The DS0 rate forms the basis for the North American digital multiplex transmission hierarchy.

DS1	Digital signal level 1. In T-carrier systems, a digital signaling rate of 1.544 Mbps. A standard used in telecommunications to transmit voice and data between devices. Also known as T1. <i>See also</i> T1.
DS3	Digital signal level 3. In T-carrier systems, a digital signaling rate of 44.736 Mbps. This level of carrier can transport 28 DS1 level signals and 672 DS0 level channels within its payload. Also known as T3. <i>See also</i> T3.
DSAP	Destination service access point. Service access point (SAP) that identifies the destination for which a logical link control protocol data unit (LPDU) is intended.
DSCP	Differentiated Services code point or DiffServ code point. Values for a 6-bit field defined for IPv4 and IPv6 packet headers that can be used to enforce class-of-service (CoS) distinctions in routers.
DSU	Data service unit. A device used to connect a DTE to a digital phone line. DSU converts digital data from a router to voltages and encoding required by the phone line. <i>See also</i> CSU/DSU.
DTCP	Dynamic Tasking Control Protocol. A means of communicating filter requests and acknowledgments between one or more clients and a monitoring platform, used in dynamic flow capture (DFC) and flow-tap configurations. The protocol is defined in Internet draft draft-cavuto-dtcp-00.txt.
DTD	Document type definition. Defines the elements and structure of an Extensible Markup Language (XML) document or data set.
DTE	Data terminal equipment. An RS-232-C interface that a computer uses to exchange information with a serial device.
dual-core processor	Two process execution systems located on the same physical processor. The dual-core processor architecture enables faster computing speed and greater data throughput.
DVMRP	Distance Vector Multicast Routing Protocol. Distributed multicast routing protocol that dynamically generates IP multicast delivery trees using a technique called reverse-path multicasting (RPM) to forward multicast traffic to downstream interfaces.
DWDM	Dense wavelength-division multiplexing. Technology that enables data from different sources to be carried together on an optical fiber, with each signal carried on its own separate wavelength.
Dynamic Host Configuration Protocol	<i>See</i> DHCP.
dynamic label-switched path	MPLS network path established by signaling protocols such as RSVP and LDP.

Dynamic Tasking Control Protocol *See* DTCP.

E

E-carrier “E” stands for European. Standards that form part of the Synchronous Digital Hierarchy (SDH), in which groups of E1 circuits are bundled onto higher-capacity E3 links between telephone exchanges or countries. E-carrier standards are used just about everywhere in the world except North America and Japan, and are incompatible with the T-carrier standards.

E1 High-speed WAN digital communication protocol that operates at a rate of 2.048 Mbps.

E3 High-speed WAN digital communication protocol that operates at a rate of 34.368 Mbps and uses time-division multiplexing to carry 16 E1 circuits.

EAL3 Common Criteria Evaluation Assurance Level 3. Evaluation Assurance Level is an assurance and compliance requirement defined by Common Criteria. Higher levels have more stringent requirements. *See also* Common Criteria.

early packet discard *See* EPD.

EBGP External BGP. A BGP configuration in which sessions are established between routers in different autonomous systems (ASs).

ECC Error checking and correction. The process of detecting errors during the transmission or storage of digital data and correcting them automatically. This usually involves sending or storing extra bits of data according to specified algorithms.

ECSA Exchange Carriers Standards Association. A standards organization created after the divestiture of the Bell System to represent the interests of interexchange carriers.

edge router In MPLS, a router located at the beginning or end of a label-switching tunnel. An edge router at the beginning of a tunnel applies labels to new packets entering the tunnel. An edge route at the end of a tunnel removes labels from packets exiting the tunnel. *See also* MPLS.

editor macros (Emacs) Shortcut keystrokes used within the router’s command-line interface (CLI). These macros move the cursor and delete characters based on the sequence you specify.

EGP Exterior gateway protocol; for example, BGP.

egress router In MPLS, the last router in a label-switched path (LSP). *See also* ingress router.

EIA Electronic Industries Association. A United States trade group that represents manufacturers of electronic devices and sets standards and specifications.

EIA-530	Serial interface that employs the EIA-530 standard for the interconnection of DTE and DCE equipment.
EIR	Equipment identity register. A mobile network database that contains information about devices using the network.
electromagnetic interference	<i>See</i> EMI.
electrostatic discharge	<i>See</i> ESD.
embedded OS software	Software used by a Juniper Networks router to operate the physical router components.
EMI	Electromagnetic interference. Any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics or electrical equipment.
Encapsulating Security Payload	<i>See</i> ESP.
end system	In IS-IS, a network entity that sends and receives packets.
EPD	Early packet discard. For ATM2 interfaces only, a limit on the number of transmit packets that can be queued. Packets that exceed the limit are dropped. <i>See also</i> queue length.
ERO	Explicit Route Object. Extension to RSVP that allows an RSVP PATH message to traverse an explicit sequence of routers that is independent of conventional shortest-path IP routing.
error checking and correction	<i>See</i> ECC.
errored frame	Frame with one or more bits with errors. This frame will be dropped at the next Ethernet node and become a lost frame.
errored second	Period of a second with one or more errored or lost frames.
ES-IS	End System-to-Intermediate System. Protocol that resolves Layer 3 ISO network service access points (NSAPs) to Layer 2 addresses. ES-IS resolution is similar to the way ARP resolves Layer 2 addresses for IPv4.
ESD	Electrostatic discharge. Stored static electricity that can damage electronic equipment and impair electrical circuitry when released.

ESP	Encapsulating Security Payload. A protocol for securing packet flows for IPsec using encryption, data integrity checks, and sender authentication, which are added as a header to an IP packet. If an ESP packet is successfully decrypted, and no other party knows the secret key the peers share, the packet was not wiretapped in transit. <i>See also</i> AH.
Established	BGP neighbor state that represents a fully functional BGP peering session.
Ethernet	Local area network (LAN) technology used for transporting information from one location to another, formalized in the IEEE standard 802.3. Ethernet uses either coaxial cable or twisted-pair cable. Transmission speeds for data transfer range from the original 10 Mbps, to Fast Ethernet at 100 Mbps, to Gigabit Ethernet at 1000 Mbps.
ETSI	European Telecommunications Standardization Institute. A nonprofit organization that produces voluntary telecommunications standards used throughout Europe.
European Telecommunications Standardization Institute	<i>See</i> ETSI.
event policy process	<i>See</i> eventd.
eventd	Event policy process that performs configured actions in response to events on a routing platform that trigger system log messages.
exact	JUNOS software routing policy match type that represents only the route specified in a route filter.
exception packet	IP packet that is not processed by the normal packet flow through the Packet Forwarding Engine. Exception packets include local delivery information, expired TTL packets, and packets with an IP option specified.
Exchange	OSPF adjacency state in which two neighboring routers are actively sending database description packets to each other to exchange their database contents.
exclusive or	<i>See</i> XOR.
EXP bits	Experimental bits, also known as the class-of-service (CoS) bits, located in each MPLS label and used to encode the CoS value of a packet as it traverses an LSP.
explicit path	<i>See</i> signaled path.
Explicit Route Object	<i>See</i> ERO.
export	Placing of routes from the routing table into a routing protocol.

ExStart	OSPF adjacency state in which the neighboring routers negotiate to determine which router is in charge of the synchronization process.
Extensible Markup Language	<i>See</i> XML.
Extensible Stylesheet Language for Transformations	<i>See</i> XSLT.
exterior gateway protocol	<i>See</i> EGP.
external BGP	<i>See</i> EBGp.
external metric	Cost included in a route when OSPF exports route information from external autonomous systems. There are two types of external metrics: Type 1 and Type 2. Type 1 external metrics are equivalent to the link-state metric; that is, the cost of the route, used in the internal autonomous system. Type 2 external metrics are greater than the cost of any path internal to the autonomous system.

F

FA	Forwarding adjacency. RSVP LSP tunnel through which one or more other RSVP LSPs can be tunneled.
fabric schedulers	Identify a packet as high or low priority based on its forwarding class, and associate schedulers with the fabric priorities.
failover	Process by which a standby or secondary system component automatically takes over the functions of an active or primary component when the primary component fails or is temporarily shut down or removed for servicing. During failover, the system continues to perform normal operations with little or no interruption in service. <i>See also</i> GRES.
far-end alarm and control	<i>See</i> FEAC.
Fast Ethernet	Term encompassing a number of Ethernet standards that carry traffic at the nominal rate of 100 Mbps, instead of the original Ethernet speed of 10 Mbps. <i>See also</i> Ethernet, Gigabit Ethernet.
fast port	Fast Ethernet port on a J4300 Services Router, and either a Fast Ethernet port or DS3 port on a J6300 Services Router. Only enabled ports are counted. A two-port Fast Ethernet PIM with one enabled port counts as one fast port. The same PIM with both ports enabled counts as two fast ports.
fast reroute	Mechanism for automatically rerouting traffic on an LSP if a node or link in an LSP fails, thus reducing the loss of packets traveling over the LSP.

FBF	Filter-based forwarding. A filter that classifies packets to determine their forwarding path within a router. FBF is used to redirect traffic for analysis.
FCS	Frame check sequence. A calculation that is added to a frame for error control. FCS is used in HDLC, Frame Relay, and other data-link layer protocols.
FDDI	Fiber Distributed Data Interface. A set of ANSI protocols for sending digital data over fiber-optic cable. FDDI networks are token-passing networks, and support data rates of up to 100 Mbps (100 million bits). FDDI networks are typically used as backbones for wide area networks.
FEAC	Far-end alarm and control. A T3 signal used to send alarm or status information from the far-end terminal back to the near-end terminal, and to initiate T3 loopbacks at the far-end terminal from the near-end terminal.
FEB	Forwarding Engine Board. In M5 and M10 routers, provides route lookup, filtering, and switching to the destination port.
FEC	Forwarding equivalence class. Criterion used to forward a set of packets, with similar or identical characteristics, using the same MPLS label. Forwarding equivalence classes are defined in the base LDP specification and can be extended through the use of additional parameters. FECs are also represented in other label distribution protocols.
FECN	Forward explicit congestion notification. In a Frame Relay network, a header bit transmitted by the source device requesting that the destination device slow down its requests for data. FECN and BECN minimize the possibility that packets will be discarded when more packets arrive than can be handled. <i>See also</i> BECN.
Federal Information Processing Standards	<i>See</i> FIPS.
Fiber Distributed Data Interface	<i>See</i> FDDI.
field-replaceable unit	<i>See</i> FRU.
FIFO	First in, first out. Scheduling method in which the first data packet stored in the queue is the first data packet removed from the queue. All JUNOS software interface queues operate in this mode by default.
File Transfer Protocol	<i>See</i> FTP.
filter	Process or device that screens packets based on certain characteristics, such as source address, destination address, or protocol, and forwards or discards packets that match the filter. Filters are used to control data packets or local packets. <i>See also</i> packet.

filter-based forwarding	<i>See</i> FBF.
FIPS	Federal Information Processing Standards. Defines, among other things, security levels for computer and networking equipment. FIPS is usually applied to military environments.
firewall	Security gateway positioned between two networks, usually between a trusted network and the Internet. A firewall ensures that all traffic that crosses it conforms to the organization's security policy. Firewalls track and control communications, deciding whether to pass, reject, discard, encrypt, or log them. Firewalls also can be used to secure sensitive portions of a local network.
firewall filter	<i>See</i> stateful firewall filter, stateless firewall filter.
firmware	Instructions and data programmed directly into the circuitry of a hardware device for the purpose of controlling the device. Firmware is used for vital programs that must not be lost when the device is powered off.
first in, first out	<i>See</i> FIFO.
flap damping	<i>See</i> damping.
flapping	<i>See</i> route flapping.
flexible bandwidth allocation	<i>See</i> bandwidth on demand.
Flexible PIC Concentrator	<i>See</i> FPC.
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.
flood and prune	Method of forwarding multicast data packets in a dense-mode network. Flooding and pruning occur every 3 minutes.
flow	Stream of routing information and packets that are handled by the Routing Engine and the Packet Forwarding Engine. The Routing Engine handles the flow of routing information between the routing protocols and the routing tables and between the routing tables and the forwarding tables, as well as the flow of local packets from the router physical interfaces to the Routing Engine. The Packet Forwarding Engine handles the flow of data packets into and out of the router physical interfaces.
flow collection interface	Interface that combines multiple cflowd records into a compressed ASCII data file and exports the file to an FTP server for storage and analysis, allowing users to manipulate the output from traffic monitoring operations.

flow control action	JUNOS software syntax used in a routing policy or firewall filter. It alters the default logical processing of the policy or filter when a set of match conditions is met.
flow monitoring	Application that monitors the flow of traffic and enables lawful interception of packets transiting between two routers. Traffic flows can be passively monitored by an offline router or actively monitored by a router participating in the network.
flow-tap application	Application that uses Dynamic Tasking Control Protocol (DTCP) requests to intercept IPv4 packets in an active monitoring router and send a copy of packets that match filter criteria to one or more content destinations. Flow-tap configurations can be used in flexible trend analysis for detecting new security threats and lawfully intercepting data.
forward explicit congestion notification	<i>See</i> FECN.
forwarding adjacency	<i>See</i> FA.
forwarding classes	Defined set of classes that are associated with each received packet on a router. These classes affect the forwarding, scheduling, and marking policies applied as the packet transits a routing platform. The forwarding class plus the loss priority define the per-hop behavior. Also known as <i>ordered aggregates</i> in the IETF Differentiated Services architecture.
Forwarding Engine Board	<i>See</i> FEB.
forwarding equivalence class	<i>See</i> FEC.
forwarding information base	<i>See</i> forwarding table.
forwarding table	JUNOS software forwarding information base. The JUNOS routing protocol process installs active routes from its routing tables into the Routing Engine forwarding table. The kernel copies this forwarding table into the Packet Forwarding Engine, which determines which interface transmits the packets.
FPC	Flexible PIC Concentrator. An interface concentrator on which PICs are mounted. An FPC is inserted into a slot in a Juniper Networks router. <i>See also</i> PIC.
fractional E1	Interface that contains one or more of the 32 DS0 time slots that can be reserved from an E1 interface. (The first time slot is reserved for framing.)

fractional interface	Interface that contains one or more DS0 time slots reserved from an E1 or T1 interface. Fractional interfaces allow service providers to provision part of an E1 or T1 interface to one customer and the other part to another customer. The individual fractional interfaces connect to different destinations, and customers pay for only the bandwidth fraction used and not for the entire E1 or T1 interface. Fractional interfaces can be configured on both channelized PICs and PIMs and unchannelized, regular E1 and T1 PICs and PIMs.
fractional T1	Interface that contains one or more of the 24 DS0 time slots that can be reserved from a T1 interface.
fragmentation	In TCP/IP, the process of breaking packets into the smallest maximum size packet data unit (PDU) supported by any of the underlying networks. In the Open Systems Interconnection (OSI) reference model, this process is known as segmentation. For JUNOS applications, split Layer 3 packets can then be encapsulated in MLFR or MLPPP for transport.
frame check sequence	<i>See</i> FCS.
Frame Relay	Efficient replacement for the older X.25 protocol that does not require explicit acknowledgment of each frame of data. Frame Relay allows private networks to reduce costs by using shared facilities between the end-point switches of a network managed by a Frame Relay service provider. Individual data-link connection identifiers (DLCIs) are assigned to ensure that each customer receives only its own traffic.
frequency-division multiplexed channel	Signals carried at different frequencies and transmitted over a single wire or wireless medium.
FRF	Frame Relay Forum. A technical committee that promotes Frame Relay by negotiating agreements and developing standards.
FRF.15	End-to-end Frame Relay Implementation Agreement. An implementation of MLFR using multiple virtual connections to aggregate logical bandwidth for end-to-end Frame Relay. Released by the Frame Relay Forum.
FRF.16	Multilink Frame Relay Implementation Agreement. An implementation of MLFR in which a single logical connection is provided by multiplexing multiple physical interfaces for user-to-network interface and network-to-network interface (UNI/NNI) connections. Released by the Frame Relay Forum.
FRU	Field-replaceable unit. A router component that customers can replace onsite.
FTP	File Transfer Protocol. Application protocol that is part of the TCP/IP protocol stack. Used for transferring files between network nodes. FTP is defined in RFC 959.
Full	OSPF adjacency state that represents a fully functional neighbor relationship.

fxp0	<i>See</i> management Ethernet interface.
fxp1	JUNOS software permanent interface used for communications between the Routing Engine and the Packet Forwarding Engine. This interface is not present in all routers.
fxp2	JUNOS software permanent interface used for communications between the Routing Engine and the Packet Forwarding Engine. This interface is not present in all routers.

G

G-CDR	GGSN call detail record. Collection of charges in ASN.1 format that is eventually billed to a mobile station user.
G.992.1	<i>See</i> ITU-T Rec. G.992.1.
G.SHDSL	Symmetric high-speed digital subscriber line (SHDSL). Standard published in 2001 by the ITU-T with recommendation ITU G.991.2 G.SHDSL. G.SHDSL incorporates features of other DSL technologies such as asymmetrical DSL (ADSL). <i>See also</i> SHDSL, ADSL.
Garbage Collection Timer	Timer used in a distance-vector network that represents the time remaining before a route is removed from the routing table.
Generalized Multiprotocol Label Switching	<i>See</i> GMPLS.
generated route	Summary route that uses an IP address next hop to forward packets in an IP network. A generated route is functionally similar to an aggregated route.
generic routing encapsulation	<i>See</i> GRE.
GGSN	Gateway GPRS support node. A router that serves as a gateway between mobile networks and packet data networks.
Gigabit Ethernet	Term describing various technologies for implementing Ethernet networking at a nominal speed of one gigabit per second. Gigabit Ethernet is supported over both optical fiber and twisted-pair cable. Physical layer standards include 1000BASE-T, 1 Gbps over CAT-5e copper cabling, and 1000BASE-SX for short to medium distances over fiber. <i>See also</i> Ethernet, Fast Ethernet.
Global System for Mobile Communications	<i>See</i> GSM.

GMPLS	Generalized Multiprotocol Label Switching. A protocol that extends the functionality of MPLS to include a wider range of label-switched path (LSP) options for a variety of network devices.
GMT	<i>See</i> UTC.
GPRS	General Packet Radio System. A packet-switched service that allows full mobility and wide-area coverage as information is sent and received across a mobile network.
graceful restart	Process that allows a router whose control plane is undergoing a restart to continue to forward traffic while recovering its state from neighboring routers. Without graceful restart, a control plane restart disrupts services provided by the router.
graceful Routing Engine switchover	<i>See</i> GRES.
graceful switchover	JUNOS software feature that allows a change from the primary device, such as a Routing Engine, to the backup device without interruption of packet forwarding.
gratuitous ARP	Broadcast request for a router's own IP address to check whether that address is being used by another node. Primarily used to detect IP address duplication.
GRE	Generic routing encapsulation. A general tunneling protocol that can encapsulate many types of packets to enable data transmission through a tunnel. GRE is used with IP to create a virtual point-to-point link to routers at remote points in a network. <i>See also</i> tunneling protocol.
GRES	Graceful Routing Engine switchover. In a router that contains a master and a backup Routing Engine, allows the backup Routing Engine to assume mastership automatically, with no disruption of packet forwarding.
group	Collection of related BGP peers.
group address	IP address used as the destination address in a multicast IP packet. The group address functionally represents the senders and interested receivers for a particular multicast data stream.
GSM	Global System for Mobile Communications. A second-generation (2G) mobile wireless networking standard defined by ETSI that uses TDMA technology and operates in the 900-MHz radio band. <i>See also</i> TDMA.
GTP	GPRS tunneling protocol. A protocol that transports IP packets between an SGSN and a GGSN. <i>See also</i> tunneling protocol.
GTP-C	GGSN tunneling protocol, control. A protocol that allows an SGSN to establish packet data network access for a mobile station. <i>See also</i> tunneling protocol.

GTP-U GGSN tunneling protocol, user plane. A protocol that carries mobile station user data packets. *See also* tunneling protocol.

H

Hashed Message Authentication Code *See* HMAC.

hashing Cryptographic technique applied over and over (iteratively) to a message of arbitrary length to produce a hash “message digest” or “signature” of fixed length that is appended to the message when it is sent. In security, used to validate that the contents of a message have not been altered in transit. The Secure Hash Algorithm (SHA-1) and Message Digest 5 (MD5) are commonly used hashes. *See also* SHA-1, MD5.

HDLC High-Level Data Link Control. An International Telecommunication Union (ITU) standard for a bit-oriented data-link layer protocol on which most other bit-oriented protocols are based.

health monitor JUNOS software extension to the RMON alarm system that provides predefined monitoring for file system, CPU, and memory usage. The health monitor also supports unknown or dynamic object instances such as JUNOS processes.

hello interval Amount of time an OSPF router continues to send a hello packet to each adjacent neighbor.

hello mechanism Process used by an RSVP router to enhance the detection of network outages in an MPLS network.

HLR Home Location Register. Database containing information about a subscriber and the current location of a subscriber’s mobile station.

HMAC Hashed Message Authentication Code. A mechanism for message authentication that uses cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function—for example, MD5 or SHA-1—in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function. Defined in RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*.

hold down Timer used by distance-vector protocols to prevent the propagation of incorrect routing knowledge to other routers in the network.

hold time Maximum number of seconds allowed to elapse between successive keepalive or update messages that a BGP system receives from a peer.

host membership query Internet Group Management Protocol (IGMP) packet sent by a router to determine whether interested receivers exist on a broadcast network for multicast traffic.

host membership report	Internet Group Management Protocol (IGMP) packet sent by an interested receiver for a particular multicast group address. Hosts send report messages when they first join a group or in response to a query packet from the local router.
host module	On an M160 router, provides the routing and system management functions of the router. Consists of the Routing Engine and Miscellaneous Control Subsystem (MCS).
host subsystem	On a T640 routing node, provides the routing and system management functions of the router. Consists of a Routing Engine and an adjacent Control Board (CB).
hot standby	In JUNOS, method used with link services intelligent queuing interfaces (LSQ) to enable rapid switchover between primary and secondary (backup) PICs. <i>See also</i> warm standby.
HSCSD	High-Speed Circuit Switched Data. Circuit-switched wireless data transmission for mobile users, at data rates up to 38.4 Kbps.
HTTP	Hypertext Transfer Protocol. Method used to publish and receive information on the Web, such as text and graphic files.
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer. Similar to HTTP with an added encryption layer that encrypts and decrypts user page requests and pages that are returned by a Web server. Used for secure communication, such as payment transactions.
Hypertext Transfer Protocol	<i>See</i> HTTP.
Hypertext Transfer Protocol over Secure Sockets Layer	<i>See</i> HTTPS.
I	
I-frame	Information frame used to transfer data in sequentially numbered logical link control protocol data units (LPDUs) between link stations.
I-SID	24-bit service instance identifier field carried inside an I-TAG. The I-SID defines the service instance to which the frame is mapped.
I-TAG	A field defined in the IEEE 802.1ah provider MAC encapsulation header that carries the service instance information (I-SID) associated with the frame.
I/O Manager ASIC	Juniper Networks ASIC responsible for segmenting data packets into 64-byte J-cells and for queuing result cells before transmission.

IANA	Internet Assigned Numbers Authority. A regulatory group that maintains all assigned and registered Internet numbers, such as IP and multicast addresses. <i>See also</i> NIC.
IBGP	Internal BGP. A BGP configuration in which sessions are established between routers in the same autonomous system (AS).
ICMP	Internet Control Message Protocol. Used in router discovery, ICMP allows router advertisements that enable a host to discover addresses of operating routers on the subnet.
ICMP Router Discovery Protocol	<i>See</i> IRDP.
IDE	Integrated Drive Electronics. Type of hard disk on a Routing Engine.
IDEA	International Data Encryption Algorithm. An algorithm that uses a 128-bit key and is one of the methods at the heart of Pretty Good Privacy (PGP). IDEA is patented by Ascom Tech AG and is popular in Europe.
Idle	Initial BGP neighbor state in which the local router refuses all incoming session requests.
IDS	Intrusion detection service. A service that inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
IEC	International Electrotechnical Commission. <i>See</i> ISO.
IEEE	Institute of Electrical and Electronics Engineers. An international professional society for electrical engineers.
IETF	Internet Engineering Task Force. An international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
IFD	(A Juniper Networks internal use acronym.) <i>See</i> physical interface.
IFF	(A Juniper Networks internal use acronym.) <i>See</i> protocol families.
IFL	(A Juniper Networks internal use acronym.) <i>See</i> logical interface.
IGMP	Internet Group Management Protocol. A host-to-router signaling protocol for IPv4, used to determine whether group members are present during IP multicasting.
IGP	Interior gateway protocol, such as IS-IS, OSPF, or RIP.

IKE	Internet Key Exchange. Part of IPsec that provides ways to securely negotiate the shared private keys that the AH and ESP portions of IPsec need to function properly. IKE employs Diffie-Hellman methods and is optional in IPsec (the shared keys can be entered manually at the endpoints).
ILMI	Integrated Local Management Interface. A specification developed by the ATM Forum that incorporates network management capabilities into the ATM user-to-network interface (UNI) and provides bidirectional exchange of management information between UNI management entities (UMEs).
IMEI	International Mobile Station Equipment Identity. A unique code used to identify an individual mobile station to a GSM network.
import	Installation of routes from the routing protocols into a routing table.
IMSI	International Mobile Subscriber Identity. Information that identifies a particular subscriber to a GSM network.
IMT-2000	International Mobile Telecommunications 2000. Global standard for third-generation (3G) wireless communications, defined by a set of interdependent ITU Recommendations. IMT-2000 provides a framework for worldwide wireless access by linking the diverse systems of terrestrial and satellite-based networks.
inet.0	Default JUNOS software routing table for IPv4 unicast routers.
inet.1	Default JUNOS software routing table for storing the multicast cache for active data streams in the network.
inet.2	Default JUNOS software routing table for storing unicast IPv4 routes specifically used to prevent forwarding loops in a multicast network.
inet.3	Default JUNOS software routing table for storing the egress IP address of an MPLS label-switched path.
inet.4	Default JUNOS software routing table for storing information generated by the Multicast Source Discovery Protocol (MSDP).
inet6.0	Default JUNOS software routing table for storing unicast IPv6 routes.
infinity metric	Metric value used in distance-vector protocols to represent an unusable route. For RIP, the infinity metric is 16.
ingress router	In MPLS, the first router in a label-switched path (LSP). <i>See also</i> egress router.
Init	OSPF adjacency state in which the local router has received a hello packet but bidirectional communication is not yet established.

insert	JUNOS software command that allows a user to reorder terms in a routing policy or a firewall filter, or change the order of a policy chain.
instance.inetflow.0	Routing table that shows route flows through BGP.
integrated bridging and routing	<i>See</i> IBR.
Integrated Drive Electronics	<i>See</i> IDE.
Integrated Local Management Interface	<i>See</i> ILMI.
Integrated Services Digital Network	<i>See</i> ISDN.
intelligent queuing	<i>See</i> IQ.
inter-AS routing	Routing of packets among different autonomous systems (ASs). <i>See also</i> EBGp.
intercluster reflection	In a BGP route reflection, the redistribution of routing information by a route reflector system to all nonclient peers (BGP peers not in the cluster). <i>See also</i> route reflection.
interface cost	Value added to all received routes in a distance-vector network before they are placed into the routing table. The JUNOS software uses a cost of 1 for this value.
interface preservation	<i>See</i> link state replication.
interface routes	Routes that are in the routing table because an interface has been configured with an IP address. Also called <i>direct routes</i> .
intermediate system	In IS-IS, the network entity that sends and receives packets and can also route packets.
internal BGP	<i>See</i> IBGP.
International Data Encryption Algorithm	<i>See</i> IDEA.
International Mobile Station Equipment Identity	<i>See</i> IMEI.
International Mobile Subscriber Identity	<i>See</i> IMSI.
International Mobile Telecommunications-2000	<i>See</i> IMT-2000.

International Organization for Standardization	<i>See</i> ISO.
International Telecommunication Union	<i>See</i> ITU-T.
Internet Assigned Numbers Authority	<i>See</i> IANA.
Internet Control Message Protocol	<i>See</i> ICMP.
Internet Engineering Task Force	<i>See</i> IETF.
Internet Group Management Protocol	<i>See</i> IGMP.
Internet Key Exchange	<i>See</i> IKE.
Internet Processor ASIC	Juniper Networks ASIC responsible for using the forwarding table to make routing decisions within the Packet Forwarding Engine. The Internet Processor ASIC also implements firewall filters.
Internet Protocol	<i>See</i> IP.
Internet Security Association and Key Management Protocol	<i>See</i> ISAKMP.
Internet service provider	<i>See</i> ISP.
interprovider VPN	VPN that provides connectivity between separate autonomous systems (ASs) with separate border edge routers. It is used by VPN customers who have connections to several different ISPs, or different connections to the same ISP in different geographic regions, each of which has a different AS.
intra-AS routing	Routing of packets within a single autonomous system (AS). <i>See also</i> IBGP.
intrusion detection service	<i>See</i> IDS.
IP	Internet Protocol. The protocol used for sending data from one point to another on the Internet.
IP Control Protocol	<i>See</i> IPCP.

IP Security *See* IPsec.

IP television *See* IPTV.

IPCP IP Control Protocol. Protocol that establishes and configures IP over the Point-to-Point Protocol (PPP).

IPsec IP Security. A standard way to add security to Internet communications. The secure aspects of IPsec are usually implemented in three parts: the authentication header (AH), the Encapsulating Security Payload (ESP), and the Internet Key Exchange (IKE).

IPTV IP television. A system using the Internet protocol to deliver digital television service over a network.

IQ Intelligent queuing. M-series and T-series routing platform interfaces that offer granular quality-of-service (QoS) capabilities; extensive statistics on packets and bytes that are transmitted, received, or dropped; and embedded diagnostic tools.

IRB Integrated bridging and routing. IRB provides simultaneous support for Layer 2 (L2) bridging and Layer 3 (L3) routing within the same bridge domain. Packets arriving on an interface of the bridge domain are L2 switched or L3 routed based on the destination MAC address. Packets addressed to the router's MAC address are routed to other L3 interfaces.

IRDP ICMP Router Discovery Protocol. A protocol that enables a host to determine the address of a router that it can use as a default gateway.

IS-IS Intermediate System-to-Intermediate System. A link-state, interior gateway routing protocol for IP networks that uses the shortest-path-first (SPF) algorithm to determine routes.

ISAKMP Internet Security Association and Key Management Protocol. A protocol that allows the receiver of a message to obtain a public key and use digital certificates to authenticate the sender's identity. ISAKMP is key exchange independent; that is, it supports many different key exchanges. *See also* IKE, Oakley.

ISDN Integrated Services Digital Network. A set of digital communications standards that enable the transmission of information over existing twisted-pair telephone lines at higher speeds than standard analog telephone service. An ISDN interface provides multiple B-channels (bearer channels) for data and one D-channel for control and signaling information. *See also* B-channel, D-channel.

ISO International Organization for Standardization. A worldwide federation of standards bodies that promotes international standardization and publishes international agreements as International Standards.

ISP	Internet service provider. Company that provides access to the Internet and related services.
ITU-T	International Telecommunication Union Telecommunication Standardization (formerly known as the CCITT). Group supported by the United Nations that makes recommendations and coordinates the development of telecommunications standards for the entire world.
ITU-T Rec. G.992.1	International standard that defines ADSL. Annex A defines how ADSL works over twisted-pair copper (POTS) lines. Annex B defines how ADSL works over ISDN lines.

J

J-cell	A 64-byte data unit used within the Packet Forwarding Engine. All IP packets processed by a Juniper Networks router are segmented into J-cells.
J-Web	Graphical Web browser interface to the JUNOS Internet software on routing platforms. With the J-Web interface, you can monitor, configure, diagnose, and manage the routing platform from a PC or laptop that has Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS) enabled.
jbase	JUNOS software package containing updates to the kernel.
jbundle	JUNOS software package containing all possible software package files.
JCS	<i>See</i> Juniper Control System.
JCS management module (MM)	Chassis management hardware and software used to access and configure the Juniper Control System (JCS) platform.
JCS switch module	Hardware device that connects Routing Engines in the Juniper Control System (JCS) chassis to a Juniper Networks router and controls traffic between the two devices. For redundancy, the JCS chassis can include two JCS switch modules.
jdocs	JUNOS software package containing the documentation set.
jitter	Small random variation introduced into the value of a timer to prevent multiple timer expirations from becoming synchronized. In real-time applications such as VoIP and video, variation in the rate at which packets in a stream are received that can cause quality degradation.
jkernel	JUNOS software package containing the basic components of the software.
Join message	PIM message sent hop by hop upstream toward a multicast source or the RP of the domain. It requests that multicast traffic be sent downstream to the router originating the message.

jpfe JUNOS software package containing the embedded OS software for operating the Packet Forwarding Engine.

jroute JUNOS software package containing the software used by the Routing Engine.

Juniper Control System (JCS) OEM blade server customized to work with Juniper Networks routers. The JCS chassis holds up to 12 single Routing Engines (or 6 redundant Routing Engine pairs). The JCS 1200 chassis enables the control plane and forwarding plane of a single interconnected platform to be scaled independently.

K

keepalive message Message sent between network devices to inform each other that they are still active.

kernel Basic software component of the JUNOS software. The kernel operates the various processes used to control the router's operations.

kernel forwarding table *See* forwarding table.

key management process *See* kmd.

kmd Key management process that provides IPsec authentication services for encryption PICs.

L

L2TP Layer 2 Tunneling Protocol. A procedure for secure communication of data across a Layer 2 network that enables users to establish PPP sessions between tunnel endpoints. L2TP uses profiles for individual user and group access to ensure secure communication that is as transparent as possible to both end users and applications. *See also* tunneling protocol.

label In MPLS, a 20-bit unsigned integer from 0 through 1,048,575, used to identify a packet traveling along an LSP.

Label Distribution Protocol *See* LDP.

label object RSVP message object that contains the label value allocated to the next downstream router.

label pop operation Function performed by an MPLS router in which the top label in a label stack is removed from the data packet.

label push operation Function performed by an MPLS router in which a new label is added to the top of the data packet.

label request object	RSVP message object that requests each router along the path of an LSP to allocate a label for forwarding.
label swap operation	Function performed by an MPLS router in which the top label in a label stack is replaced with a new label before the data packet is forwarded to the next-hop router.
label switching	<i>See</i> MPLS.
label values	20-bit field in an MPLS header used by routers to forward data traffic along an MPLS label-switched path.
label-switched interface	<i>See</i> LSI.
label-switched path	<i>See</i> LSP.
label-switching router	<i>See</i> LSR.
LAN PHY	Local Area Network Physical Layer Device. A physical layer device that allows 10-Gigabit Ethernet wide area links to use existing Ethernet applications. <i>See also</i> PHY and WAN PHY.
Layer 2 circuits	Collection of transport modes that accept a stream of ATM cells, convert them to an encapsulated Layer 2 format, then tunnel them over an MPLS or IP backbone, where a similarly configured routing platform segments these packets back into a stream of ATM cells, to be forwarded to the virtual circuit configured for the far-end routing platform. Layer 2 circuits are designed to transport Layer 2 frames between provider edge (PE) routing platforms across a Label Distribution Protocol (LDP)-signaled MPLS backbone. <i>See also</i> AAL5 mode, cell-relay mode, standard AAL5 mode, trunk mode.
Layer 2 Tunneling Protocol	<i>See</i> L2TP.
Layer 2 VPN	Provides a private network service among a set of customer sites using a service provider's existing MPLS and IP network. A customer's data is separated from other data using software rather than hardware. In a Layer 2 VPN, the Layer 3 routing of customer traffic occurs within the customer's network.
Layer 3 VPN	Provides a private network service among a set of customer sites using a service provider's existing MPLS and IP network. A customer's routes and data are separated from other routes and data using software rather than hardware. In a Layer 3 VPN, the Layer 3 routing of customer traffic occurs within the service provider's network.
LCC	Line-card chassis. Term used by the JUNOS command-line interface (CLI) to refer to a T640 routing node in a routing matrix.
LCP	Link Control Protocol. A traffic controller used to establish, configure, and test data-link connections for the Point-to-Point Protocol (PPP).

LDAP	Lightweight Directory Access Protocol. Software protocol used for locating resources on a public or private network.
LDP	Label Distribution Protocol. A protocol for distributing labels in non-traffic-engineered applications. LDP allows routers to establish label-switched paths (LSPs) through a network by mapping network-layer routing information directly to data-link layer switched paths.
leaf node	Terminating node of a multicast distribution tree. A router that is a leaf node only has receivers and does not forward multicast packets to other routers.
learning domain	MAC address database where MAC addresses are added based on the normalized VLAN tags.
LFI	Link fragmentation and interleaving. A method that reduces excessive delays by fragmenting long packets into smaller packets and interleaving them with real-time frames. For example, short delay-sensitive packets, such as packetized voice, can race ahead of larger delay-insensitive packets, such as common data packets.
LFM	Link fault management. A method used to detect problems on links and spans on an Ethernet network defined in IEEE 802.3ah. <i>See also</i> OAM.
liblicense	Library that includes messages generated for routines for software license management.
libpcap	Implementation of the pcap application programming interface. libpcap is used by a program to capture packets traveling over a network. <i>See also</i> pcap.
Lightweight Directory Access Protocol	<i>See</i> LDAP.
limited operational environment	Term used to describe the restrictions placed on FIPS-certified equipment. <i>See</i> FIPS.
line loopback	Method of troubleshooting a problem with physical transmission media in which a transmission device in the network sends the data signal back to the originating router.
line-card chassis	<i>See</i> LCC.
link	Communication path between two neighbors. A link is up when communication is possible between the two end points.
Link Control Protocol	<i>See</i> LCP.
link fault management	<i>See</i> LFM.

link fragmentation and interleaving	<i>See</i> LFI.
Link Management Protocol	<i>See</i> LMP.
link protection	Method of establishing bypass label-switched paths (LSPs) to ensure that traffic going over a specific interface to a neighboring router can continue to reach the router if that interface fails. The bypass LSP uses a different interface and path to reach the same destination.
link services intelligent queuing interfaces	<i>See</i> LSQ.
link-state acknowledgement	OSPF data packet used to inform a neighbor that a link-state update packet has been successfully received.
link-state advertisement	<i>See</i> LSA.
link-state database	All routing knowledge in a link-state network is contained in this database. Each router runs the SPF algorithm against this database to locate the best network path to each destination in the network.
link-state PDU	Packet that contains information about the state of adjacencies to neighboring systems.
link-state replication	Addition to the SONET Automatic Protection Switching (APS) functionality that helps promote redundancy of the link PICs used in LSQ configurations. If the active SONET PIC fails, links from the standby PIC are used without causing a link renegotiation. Also called <i>interface preservation</i> .
link-state request list	List generated by an OSPF router during the exchange of database information while forming an adjacency. Advertised information by a neighbor that the local router does not contain is placed in this list.
link-state request packet	OSPF data packet used by a router to request database information from a neighboring router.
link-state update	OSPF data packet that contains one of multiple LSAs. It is used to advertise routing knowledge into the network.
linktrace message	<i>See</i> LTM.

Linktrace Protocol	Protocol used for path discovery between a pair of maintenance points. Linktrace messages are triggered by an administrator using the traceroute command to verify the path between a pair of maintenance end points (MEPs) under the same maintenance association. Linktrace messages can also be used to verify the path between an MEP and a maintenance intermediate point (MIP) under the same maintenance domain. The operation of IEEE 802.1ag linktrace request and response messages is similar to the operation of Layer 3 traceroute commands.
linktrace response	<i>See</i> LTR.
LLC	Logical link control. Data-link layer protocol used on a LAN. LLC1 provides connectionless data transfer, and LLC2 provides connection-oriented data transfer.
LLC frame	Unit of data that contains specific information about the LLC layer and identifies line protocols associated with the layer. <i>See also</i> LLC.
LMI	Local Management Interface. Enhancements to the basic Frame Relay specifications, providing support for the following: <ul style="list-style-type: none"> ■ A keepalive mechanism that verifies the flow of data ■ A multicast mechanism that provides a network server with a local DLCI and multicast DLCI ■ In Frame Relay networks, global addressing that gives DLCIs global instead of local significance ■ A status mechanism that provides a switch with ongoing status reports on known DLCIs
LMP	Link Management Protocol. Part of GMPLS, a protocol used to define a forwarding adjacency between peers and to maintain and allocate resources on the traffic engineering links.
lo0	<i>See</i> loopback interface (lo0).
load balancing	Process that installs all next-hop destinations for an active route in the forwarding table. You can use load balancing across multiple paths between routers. The behavior of load balancing depends on the version of the Internet Processor ASIC in the router. Also called <i>per-packet load balancing</i> .
loading	OSPF adjacency state in which the local router sends link-state request packets to its neighbor and waits for the appropriate link-state updates from that neighbor.
Local Management Interface	<i>See</i> LMI.
local packet	Chunk of data destined for or sent by the Routing Engine.

local preference	Optional BGP path attribute carried in internal BGP update packets that indicates the degree of preference for an external route.
local RIB	Logical software table that contains BGP routes used by the local router to forward data packets.
local significance	Concept used in an MPLS network where the label values are unique only between two neighbor routers.
logical interface	On a physical interface, the configuration of one or more units which include all addressing, protocol information, and other logical interface properties that enable the physical interface to function.
logical link control	<i>See</i> LLC.
logical operator	Characters used in a firewall filter to represent a Boolean AND or OR operation.
logical router	<i>See</i> logical system.
logical system	Logical routing device that is partitioned from an M-series or T-series routing platform. Each logical system independently performs a subset of the tasks performed by the main router and has a unique routing table, interfaces, policies, and routing instances.
longer	JUNOS software routing policy match type that represents all routes more specific than the given subnet, but not the given subnet itself. It is similar to a mathematical greater-than operation.
loopback interface (lo0)	Interface that is always available because it is independent of any physical interfaces. When configured with an address, the loopback interface is the default address for the routing platform and any unnumbered interfaces. <i>See also</i> unnumbered interface.
loose hop	In the context of traffic engineering, a path that can use any router or any number of other intermediate (transit) points to reach the next address in the path. (Definition from RFC 791, modified to fit LSPs.)
loss-priority map	Maps the loss priority of incoming packets based on code point values.
lower-speed IQ interfaces	E1, NxDS0, and T1 interfaces configured on an IQ PIC.
LPDU	LLC protocol data unit. LLC frame on a DLSw network. <i>See</i> LLC frame.
LSA	Link-state advertisement. OSPF data structure that is advertised in a link-state update packet. Each LSA uniquely describes a portion of the OSPF network.

LSI	Label-switched interface. A logical interface supported by the JUNOS software that provides VPN services (such as VPLS and Layer 3 VPNs) normally provided by a Tunnel Services PIC.
LSP	Label-switched path. Sequence of routers that cooperatively perform MPLS operations for a packet stream. The first router in an LSP is called the ingress router, and the last router in the path is called the egress router. An LSP is a point-to-point, half-duplex connection from the ingress router to the egress router. (The ingress and egress routers cannot be the same router.) <i>See</i> link-state PDU.
LSQ	Link services intelligent queuing interfaces. Interfaces configured on the Adaptive Services PIC or ASM that support MLPPP and MLFR traffic and also fully support JUNOS class-of-service (CoS) components.
LSR	Label-switching router. A router on which MPLS is enabled and that can process label-switched packets.
LTM	Linktrace message. Message used by one MEP to trace the path to another maintenance end point (MEP) or maintenance intermediate point (MIP) in the same domain. It is needed for loopback (ping). All intermediate MIPs respond back with a linktrace response to the originating MEP. After decreasing the TTL by one, intermediate MIPs forward the linktrace message until the destination MIP/MEP is reached. If the destination is a MEP, every MIP along a given maintenance association responds to the originating MEP. The originating MEP can then determine the MAC address of all MIPs along the maintenance association and their precise location with respect to the originating MEP.
LTR	Linktrace response. <i>See</i> LTM.

M

MAC	Media access control. In the OSI seven-layer networking model defined by the IEEE, MAC is the lower sublayer of the data link layer. The MAC sublayer governs protocol access to the physical network medium. By using the MAC addresses that are assigned to all ports on a router, multiple devices on the same physical link can uniquely identify one another at the data link layer. <i>See also</i> MAC address.
MAC address	Serial number permanently stored in a device adapter to uniquely identify the device. <i>See also</i> MAC.
maintenance association	Combined set of nodes (MEPs and MIPs) within a maintenance domain. <i>See also</i> LTR.
maintenance association end point	<i>See</i> MEP.
maintenance association ID	ID associated with the maintenance association.

maintenance association intermediate point	<i>See</i> MIP.
maintenance domain	Part of the network where connectivity fault detection is performed.
maintenance point	<i>See</i> MP.
MAM	Maximum allocation bandwidth constraints model. In Differentiated Services-aware traffic engineering, a constraint model that divides the available bandwidth among the different classes. Sharing of bandwidth among the class types is not allowed.
management daemon	<i>See</i> mgd.
management Ethernet interface	Permanent interface that provides an out-of-band method, such as SSH and telnet, to connect to the routing platform. SNMP can use the management interface to gather statistics from the routing platform. Called fxp0 on some routing platforms. <i>See also</i> permanent interface.
Management Information Base	<i>See</i> MIB.
Management Module, JCS	<i>See</i> JCS Management Module.
mapping agent	Router used in an auto-RP multicast network to select the rendezvous point for all multicast group addresses. The rendezvous point is then advertised to all other routers in the domain.
martian address	Network address about which all information is ignored.
martian route	Network routes about which all information is ignored. The JUNOS software does not allow martian routes in the inet.0 routing table.
MAS	Mobile network access subsystem. A GSN application subsystem that contains the access server.
mask	<i>See</i> subnet mask.
master	Router in control of the OSPF database exchange during an adjacency formation.
match	Logical concept used in a routing policy or firewall filter. A match denotes the criteria used to find a route or IP packet before an action is performed.
match type	JUNOS software syntax used in a route filter to better describe the routes that should match the policy term.

maximum allocation bandwidth constraints model	<i>See</i> MAM.
maximum received reconstructed unit	<i>See</i> MRRU.
maximum transmission unit	<i>See</i> MTU.
MBGP	Multiprotocol Border Gateway Protocol. An extension to BGP that allows you to connect multicast topologies within and between BGP ASs.
MBone	Multicast Backbone. An interconnected set of subnetworks and routers that support the delivery of IP multicast traffic. The MBone is a virtual network that is layered on top of sections of the physical Internet.
MCS	Miscellaneous Control Subsystem. On the M40e and M160 routers, provides control and monitoring functions for router components and SONET clocking for the router.
MD5	Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash used for generating message authentication signatures. MD5 is used in AH and ESP. <i>See also</i> hashing, SHA-1.
MDRR	Modified deficit round robin. A method for selecting queues to be serviced. <i>See</i> queue.
MDT	Multicast distribution tree. The path between the sender (host) and the multicast group (receiver or listener).
mean time between failures	<i>See</i> MTBF.
MED	Multiple exit discriminator. An optional BGP path attribute consisting of a metric value that is used to determine the exit point to a destination when all other factors determining the exit point are equal.
MEP	Start and end point within a maintenance domain. <i>See also</i> LTM.
mesh	Network topology in which devices are organized in a manageable, segmented manner with many, often redundant, interconnections between network nodes.
message aggregation	Extension to the Resource Reservation Protocol (RSVP) specification that allows neighboring routers to bundle up to 30 RSVP messages into a single protocol packet.
Message Digest 5	<i>See</i> MD5.
mgd	Management daemon. JUNOS software process responsible for managing all user access to the router.

MIB	Management Information Base. Definition of an object that can be managed by SNMP.
midplane	Physically separates front and rear cavities inside the chassis, distributes power from the power supplies, and transfers packets and signals between router components, which plug into it.
MIP	Intermediate node within the maintenance domain. <i>See also</i> LTM.
Miscellaneous Control Subsystem	<i>See</i> MCS.
MLD	Multicast listener discovery. Protocol that manages the membership of hosts and routers in multicast groups. IPv6 multicast routers use MLD to learn, for each of their attached physical networks, which groups have interested listeners.
MLFR	Multilink Frame Relay. Logically ties together individual circuits, creating a bundle. The logical equivalent of MLPPP, MLFR is used for Frame Relay traffic instead of PPP traffic. FRF.15 and FRF.16 are two implementations of MLFR.
MLPPP	Multilink Point-to-Point Protocol. Enables you to bundle multiple PPP links into a single logical link between two network devices to provide an aggregate amount of bandwidth. The technique is often called bonding or link aggregation. Defined in RFC 1990. <i>See also</i> PPP.
MM	JCS management module.
MMF	Multimode fiber. Optical fiber supporting the propagation of multiple frequencies of light. MMF is used for relatively short distances because the modes tend to disperse over longer lengths (called modal dispersion). For longer distances, single-mode fiber (sometimes called monomode) is used. <i>See also</i> single-mode fiber.
mobile network access subsystem	<i>See</i> MAS.
mobile point-to-point control subsystem	<i>See</i> MPS.
mobile station	Mobile device, such as a cellular phone or a mobile personal digital assistant (PDA).
Mobile Station Integrated Services Digital Network Number	<i>See</i> MSISDN.
Mobile Switching Center	<i>See</i> MSC.

mobile transport subsystem *See* MTS.

MPLS Multiprotocol Label Switching. Mechanism for engineering network traffic patterns that functions by assigning to network packets short labels that describe how to forward them through the network. Also called label switching. *See also* traffic engineering.

MPLS EXP classifier Class-of-service (CoS) behavior classifier for classifying packets based on the MPLS experimental bit. *See also* EXP bits.

MPS Mobile point-to-point control subsystem. A GSN application subsystem that controls all functionality associated with a particular connection.

MRRU Maximum received reconstructed unit. Similar to the MTU, but is specific to link services interfaces. *See also* MTU.

MSA Multisource Agreement. Definition of a fiber-optic transceiver module that conforms to the 10-Gigabit Ethernet standard. *See also* XENPAK module.

MSC Mobile Switching Center. Provides origination and termination functions to calls from a mobile station user.

MSDP Multicast Source Discovery Protocol. A protocol used to connect multicast routing domains to allow the domains to discover multicast sources from other domains. It typically runs on the same router as the PIM sparse mode rendezvous point (RP).

MSISDN Mobile Station Integrated Services Digital Network Number. A number that callers use to reach a mobile services subscriber.

MST *See* MSTP.

MSTI Multiple Spanning Tree Instance. One of a number of spanning trees calculated by MSTP within an MST region. The MSTI provides a simple and fully connected active topology for frames classified as belonging to a VLAN that is mapped to the MSTI by the MST configuration table used by the MST bridges of that MST region. *See also* CIST.

MSTP Multiple Spanning Tree Protocol. Spanning-tree protocol used to prevent loops in bridge configurations. Unlike other types of STPs, MSTP can block ports selectively by VLAN. *See also* RSTP.

MTBF Mean time between failures. Measure of hardware component reliability.

MTS Mobile transport subsystem. A GSN application subsystem that implements all the protocols used by the GSN.

MTU	Maximum transmission unit. Limit on the data size for a network.
multicast	Operation of sending network traffic from one network node to multiple network nodes.
multicast distribution tree	<i>See</i> MDT.
multicast listener discovery	<i>See</i> MLD.
Multicast Source Discovery Protocol	<i>See</i> MSDP.
multicast-scope number	Number used for configuring the multicast scope. Configuring a scope number constrains the scope of a multicast session. The number value can be any hexadecimal number from 0 through F. The multicast-scope value is a number from 0 through 15, or a specified keyword with an associated prefix range. For example, link-local (value = 2), corresponding prefix 224.0.0.0/24.
multiclass LSP	In Differentiated Services-aware traffic engineering, a multiclass label-switched path (LSP) functions like a standard LSP, but also allows you to reserve bandwidth for multiple class types. The experimental (EXP) bits of the MPLS header are used to distinguish between class types.
multiclass MLPPP	Enables multiple classes of service when you use MLPPP. Defined in RFC 2686, <i>The Multi-Class Extension to Multi-Link PPP</i> .
multifield classifier	Method for classifying traffic flows. Unlike a behavior aggregate (BA) classifier, a multifield classifier examines multiple fields in the packet to apply class-of-service (CoS) settings. Examples of fields that a multifield classifier examines include the source and destination address of the packet, as well as the source and destination port numbers of the packet. <i>See also</i> BA classifier, classification.
multihoming	Network topology that uses multiple connections between customer and provider devices to provide redundancy.
Multilink Frame Relay	<i>See</i> MLFR.
multimode fiber	<i>See</i> MMF.
multiple exit discriminator	<i>See</i> MED.
multiple spanning tree instance	<i>See</i> MSTI.
Multiple Spanning Tree Protocol	<i>See</i> MSTP.

multiprotocol BGP	<i>See</i> MBGP.
Multiprotocol Label Switching	<i>See</i> MPLS.
Multisource Agreement	<i>See</i> MSA.
MVS	Mobile visitor register subsystem.

N

n-selector	Last byte of a nonclient peer address.
named path	JUNOS software syntax that specifies a portion of or the entire network path that should be used as a constraint in signaling an MPLS label-switched path.
NAPT	Network Address Port Translation. A method that translates the addresses and transport identifiers of many private hosts into a few external addresses and transport identifiers to make efficient use of globally registered IP addresses. NAPT extends the level of translation beyond that of basic NAT. <i>See also</i> NAT.
NAT	Network Address Translation. A method of concealing a set of host addresses on a private network behind a pool of public addresses. It can be used as a security measure to protect the host addresses from direct targeting in network attacks.
National Institute of Standards and Technology	<i>See</i> NIST.
NCP	Network Control Protocol. A traffic controller used to establish and configure different network layer protocols for the Point-to-Point Protocol (PPP).
NDP	Neighbor Discovery Protocol. Protocol used by IPv6 nodes on the same link to discover each other's presence, determine each other's link-layer addresses, find routers, and maintain reachability information about the paths to active neighbors. NDP is defined in RFC 2461 and is equivalent to the Address Resolution Protocol (ARP) used with IPv4. <i>See also</i> ARP.
neighbor	Adjacent system reachable by traversing a single subnetwork. An immediately adjacent router. Also called a <i>peer</i> .
NET	Network entity title. Network address defined by the ISO network architecture and used in CLNS-based networks.

NetBIOS	Network basic input/output system. An application programming interface (API) used by programs on a LAN. NetBIOS provides a uniform set of commands for requesting the lower-level services required to manage names, conduct sessions, and send datagrams between nodes on a network.
Network Address Port Translation	<i>See</i> NAPT.
Network Address Translation	<i>See</i> NAT.
network basic input/output system	<i>See</i> NetBIOS.
Network Control Protocol	<i>See</i> NCP.
network entity title	<i>See</i> NET.
network interface	Interface, such as an Ethernet or SONET/SDH interface, that primarily provides traffic connectivity. <i>See also</i> PIC and services interface.
network layer reachability information	<i>See</i> NLRI.
network link advertisement	OSPF link-state advertisement flooded throughout a single area by designated routers to describe all routers attached to the network.
network LSA	OSPF link-state advertisement sent by the designated router on a broadcast or NBMA segment. It advertises the subnet associated with the designated router's segment.
network service access point	<i>See</i> NSAP.
network summary LSA	OSPF link-state advertisement sent by an ABR to advertise internal OSPF routing knowledge across an area boundary. <i>See also</i> ABR.
Network Time Protocol	<i>See</i> NTP.
NIC	Network Information Center. Internet authority responsible for assigning Internet-related numbers, such as IP addresses and autonomous system (AS) numbers. <i>See also</i> IANA.
NIST	National Institute of Standards and Technology. A nonregulatory U.S. federal agency whose mission is to develop and promote measurement, standards, and technology.
NLRI	Network layer reachability information. Information carried in BGP packets and used by MBGP.

nonclient peer	In a BGP route reflection, a BGP peer that is not a member of a cluster. <i>See also</i> client peer.
nonstop routing	<i>See</i> NSR.
not-so-stubby area	<i>See</i> NSSA.
notification cell	JUNOS software data structure generated by the Distribution Buffer Manager ASIC that represents the header contents of an IP packet. The Internet Processor ASIC uses the notification cell to perform a forwarding table lookup.
Notification message	BGP message that informs a neighbor about an error condition, and then in some cases terminates the BGP peering session.
NSAP	Network service access point. Connection to a network that is identified by a network address.
NSR	Nonstop routing. A high availability feature that allows a routing platform with redundant Routing Engines to preserve routing information on the backup Routing Engine and switch over from the primary Routing Engine to the backup Routing Engine without alerting peer nodes that a change has occurred. NSR uses the graceful Routing Engine switchover (GRES) infrastructure to preserve interface, kernel, and routing information.
NSSA	Not-so-stubby area. In OSPF, a type of stub area in which external routes can be flooded.
NTP	Network Time Protocol. A protocol used to synchronize computer clock times on a network.
Null Register message	PIM message sent by the first-hop router to the rendezvous point (RP). The message informs the RP that the local source is still actively sending multicast packets into the network. <i>See also</i> RP.
numeric range match conditions	Use of numeric values (protocol and port numbers) in the header of an IP packet to match criteria in a firewall filter.

O

Oakley	Key determination protocol based on the Diffie-Hellman algorithm that provides added security, including authentication. Oakley was the key-exchange algorithm mandated for use with the initial version of ISAKMP, although other algorithms can be used. Oakley describes a series of key exchanges called modes and details the services provided by each; for example, Perfect Forward Secrecy for keys, identity protection, and authentication. <i>See also</i> ISAKMP.
---------------	---

OAM	<ul style="list-style-type: none"> ■ Operation, Administration, and Maintenance. An ATM Forum specification for monitoring ATM virtual connections. OAM performs standard loopback, fault detection and notification, and remote defect identification for each connection, verifying that the connection is up and the router is operational. <i>See also</i> LFM. ■ Operation, Administration, and Maintenance. A set of Ethernet connectivity specifications and functions providing connectivity monitoring, fault detection and notification, fault verification, fault isolation, loopback, and remote defect identification. The primary specifications defining Ethernet OAM are IEEE 902.3ah link-fault management (LFM) and IEEE 902.1ag Ethernet connectivity-fault management (CFM). <i>See also</i> CFM and LFM.
OC	Optical carrier. In SONET, the OC level indicates the transmission rate of digital signals on optical fiber.
OC12	SONET line with a transmission speed of 622 Mbps using fiber-optic cables.
OC3	SONET line with a transmission speed of 155.52 Mbps (payload of 150.336 Mbps) using fiber-optic cables. For SDH interfaces, OC3 is also known as STM1.
OIF	Outgoing interface. An interface used by multicast functions within a router to determine which egress ports to use for forwarding multicast groups.
op script	Operational script. Extensible Stylesheet Language for Transformations (XSLT) script written to automate network troubleshooting and network management. Op scripts can perform any function available through JUNOScript remote procedure calls (RPCs).
Open message	BGP message that allows two neighbors to negotiate the parameters of the peering session.
OpenConfirm	BGP neighbor state that shows that a valid Open message was received from the remote peer.
OpenSent	BGP neighbor state that shows that an Open message was sent to the remote peer and the local router is waiting for an Open message to be returned.
operation script	<i>See</i> op script.
Operation, Administration, and Maintenance	<i>See</i> OAM.
operational mode	JUNOS software mode that allows a user to view statistics and information about the router's current operating status.
optical carrier	<i>See</i> OC.
origin	In BGP, an attribute that describes the source of the route.

orlonger	JUNOS software routing policy match type that represents all routes more specific than the given subnet, including the given subnet itself. It is similar to a mathematical greater-than-or-equal-to operation.
OSI	Open Systems Interconnection. Standard reference model for how messages are transmitted between two points on a network.
OSPF	Open Shortest Path First. A link-state IGP that makes routing decisions based on the shortest-path-first (SPF) algorithm (also referred to as the Dijkstra algorithm).
OSPF hello packet	Message sent by each OSPF router to each adjacent router. It is used to establish and maintain the router's neighbor relationships.
outgoing interface	<i>See</i> OIF.
overlay network	Network design in which a logical Layer 3 topology (IP subnets) is operating over a logical Layer 2 topology (ATM PVCs). Layers in the network do not have knowledge of each other, and each layer requires separate management and operation.
oversubscription	Method that allows provisioning of more bandwidth than the line rate of the physical interface.

P

P2MP LSP	<i>See</i> point-to-multipoint LSP.
package	Collection of files that make up a JUNOS software component.
packet	Fundamental unit of information (message or fragment of a message) carried in a packet-switched network, for example, the Internet. <i>See also</i> PSN.
packet aging	Occurs when packets in the output buffer are overwritten by newly arriving packets. This happens because the available buffer size is greater than the available transmission bandwidth.
packet capture	<p>Packet capture can be either of the following:</p> <ol style="list-style-type: none"> 1. Packet sampling method, in which entire IPv4 packets flowing through a router are captured for analysis. Packets are captured in the Routing Engine and stored as libpcap-formatted files on the router. Packet capture files can be opened and analyzed offline with packet analyzers such as tcpdump or Ethereal. <i>See also</i> traffic sampling. 2. J-Web packet sampling method for quickly analyzing router control traffic destined for or originating from the Routing Engine. You can either decode and view the captured packets in the J-Web interface as they are captured, or save the packets to a file and analyze them offline with packet analyzers such as Ethereal. J-Web packet capture does not capture transient traffic.

packet classification	<i>See</i> classification.
packet data protocol	<i>See</i> PDP.
Packet Forwarding Engine	Portion of the router that processes packets by forwarding them between input and output interfaces.
packet loss priority	<i>See</i> PLP.
packet or cell switching	Transmission of packets from many sources over a switched network.
packet-switched network	<i>See</i> PSN.
PADI	PPPoE Active Discovery Initiation packet. A Point-to-Point Protocol over Ethernet (PPPoE) initiation packet that is broadcast by the client to start the discovery process.
PADO	PPPoE Active Discovery Offer packet. A Point-to-Point Protocol over Ethernet (PPPoE) offer packet that is sent to the client by one or more access concentrators in reply to a PPPoE Active Discovery Initiation (PADI) packet.
PADR	PPPoE Active Discovery Request packet. A Point-to-Point Protocol over Ethernet (PPPoE) packet sent by the client to one selected access concentrator to request a session.
PADS	PPPoE Active Discovery Session Confirmation packet. A Point-to-Point Protocol over Ethernet (PPPoE) packet sent by the selected access concentrator to confirm the session.
PADT	PPPoE Active Discovery Termination packet. A Point-to-Point Protocol over Ethernet (PPPoE) packet sent by either the client or the access concentrator to terminate a session.
partial sequence number PDU	<i>See</i> PSNP.
passive flow monitoring	Technique to intercept and observe specified data network traffic by using a routing platform such as a monitoring station that is not participating in the network.
path attribute	Information about a BGP route, such as the route origin, AS path, and next-hop router.
PathErr message	RSVP message indicating that an error has occurred along an established path LSP. The message is advertised upstream toward the ingress router and does not remove any RSVP soft state from the network.

PathTear message	RSVP message indicating that the established LSP and its associated soft state should be removed by the network. The message is advertised downstream hop by hop toward the egress router.
PBB	Provider backbone bridge. Defined in IEEE 802.1ah, PBBs offer a scalable solution for building large bridged networks by improving MAC address scalability and service instance scalability.
PBBN	Provider backbone bridge network. <i>See</i> PBB.
PC Card	(Previously known as a PCMCIA Card.) The removable storage media that ships with each router that contains a copy of the JUNOS software. The PC Card is based on standards published by the Personal Computer Memory Card International Association (PCMCIA).
pcap	Software library for packet capturing. <i>See also</i> libpcap.
PCI	Peripheral Component Interconnect. Standard, high-speed bus for connecting computer peripherals. Used on the Routing Engine.
PCI Express	Peripheral Component Interconnect Express. Next-generation, higher-bandwidth bus for connecting computer peripherals. A PCI Express bus uses point-to-point bus topology with a shared switch rather than the shared bus topology of a standard PCI bus. The shared switch on a PCI Express bus provides centralized traffic routing and management and can prioritize traffic. On some J-series Services Routers, PCI Express slots are backward compatible with PCI and can accept Physical Interface Modules (PIMs) intended for either PCI Express or PCI slots.
PCMCIA	Personal Computer Memory Card International Association. Industry group that promotes standards for credit card-size memory and I/O devices.
PDH	Plesiochronous Digital Hierarchy. Developed to carry digitized voice more efficiently. Evolved into the North America, European, and Japanese Digital Hierarchies, in which only a discrete set of fixed rates is available, namely, NxDS0 (DS0 is a 64-Kbps rate).
PDP	Packet data protocol. Network protocol, such as IP, used by packet data networks connected to a GPRS network.
PDU	Protocol data unit. A packet of data passed across a network. The term refers to a specific layer of the OSI seven-layer model and a specific protocol.
PE router	Provider edge router. A router in the service provider's network that is connected to a customer edge (CE) device and participates in a virtual private network (VPN).
peak information rate	<i>See</i> PIR.

PEC	Policing equivalence classes. In traffic policing, a set of packets that are treated the same way by the packet classifier.
peer	Immediately adjacent router with which a protocol relationship has been established. Also called a neighbor.
peering	Practice of exchanging Internet traffic with directly connected peers according to commercial and contractual agreements.
PEM	Privacy Enhanced Mail. A technique for securely exchanging electronic mail over a public medium. Power Entry Module. Distributes DC power within the router chassis. Supported on M40e, M160, M320, and T-series routing platforms.
penultimate hop popping	<i>See</i> PHP.
penultimate router	Last transit router before the egress router in an MPLS label-switched path.
Perfect Forward Secrecy	<i>See</i> PFS.
Peripheral Component Interconnect	<i>See</i> PCI.
permanent interface	Interface that is always present in the routing platform. <i>See also</i> management Ethernet interface and transient interface.
permanent virtual circuit	<i>See</i> PVC.
persistent change	Commit script-generated configuration change that is copied to the candidate configuration. Persistent changes remain in the candidate configuration unless you explicitly delete them. <i>See also</i> transient change.
Personal Computer Memory Card International Association	<i>See</i> PCMCIA.
PFC	Protocol Field Compression. Normally, PPP-encapsulated packets are transmitted with a two-byte protocol field. For example, IPv4 packets are transmitted with the protocol field set to 0x0021, and MPLS packets are transmitted with the protocol field set to 0x0281. For all protocols with identifiers from 0x0000 through 0x00ff, PFC enables routers to compress the protocol field to one byte, as defined in RFC 1661, <i>The Point-to-Point Protocol (PPP)</i> . PFC allows you to conserve bandwidth by transmitting less data. <i>See also</i> ACFC.

PFS	Perfect Forward Secrecy protocol. A protocol derived from an encryption system that changes encryption keys often and ensures that no two sets of keys have any relation to each other. If one set of keys is compromised, only communications using those keys are at risk. An example of a system that uses PFS is Diffie-Hellman.
PGM	Pragmatic General Multicast. A protocol layer that can be used between the IP layer and the multicast application on sources, receivers, and routers to add reliability, scalability, and efficiency to multicast networks.
PGP	Pretty Good Privacy. A strong cryptographic technique invented by Philip Zimmerman in 1991.
PHP	Penultimate hop popping. A mechanism used in an MPLS network that allows the transit router before the egress router to perform a label pop operation and forward the remaining data (often an IPv4 packet) to the egress router.
PHY	PHY can be either of the following: <ol style="list-style-type: none"> 1. Special electronic integrated circuit or functional block of a circuit that performs encoding and decoding between a pure digital domain (on-off) and a modulation in the analog domain. <i>See also</i> LAN PHY and WAN PHY. 2. Open Systems Interconnection (OSI) physical layer. Layer 1 of the OSI model that defines the physical link between devices.
physical interface	Port on a Physical Interface Card (PIC) or Physical Interface Module (PIM).
Physical Interface Card	<i>See</i> PIC.
Physical Interface Module	<i>See</i> multicast.
PIC	Physical Interface Card. A network interface-specific card that can be installed on an FPC in the router.
PIC I/O Manager ASIC	Juniper Networks ASIC responsible for receiving and transmitting information on the physical media. It performs media-specific tasks within the Packet Forwarding Engine.

PIM	<p>PIM can be either of the following:</p> <ol style="list-style-type: none"> 1. Protocol Independent Multicast. A protocol-independent multicast routing protocol. PIM dense mode is a flood-and-prune protocol. PIM sparse mode routes to multicast groups that use join messages to receive traffic. PIM sparse-dense mode allows some multicast groups to be dense groups (flood-and-prune) and some groups to be sparse groups (join and leave). 2. Physical Interface Module. A network interface card installed in a J-series Services Router to provide physical connections to a LAN or WAN. PIMs can be fixed or removable and interchangeable. The PIM receives incoming packets from the network and transmits outgoing packets to the network. Each PIM is equipped with a dedicated network processor that forwards incoming data packets to and receives outgoing data packets from the Routing Engine. During this process, the PIM performs framing and line-speed signaling for its medium type—for example, E1, serial, Fast Ethernet, or ISDN.
PIR	Peak information rate. The PIR must be equal to or greater than the CIR, and both must be configured to be greater than 0. Packets that exceed the PIR are marked red, which corresponds to high loss priority. <i>See also</i> CIR, trTCM.
PKI	Public key infrastructure. A hierarchy of trust that enables users of a public network to securely and privately exchange data through the use of public and private cryptographic key pairs that are obtained and shared with peers through a trusted authority.
Plesiochronous Digital Hierarchy	<i>See</i> PDH.
PLMN	Public Land Mobile Network. A telecommunications network for mobile stations.
PLP	Packet loss priority. Used to determine the random early detection (RED) drop profile when a packet is queued. You can set it by configuring a classifier or policer. The system supports two PLP designations: low and high.
PLP bit	Packet loss priority bit. Used to identify packets that have experienced congestion or are from a transmission that exceeded a service provider's customer service license agreement. This bit can be used as part of a router's congestion control mechanism and can be set by the interface or by a filter.
PLR	Point of local repair. The ingress router of a backup tunnel or a detour LSP.
point of local repair	<i>See</i> PLR.
Point of Presence	<i>See</i> POP.
point-to-multipoint connection	Unidirectional connection in which a single source system transmits data to multiple destination end systems. Point-to-multipoint is one of two fundamental connection types. <i>See also</i> point-to-point connection.

point-to-multipoint LSP	RSVP-signaled LSP with a single source and multiple destinations.
point-to-point connection	Unidirectional or bidirectional connection between two end systems. Point-to-point is one of two fundamental connection types. <i>See also</i> point-to-multipoint connection.
Point-to-Point Protocol	<i>See</i> PPP.
Point-To-Point Protocol process	<i>See</i> pppd.
poison reverse	Method used in distance-vector networks to avoid routing loops. Each router advertises routes back to the neighbor it received them from with an infinity metric assigned.
policer	Filter that limits traffic of a certain class to a specified bandwidth or burst size. Packets exceeding the policer limits are discarded, or assigned to a different forwarding class, a different loss priority, or both.
policing	Method of applying rate limits on bandwidth and burst size for traffic on a particular interface.
policing equivalence classes	<i>See</i> PEC.
policy chain	Application of multiple routing policies in a single location. The policies are evaluated in a predefined manner and are always followed by the default policy for the specific application location.
pop	Removal of the last label, by a router, from a packet as it exits an MPLS domain.
POP	Point of presence. A physical access point to the Internet. The location of the servers, routers, and ATM switches used to provide access to the Internet.
port mirroring	Method in which a copy of an IPv4 packet is sent from the routing platform to an external host address or a packet analyzer for analysis.
PPP	Point-to-Point Protocol. A link-layer protocol that provides multiprotocol encapsulation. PPP is used for link-layer and network-layer configuration. Provides a standard method for transporting multiprotocol datagrams over point-to-point links. Defined in RFC 1661.
pppd	Point-to-Point Protocol process (daemon) that processes packets that use PPP.
PPPoE	Point-to-Point Protocol over Ethernet. Network protocol that encapsulates PPP frames in Ethernet frames and connects multiple hosts over a simple bridging access device to a remote access concentrator.

PPPoE Active Discovery Initiation packet	<i>See</i> PADI.
PPPoE Active Discovery Offer packet	<i>See</i> PADO.
PPPoE Active Discovery Request packet	<i>See</i> PADR.
PPPoE Active Discovery Session Confirmation packet	<i>See</i> PADS.
PPPoE Active Discovery Termination packet	<i>See</i> PADT.
PPPoE over ATM	Point-to-Point Protocol over Ethernet frames in Asynchronous Transfer Mode. Network protocol that encapsulates Point-to-Point Protocol over Ethernet (PPPoE) frames in Asynchronous Transfer Mode (ATM) frames for digital subscriber line (DSL) transmission, and connects multiple hosts over a simple bridging access device to a remote access concentrator.
Pragmatic General Multicast	<i>See</i> PGM.
precedence bits	First three bits in the type-of-service (ToS) byte. On a Juniper Networks router, these bits are used to sort or classify individual packets as they arrive at an interface. The classification determines the queue to which the packet is directed upon transmission.
preference	Desirability of a route to become the active route. A route with a lower preference value is more likely to become the active route. The preference is an arbitrary value from 0 through 255 that the routing protocol process uses to rank routes received from different protocols, interfaces, or remote systems.
preferred address	On an interface, the default local address used for packets sourced by the local router to destinations on the subnet.
prefix-length-range	JUNOS software routing policy match type representing all routes that share the same most-significant bits. The prefix length of the route must also lie between the two supplied lengths in the route filter.
Pretty Good Privacy	<i>See</i> PGP.
primary address	On an interface, the address used by default as the local address for broadcast and multicast packets sourced locally and sent out the interface.

primary contributing route	Contributing route with the numerically smallest prefix and smallest JUNOS software preference value. This route is the default next hop used for a generated route.
primary interface	Router interface that packets go out on when no interface name is specified and when the destination address does not specify a particular outgoing interface.
Privacy Enhanced Mail	<i>See</i> PEM.
promiscuous mode	Used with ATM CCC Cell Relay encapsulation, enables mapping of all incoming cells from an interface port or from a virtual path (VP) to a single label-switched path (LSP) without restricting the VCI number.
Protected System Domain	A set of Flexible PIC Concentrators (FPCs) on a Juniper Networks routing platform matched with a redundant Routing Engine pair (or single Routing Engine) on the JCS 1200 platform to form a secure, virtual hardware router.
protocol address	Logical Layer 3 address assigned to an interface within the JUNOS software.
protocol data unit	<i>See</i> PDU.
protocol families	Grouping of logical properties within an interface configuration, for example, the inet, inet4, and mpls protocol families.
Protocol Field Compression	<i>See</i> PFC.
Protocol Independent Multicast	<i>See</i> multicast.
protocol preference	32-bit value assigned to all routes placed into the routing table. The protocol preference is used as a tiebreaker when multiple exact routes are placed into the table by different protocols.
provider backbone bridge	<i>See</i> PBB.
provider backbone bridge network	<i>See</i> PBBN.
provider edge router	<i>See</i> PE router.
provider router	Router in the service provider's network that is not connected to a customer edge (CE) device.
Prune message	PIM message sent upstream to a multicast source or the rendezvous point (RP) of the domain. The message requests that multicast traffic stop being transmitted to the router originating the message.

PSD	<i>See</i> Protected System Domain.
PSN	Packet-switched network. Network in which messages or fragments of messages (packets) are sent to their destination through the most expedient route, as determined by a routing algorithm. Packet switching optimizes bandwidth in a network and minimizes latency.
PSNP	Partial sequence number PDU. A packet that contains only a partial list of the LSPs in the IS-IS link-state database.
public key infrastructure	<i>See</i> PKI.
Public Land Mobile Network	<i>See</i> PLMN.
push	Addition of a label or stack of labels, by a router, to a packet as it enters an MPLS domain.
PVC	Permanent virtual circuit. A software-defined logical connection in a network. <i>See also</i> SVC.

Q

Q-in-Q	<i>See</i> 802.1ad.
QoS	Quality of service. Performance, such as transmission rates and error rates, of a communications channel or system.
quad-wide	Type of PIC that combines the PIC and FPC within a single FPC slot.
qualified next hop	Next hop for a static route that allows a second next hop for the same static route to have different metric and preference properties from the original next hop.
quality of service	<i>See</i> QoS.
querier router	PIM router on a broadcast subnet responsible for generating IGMP query messages for the segment.
queue	First-in, first-out (FIFO) number of packets waiting to be forwarded over a router interface. You can configure the minimum and maximum size of the packet queue, queue admission policies, and other parameters to manage the flow of packets through the router.
queue fullness	For random early detection (RED), the memory used to store packets expressed as a percentage of the total memory allocated for that specific queue. <i>See also</i> drop profile.

queue length For ATM1 interfaces only, a limit on the number of transmit packets that can be queued. Packets that exceed the limit are dropped. *See also* EPD.

queuing In routing, the arrangement of packets waiting to be forwarded. Packets are organized into queues according to their priority, time of arrival, or other characteristics, and are processed one at a time. After a packet is sent to the outgoing interface on a router, it is queued for transmission on the physical media. The amount of time a packet is queued on the router is determined by the availability of the outgoing physical media, bandwidth, and the amount of traffic using the interface.

R

RA Registration authority. A trusted third-party organization that acts on behalf of a certificate authority (CA) to verify the identity of a digital certificate user.

radio frequency interference *See* RFI.

radio network controller *See* RNC.

RADIUS Remote Authentication Dial-In User Service. An authentication method for validating users who attempt to access the router using telnet.

random early detection *See* RED.

Rapid Spanning Tree Protocol *See* RSTP.

rate limiting *See* policing.

RBOC (Pronounced “are-bock”) Regional Bell operating company. Regional telephone companies formed as a result of the divestiture of the Bell System.

RC2, RC4, RC5 RSA codes. A family of proprietary (RSA Data Security, Inc.) encryption schemes often used in Web browsers and servers. These codes use variable-length keys up to 2048 bits.

RDBMS Relational database management system. A system that presents data in a tabular form with a means of manipulating the tabular data with relational operators.

RDM Russian-dolls bandwidth allocation model. An allocation model that makes efficient use of bandwidth by allowing the class types to share bandwidth. RDM is defined in the Internet draft draft-ietf-tewg-diff-te-russian-03.txt, *Russian Dolls Bandwidth Constraints Model for Diff-Serv-aware MPLS Traffic Engineering*.

Real-Time Performance Monitoring *See* RPM.

Real-Time Transport Protocol	<i>See</i> RTP.
receive	Next hop for a static route that allows all matching packets to be sent to the Routing Engine for processing.
record route object	<i>See</i> RRO.
recursive lookup	Method of consulting the routing table to locate the actual physical next hop for a route when the supplied next hop is not directly connected.
RED	Random early detection. Gradual drop profile for a given class that is used for congestion avoidance. RED tries to anticipate incipient congestion by dropping a small percentage of packets from the head of the queue to ensure that a queue never actually becomes congested.
refresh reduction	In RSVP, an extension that addresses the problems of scaling, reliability, and latency when Refresh messages are used to cover message loss.
Regional Bell operating company	<i>See</i> RBOC.
Register message	PIM message unicast by the first-hop router to the rendezvous point (RP) that contains the multicast packets from the source encapsulated within its data field.
Register Stop message	PIM message sent by the RP to the first-hop router to halt the sending of encapsulated multicast packets.
registration authority	<i>See</i> RA.
reject	Next hop for a configured route that drops all matching packets from the network and returns an ICMP message to the source IP address. Also used as an action in a routing policy or firewall filter.
relational database management system	<i>See</i> RDBMS.
Remote Authentication Dial-In User Service	<i>See</i> RADIUS.
remote monitoring	<i>See</i> RMON.
remote procedure call	<i>See</i> RPC.
rename	JUNOS software command that allows a user to change the name of a routing policy, firewall filter, or any other variable character string defined in the router configuration.
rendezvous point	<i>See</i> RP.

Request for Comments	<i>See</i> RFC.
Request message	RIP message used by a router to ask for all or part of the routing table from a neighbor.
resolve	Next hop for a static route that allows the router to perform a recursive lookup to locate the physical next hop for the route.
Resource Reservation Protocol	<i>See</i> RSVP.
Response message	RIP message used to advertise routing information into a network.
result cell	JUNOS software data structure generated by the Internet Processor ASIC after performing a forwarding table lookup.
ResvConf message	RSVP message that allows the egress router to receive an explicit confirmation message from a neighbor that its Resv message was received.
ResvErr message	RSVP message indicating that an error has occurred along an established LSP. The message is advertised downstream toward the egress router, and it does not remove any RSVP soft state from the network.
ResvTear message	RSVP message indicating that the established LSP and its associated soft state should be removed by the network. The message is advertised upstream toward the ingress router.
reverse-path forwarding	<i>See</i> RPF.
reverse-path multicasting	<i>See</i> RPM.
revert timer	For SONET Automatic Protection Switching (APS), a timer that specifies the amount of time (in seconds) to wait after the working circuit has become functional before making the working circuit active again.
rewrite rules	Set the appropriate class-of-service (CoS) bits in an outgoing packet. This allows the next downstream router to classify the packet into the appropriate service group.
RFC	Request for Comments. Internet standard specifications published by the Internet Engineering Task Force (IETF).
RFI	Radio frequency interface. Interference from high-frequency electromagnetic waves emanating from electronic devices.
RIB	Routing information base. A logical data structure used by BGP to store routing information. <i>See also</i> routing table.

RID	Router ID. An IP address used by a router to uniquely identify itself to a routing protocol. This address may not be equal to a configured interface address.
RIP	Routing Information Protocol. Used in IPv4 networks, a distance-vector interior gateway protocol that makes routing decisions based on hop count.
RIPng	Routing Information Protocol next generation. Used in IPv6 networks, a distance-vector interior gateway protocol that makes routing decisions based on hop count.
RMON	Remote monitoring. A standard MIB that defines current and historical MAC-layer statistics and control objects, allowing you to capture real-time information across the entire network. This allows you to detect, isolate, diagnose, and report potential and actual network problems.
RNC	Radio network controller. Manages the radio part of the network in UMTS.
Root System Domain	Pair of redundant Routing Engines on a Juniper Networks routing platforms connected to the switch fabric on the Juniper Control System (JCS) platform. The configuration on the Routing Engines on the Juniper Networks routing platforms provides the RSD identification and the configuration of up to eight Protected System Domains (PSDs).
route distinguisher	6-byte value identifying a VPN that is prefixed to an IPv4 address to create a unique IPv4 address. The new address is part of the VPN IPv4 address family, which is a BGP address family added as an extension to the BGP protocol. It allows you to configure private addresses within the VPN by preventing overlap with the private addresses in other VPNs.
route filter	JUNOS software syntax used in a routing policy to match an individual route or a group of routes.
route flapping	Condition of network instability where a route is announced and withdrawn repeatedly, often as the result of an intermittently failing link.
route identifier	IP address of the router from which a BGP, IGP, or OSPF packet originated.
route redistribution	Method of placing learned routes from one protocol into another protocol operating on the same router. The JUNOS software accomplishes this with a routing policy.
route reflection	In BGP, the configuration of a group of routers into a cluster in which one system acts 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.
router ID	<i>See</i> RID.
router LSA	OSPF link-state advertisement sent by each router in the network. It describes the local router's connected subnets and their metric values.

router priority	Numerical value assigned to an OSPF or IS-IS interface that is used as the first criterion in electing the designated router or designated intermediate system, respectively.
router-link advertisement	OSPF link-state advertisement flooded throughout a single area by all routers to describe the state and cost of the router's links to the area.
routing domain	<i>See AS.</i>
Routing Engine	Portion of the router that handles all routing protocol processes, as well as other software processes that control the router's interfaces, some of the chassis components, system management, and user access to the router.
routing gateway	A firewall, network address translation (NAT) router, or other routing device used as a customer premises (CPE) terminator in the home, office, or local point of presence (POP).
routing information base	<i>See RIB.</i>
Routing Information Protocol	<i>See RIP.</i>
Routing Information Protocol next generation	<i>See RIPvng.</i>
routing instance	Collection of routing tables, interfaces, and routing protocol parameters. The set of interfaces is contained in the routing tables, and the routing protocol parameters control the information in the routing tables.
routing matrix	Terabit routing system interconnecting up to four T640 routing nodes and a TX Matrix platform to deliver up to 2.56 terabits per second (Tbps) of subscriber switching capacity.
routing plane	Used to describe the interconnected routing engines within a routing matrix. There are two routing planes, the master routing plane, which includes all master Routing Engines, and the backup routing plane, which includes all backup routing planes.
routing protocol daemon	<i>See rpd.</i>
routing table	Common database of routes learned from one or more routing protocols. All routes are maintained by the JUNOS routing protocol process.
RP	Rendezvous point. For PIM sparse mode, a core router acting as the root of the distribution tree in a shared tree.

RPC	Remote procedure call. A type of protocol that allows a computer program running on one computer to cause a function on another computer to be executed without explicitly coding the details for this interaction.
rpd	JUNOS software routing protocol process (daemon). A user-level background process responsible for starting, managing, and stopping the routing protocols on a Juniper Networks router.
RPF	Reverse path forwarding. An algorithm that checks the unicast routing table to determine whether there is a shortest path back to the source address of the incoming multicast packet. Unicast RPF helps determine the source of denial-of-service attacks and rejects packets from unexpected source addresses.
RPM	RPM can be either of the following: <ul style="list-style-type: none"> ■ Reverse-path multicasting. Routing algorithm used by Distance Vector Multicast Routing Protocol (DVMRP) to forward multicast traffic. ■ Real-Time Performance Monitoring. A tool for creating active probes to track and monitor traffic.
RRO	Record route object. An RSVP message object that notes the IP address of each router along the path of an LSP.
RSA codes	<i>See</i> RC2, RC4, RC5.
RSD	<i>See</i> Root System Domain.
RSTP	Rapid Spanning Tree Protocol. A spanning-tree protocol used to prevent loops in bridge configurations. RSTP is not aware of VLANs and blocks ports at the physical level. <i>See also</i> MSTP.
RSVP	Resource Reservation Protocol. A signaling protocol that establishes a session between two routers to transport a specific traffic flow.
RSVP Path message	RSVP message sent by the ingress router downstream toward the egress router. It begins the establishment of a soft state database for a particular label-switched path.
RSVP Resv message	RSVP message sent by the egress router upstream toward the ingress router. It completes the establishment of the soft state database for a particular label-switched path.
RSVP signaled LSP	Label-switched path that is dynamically established using RSVP Path and Resv messages.
RSVP-TE	RSVP-traffic engineering; RSVP with traffic engineering extensions as defined by RFC 3209. These extensions allow RSVP to establish label-switched paths (LSPs) in MPLS networks. <i>See also</i> MPLS, RSVP.

RTP	Real-Time Transport Protocol. An Internet protocol that provides mechanisms for the transmission of real-time data, such as audio, video, or voice, over IP networks. Compressed RTP is used for VoIP traffic.
RTVBR	Real-time variable bit rate. For ATM2 intelligent queuing (IQ) interfaces, data that is serviced at a higher priority rate than other VBR data. RTVBR is suitable for carrying packetized video and audio. RTVBR provides better congestion control and latency guarantees than non-real-time VBR.

S

S-TAG	Field defined in the IEEE 802.1ad Q-in-Q encapsulation header that carries the S-VLAN identifier information. <i>See also</i> B-TAG.
S-tagged service interface	Interface between a customer edge (CE) device and the I-BEB or IB-BEB network components. Frames passed through this interface contain an S-TAG field. <i>See also</i> B-tagged service interface.
S-VLAN	Specific service instance VLAN identifier carried inside the S-TAG field. <i>See also</i> B-VID.
S/T interface	System reference point/terminal reference point interface. A four-pair connection between the ISDN provider service and the customer terminal equipment.
SA	Security association. An IPsec term that describes an agreement between two parties about what rules to use for authentication and encryption algorithms, key exchange mechanisms, and secure communications.
sampling	Method where the sampling key based on the IPv4 header is sent to the Routing Engine. There, the key is placed in a file, or cflowd packets based on the key are sent to a cflowd server.
SAP	SAP can be either of the following: <ol style="list-style-type: none"> 1. Session Announcement Protocol. Used with multicast protocols to handle session conference announcements. 2. Service access point. Device that identifies routing protocols and provides the connection between the network interface card and the rest of the network.
SAR	Segmentation and reassembly. Buffering used with ATM.
SCB	System Control Board. On an M40 router, the part of the Packet Forwarding Engine that performs route lookups, monitors system components, and controls FPC resets.
SCC	Switch-card chassis. Term used by the JUNOS command-line interface (CLI) to refer to the TX Matrix platform in a routing matrix.

SCEP	Simple Certificate Enrollment Protocol. A protocol for digital certificates that supports certificate authority (CA) and registration authority (RA) public key distribution, certificate enrollment, certificate revocation, certificate queries, and certificate revocation list (CRL) queries.
SCG	SONET Clock Generator. On a T640 routing node, provides the Stratum 3 clock signal for the SONET/SDH interfaces. Also provides external clock inputs.
scheduler maps	In class of service, schedule maps associate schedulers with specific forwarding classes. <i>See also</i> schedulers, forwarding classes.
schedulers	Define the priority, bandwidth, delay buffer size, rate control status, and RED drop profiles of a packet transmission. Schedulers are mapped to a specific forwarding class by a scheduler map. <i>See also</i> scheduler maps.
scheduling	Method of determining which type of packet or queue is transmitted before another. An individual router interface can have multiple queues assigned to store packets. The router then determines which queue to service based on a particular method of scheduling. This process often involves a determination of which type of packet should be transmitted before another. For example, first in, first out (FIFO). <i>See also</i> FIFO.
scp	Secure copy. Means of securely transferring computer files between a local and remote host or between two remote hosts, using the Secure Shell (SSH) protocol.
SCU	Source class usage. A means of tracking traffic originating from specific prefixes on the provider core router and destined for specific prefixes on the customer edge router, based on the IP source and destination addresses.
SDH	Synchronous Digital Hierarchy. A CCITT variation of the SONET standard.
SDP	Session Description Protocol. Used with multicast protocols to handle session conference announcements.
SDRAM	Synchronous dynamic random-access memory. An electronic standard in which the inputs and outputs of SDRAM data are synchronized to an externally supplied clock, allowing for extremely fast consecutive read and write capacity.
SDX software	Service Deployment System software. Deprecated term. <i>See</i> SRC software.
secure copy	<i>See</i> SCP.
Secure Hash Algorithm	<i>See</i> SHA-1.
Secure Shell	<i>See</i> SSH.

Secure Shell with Transport Layer Security	<i>See</i> SSH/TLS.
Secure Sockets Layer	<i>See</i> SSL.
security association	<i>See</i> SA.
Security Parameter Index	<i>See</i> SPI.
segmentation and reassembly	<i>See</i> SAR.
serial interface	DTE/DCE interface for WAN links. <i>See also</i> DTE and DCE.
service access point	<i>See</i> SAP.
Service Deployment System software	<i>See</i> SRX software.
Service Profile Identifier	<i>See</i> SPID.
services interface	Interface that provides specific capabilities for manipulating traffic before it is delivered to its destination, for example, the adaptive services interface and the tunnel services interface. <i>See also</i> network interface.
Serving GPRS Support Node	<i>See</i> SGSN.
Session and Resource Control software	<i>See</i> SRX software.
Session Announcement Protocol	<i>See</i> SAP.
session attribute object	RSVP message object used to control the priority, preemption, affinity class, and local rerouting of the LSP.
Session Description Protocol	<i>See</i> SDP.
Session Initiation Protocol	<i>See</i> SIP.
set-top box	The end host or device used to receive IPTV video streams.
SFM	Switching and Forwarding Module. On an M160 router, a component of the Packet Forwarding Engine that provides route lookup, filtering, and switching to FPCs.

SFP	Small form-factor pluggable transceiver. A transceiver that provides support for optical or copper cables. SFPs are hot-insertable and hot-removable. <i>See also</i> XFP.
SGSN	Serving GPRS Support Node. Device in the mobile network that requests PDP contexts with a GGSN.
SHA-1	Secure Hash Algorithm 1. A secure hash algorithm standard defined in FIPS PUB 180-1 (SHA-1). Developed by the National Institute of Standards and Technology (NIST), SHA-1 (which effectively replaces SHA-0) produces a 160-bit hash for message authentication. Longer-hash variants include SHA-224, SHA-256, SHA-384, and SHA-512 (sometimes grouped under the name “SHA-2”). SHA-1 is more secure than MD5. <i>See also</i> hashing, MD5.
sham link	Unnumbered point-to-point intra-area link advertised by a type 1 link-state advertisement (LSA).
shaping rate	In class of service, controls the maximum rate of traffic transmitted on an interface. <i>See also</i> traffic shaping.
shared scheduling and shaping	Allocation of separate pools of shared resources to subsets of logical interfaces belonging to the same physical port.
shared tree	Multicast forwarding tree established from the rendezvous point (RP) to the last-hop router for a particular group address.
SHDSL	Symmetric high-speed digital subscriber line. A standardized multirate symmetric DSL that transports rate-adaptive symmetrical data across a single copper pair at data rates from 192 Kbps to 2.3 Mbps, or from 384 Kbps to 4.6 Mbps over two pairs, covering applications served by HDSL, SDSL, T1, E1, and services beyond E1. SHDSL conforms to the following recommendations: ITU G.991.2 G.SHDSL, ETSI TS 101-524 SDSL, and the ANSI T1E1.4/2001-174 G.SHDSL. <i>See also</i> G.SHDSL.
SHDSL transceiver unit-central office	<i>See</i> STU-C.
SHDSL transceiver unit-remote	<i>See</i> STU-R.
shim header	Location of the MPLS header in a data packet. The JUNOS software always places (shims) the header between the existing Layer 2 and Layer 3 headers.
short message service	<i>See</i> SMS.
shortest path first	<i>See</i> SPF.
shortest-path tree	<i>See</i> SPT.

SIB	Switch Interface Board. On a T640 routing node, provides the switching function to the destination Packet Forwarding Engine.
signaled path	In traffic engineering, an explicit path; that is, a path determined using RSVP signaling. The Explicit Route Object carried in the packets contains the explicit path information.
Signaling System 7	<i>See SS7.</i>
Simple Certificate Enrollment Protocol	<i>See SCEP.</i>
Simple Network Management Protocol	<i>See SNMP.</i>
simplex interface	Interface that treats packets it receives from itself as the result of a software loopback process. The interface does not consider these packets when determining whether the interface is functional.
single-mode fiber	Optical fiber designed for transmission of a single ray or mode of light as a carrier and used for long-distance signal transmission. For short distances, multimode fiber is used. <i>See also</i> MMF.
SIP	Session Initiation Protocol. An adaptive services application protocol option used for setting up sessions between endpoints on the Internet. Examples include telephony, fax, videoconferencing, file exchange, and person-to-person sessions.
small form-factor pluggable transceiver	<i>See SFP.</i>
SMS	Short message service. A GSM service that enables short text messages to be sent to and from mobile telephones.
SNA	System Network Architecture. IBM proprietary networking architecture consisting of a protocol stack that is used primarily in banks and other financial transaction networks.
SNMP	Simple Network Management Protocol. A protocol governing network management and the monitoring of network devices and their functions.
soft state	In RSVP, control state in hosts and routers that expires if not refreshed within a specified amount of time.
SONET	Synchronous Optical Network. A high-speed (up to 2.5 Gbps) synchronous network specification developed by Bellcore and designed to run on optical fiber. STS1 is the basic building block of SONET. Approved as an international standard in 1988. <i>See also</i> SDH.

SONET Clock Generator	<i>See</i> SCG.
source class usage	<i>See</i> SCU.
source service access point	<i>See</i> SSAP.
source-based tree	Multicast forwarding tree established from the source of traffic to all interested receivers for a particular group address. It is often used in a dense-mode forwarding environment.
source-specific multicast	<i>See</i> SSM.
Spanning Tree Protocol	<i>See</i> STP.
sparse mode	Method of operating a multicast domain where sources of traffic and interested receivers meet at a central rendezvous point. A sparse-mode network assumes that there are very few receivers for each group address.
SPF	Shortest path first. An algorithm used by IS-IS and OSPF to make routing decisions based on the state of network links. Also called the <i>Dijkstra algorithm</i> .
SPI	Security Parameter Index. In IPsec, a numeric identifier used with the destination address and security protocol to identify an SA. When IKE is used to establish an SA, the SPI is randomly derived. When manual configuration is used for an SA, the SPI must be entered as a parameter.
SPID	Service Profile Identifier. Used only in Basic Rate Interface (BRI) implementations of ISDN. The SPID specifies the services available on the service provider switch and defines the feature set ordered when the ISDN service is provisioned.
split horizon	Method used in distance-vector networks to avoid routing loops. Each router does not advertise routes back to the neighbor from which it received them.
SPQ	Strict-priority queuing. A dequeuing method that provides a special queue that is serviced until it is empty. The traffic sent to this queue tends to maintain a lower latency and more consistent latency numbers than traffic sent to other queues. <i>See also</i> APQ.
SPT	Shortest-path tree. An algorithm that builds a network topology that attempts to minimize the path from one router (the root) to other routers in a routing area.
SQL	Structured query language. International standard language used to create, modify, and select data from relational databases.
src port	TCP or UDP port for the source IP address in a packet.

SRX software	Session and Resource Control software. Customizable Juniper Networks product with which service providers can rapidly deploy IP services—such as video on demand (VoD), IP television, stateful firewalls, Layer 3 VPNs, and bandwidth on demand (BoD)—to hundreds of thousands of subscribers over a variety of broadband access technologies. Formerly known as Service Deployment System software.
SS7	Signaling System 7. A protocol used in telecommunications for delivering calls and services.
SSAP	Source service access point. Device that identifies the origin of an LPDU on a DLSw network.
SSB	System and Switch Board. On an M20 router, a Packet Forwarding Engine component that performs route lookups and component monitoring and monitors FPC operation.
SSH	Secure Shell. A protocol that uses strong authentication and encryption for remote access across a nonsecure network. SSH provides remote login, remote program execution, file copy, and other functions. In a UNIX environment, SSH is intended as a secure replacement for rlogin, rsh, and rcp.
SSH/TLS	Secure Shell with Transport Layer Security. A combination of two standard methods used to secure communications over the Internet. TLS is the name of a standard protocol based on SSL 3.0 and is defined in RFC 2246. In combination, SSH/TLS is also known as SSHv2 and uses FIPS-restricted cipher sets in a FIPS environment.
SSL	Secure Sockets Layer. A protocol that encrypts security information using public-private key technology, which requires a paired private key and authentication certificate, before transmitting data across a network.
SSM	Source-specific multicast. A service that allows a client to receive multicast traffic directly from the source. Typically, SSM uses a subset of the PIM sparse-mode functionality along with a subset of IGMPv3 to create a shortest-path tree between the client and the source, but it builds the shortest-path tree without the help of a rendezvous point.
SSP	Switch-to-Switch Protocol. Protocol implemented between two DLSw routers that establishes connections, locates resources, forwards data, and handles error recovery and flow control.
SSRAM	Synchronous static random-access memory. Used for storing routing tables, packet pointers, and other data such as route lookups, policer counters, and other statistics to which the microprocessor needs quick access.
standard AAL5 mode	Transport mode that allows multiple applications to tunnel the protocol data units of their Layer 2 protocols over an ATM virtual circuit. You use this transport mode to tunnel IP packets over an ATM backbone. <i>See also</i> AAL5 mode, cell-relay mode, Layer 2 circuits, trunk mode.

starvation	Problem that occurs when lower-priority traffic, such as data and protocol packets, is locked out (starved) because a higher-priority queue uses all of the available transmission bandwidth.
stateful firewall	<i>See</i> stateful firewall filter and stateless firewall filter.
stateful firewall filter	Type of firewall filter that evaluates the context of connections, permits or denies traffic based on the context, and updates this information dynamically. Context includes IP source and destination addresses, port numbers, TCP sequencing information, and TCP connection flags. The context established in the first packet of a TCP session must match the context contained in all subsequent packets if a session is to remain active. <i>See also</i> stateless firewall filter.
stateful firewall recovery	Recovery strategy that preserves parameters concerning the history of connections, sessions, or application status before failure. <i>See also</i> stateless firewall recovery.
stateless firewall filter	Type of firewall filter that statically evaluates the contents of packets transiting the router and packets originating from or destined for the Routing Engine. Packets are accepted, rejected, forwarded, or discarded and collected, logged, sampled, or subjected to classification according to a wide variety of packet characteristics. Sometimes called access control lists (ACLs) or simply firewall filters, stateless firewall filters protect the processes and resources owned by the Routing Engine. A stateless firewall filter can evaluate every packet, including fragmented packets. In contrast to a stateful firewall filter, a stateless firewall filter does not maintain information about connection states. <i>See also</i> stateful firewall filter.
stateless firewall recovery	Recovery strategy that does not attempt to preserve the history of connections, sessions, or application status before failure. <i>See also</i> stateful firewall recovery.
static LSP	<i>See</i> static path.
static path	In the context of traffic engineering, a static route that requires hop-by-hop manual configuration. No signaling is used to create or maintain the path. Also called a static LSP.
static route	Explicitly configured route that is entered into the routing table. Static routes have precedence over routes chosen by dynamic routing protocols.
static RP	One of three methods of learning the rendezvous point (RP) to group address mapping in a multicast network. Each router in the domain must be configured with the required RP information.
STM	Synchronous transport module. CCITT specification for SONET at 155.52 Mbps.

STP	Spanning Tree Protocol. Defined in the IEEE standard 802.1D, the Spanning Tree Protocol is an OSI Layer 2 protocol that ensures a loop-free topology for any bridged LAN. This protocol creates a spanning tree within a mesh network of connected Layer 2 bridges (typically Ethernet switches), and disables the links that are not part of that tree, leaving a single active path between any two network nodes.
strict	In the context of traffic engineering, a route that must go directly to the next address in the path. (Definition from RFC 791, modified to fit LSPs.)
strict hop	Routers in an MPLS named path that must be directly connected to the previous router in the configured path.
strict-priority queue	<i>See</i> SPQ.
structured query language	<i>See</i> SQL.
STS	Synchronous transport signal. Synchronous transport signal level 1 is the basic building block signal of SONET, operating at 51.84 Mbps. Faster SONET rates are defined as STS-n, where n is an integer by which the basic rate of 51.84 Mbps is multiplied. <i>See also</i> SONET.
STU-C	Symmetric high-speed digital subscriber line (SHDSL) transceiver unit-central office. Equipment at the telephone company central office that provides SHDSL connections to remote user terminals.
STU-R	Symmetric high-speed digital subscriber line (SHDSL) transceiver unit-remote. Equipment at the customer premises that provides SHDSL connections to remote user terminals.
stub area	In OSPF, an area through which, or into which, AS external advertisements are not flooded.
sub-LSP	Part of a point-to-multipoint label-switched-path (LSP). A sub-LSP carries traffic from the main LSP to one of the egress PE routers. Each point-to-multipoint LSP has multiple sub-LSPs. <i>See also</i> point-to-multipoint LSP.
subnet mask	Number of bits of the network address used for the host portion of a Class A, Class B, or Class C IP address.
substrate value	Value that reduces the maximum allowable peak rate by limiting the HDLC-encapsulated payload. The substrate value must exactly match that of the remote channel service unit (CSU).
summary link advertisement	OSPF link-statement advertisement flooded throughout the advertisement's associated areas by area border routers to describe the routes that they know about in other areas.

SVC	Switched virtual connection. A dynamically established, software-defined logical connection that stays up as long as data is being transmitted. When transmission is complete, the software tears down the SVC. <i>See also</i> PVC.
switch	A network device that attempts to perform as much of the forwarding task in hardware as possible. The switch can function as a bridge (LAN switch), router, or some other specialized device, and forwards frames, packets, or other data units. <i>See also</i> bridge.
Switch Interface Board	<i>See</i> SIB.
switch-card chassis	<i>See</i> SCC.
Switch-to-Switch Protocol	<i>See</i> SSP.
switched virtual connection	<i>See</i> SVC.
Switching and Forwarding Module	<i>See</i> SFM.
symmetric high-speed digital subscriber line	<i>See</i> SHDSL.
Synchronous Digital Hierarchy	<i>See</i> SDH.
synchronous dynamic random-access memory	<i>See</i> SDRAM.
Synchronous Optical Network	<i>See</i> SONET.
synchronous static random-access memory	<i>See</i> SSRAM.
synchronous transport module	<i>See</i> STM.
synchronous transport signal	<i>See</i> STS.
sysid	System identifier. Portion of the ISO nonclient peer. The system ID can be any 6 bytes that are unique throughout a domain.
syslog	System log. A method for storing messages to a file for troubleshooting or record-keeping. It can also be used as an action within a firewall filter to store information to the messages file.

System and Switch Board	<i>See</i> SSB.
System Control Board	<i>See</i> SCB.
system ID	<i>See</i> sysid.
system log	<i>See</i> syslog.
System Network Architecture	<i>See</i> SNA.
T	
T-carrier	Generic designator for any of several digitally multiplexed telecommunications carrier systems originally developed by Bell Labs and used in North America and Japan.
T1	Basic physical layer protocol used by the Digital Signal level 1 (DS1) multiplexing method in North America. A T1 interface operates at a bit rate of 1.544 Mbps and can support 24 DS0 channels.
T3	Physical layer protocol used by the Digital Signal level 3 (DS3) multiplexing method in North America. A T3 interface operates at a bit rate of 44.736 Mbps.
TACACS+	Terminal Access Controller Access Control System Plus. Authentication method for validating users who attempt to access the router using telnet.
tail drop	Queue management algorithm for dropping packets from the input end (tail) of the queue when the length of the queue exceeds a configured threshold. <i>See also</i> RED.
TCM	Tricolor marking. Traffic policing mechanism that extends the functionality of class-of-service (CoS) traffic policing by providing three levels of drop precedence (loss priority or PLP) instead of two. There are two types of TCM: single-rate and two-rate. The JUNOS software currently supports two-rate TCM only. <i>See also</i> trTCM.
TCP	Transmission Control Protocol. Works in conjunction with the Internet Protocol (IP) to send data over the Internet. Divides a message into packets and tracks the packets from point of origin to destination.
TCP port 179	Well-known port number used by BGP to establish a peering session with a neighbor.
tcpdump	UNIX packet monitoring utility used by the JUNOS software to view information about packets sent or received by the Routing Engine.

TDMA	Time-Division Multiple Access. A type of multiplexing in which two or more channels of information are transmitted over the same link, where the channels take turns to use the link. Each link is allocated a different time interval (“slot” or “slice”) for the transmission of each channel. For the receiver to distinguish one channel from the other, some kind of periodic synchronizing signal or distinguishing identifier is required. <i>See also</i> GSM.
TEI	Terminal Endpoint Identifier. A terminal endpoint can be any ISDN-capable device attached to an ISDN network. The TEI is a number between 0 and 127, where 0 through 63 are used for static TEI assignment, 64 through 126 are used for dynamic assignment, and 127 is used for group assignment.
Terminal Access Controller Access Control System Plus	<i>See</i> TACACS + .
Terminal Endpoint Identifier	<i>See</i> TEI.
terminating action	Action in a routing policy or firewall filter that halts the logical software processing of a policy or filter.
terms	Used in a routing policy or firewall filter to segment the policy or filter into small match and action pairs.
Third-Generation Partnership Project	<i>See</i> 3GPP.
through	JUNOS software routing policy match type representing all routes that fall between the two supplied prefixes in the route filter.
Time-Division Multiple Access	<i>See</i> TDMA.
time-division multiplexed channel	Channel derived from a given frequency and transmitted over a single wire or wireless medium. The channel is preassigned a time slot whether or not there is data to transmit.
timeout timer	Used in a distance-vector protocol to ensure that the current route is still usable for forwarding traffic.
TNP	Trivial Network Protocol. A Juniper Networks proprietary protocol automatically configured on an internal interface by the JUNOS software. TNP is used to communicate between the Routing Engine and components of the Packet Forwarding Engine, and is critical to the operation of the router.
token-bucket algorithm	Used in a rate-policing application to enforce an average bandwidth while allowing bursts of traffic up to a configured maximum value.

ToS	Type of service. The method of handling traffic using information extracted from the fields in the ToS byte to differentiate packet flows.
totally stubby area	OSPF area type that prevents Type 3, 4, and 5 link-state advertisements (LSAs) from entering the nonbackbone area.
traffic engineering	Process of selecting the paths chosen by data traffic in order to balance the traffic load on the various links, routers, and switches in the network. (Definition from http://www.ietf.org/internet-drafts/draft-ietf-mpls-framework-04.txt .) <i>See also</i> MPLS.
traffic engineering class	In Differentiated Services-aware traffic engineering, a paired class type and priority.
traffic engineering class map	In Differentiated Services-aware traffic engineering, a map among the class types, priorities, and traffic engineering classes. The traffic engineering class mapping must be consistent across the Differentiated Services domain.
traffic policing	Examines traffic flows and discards or marks packets that exceed service-level agreements (SLAs).
traffic sampling	Method used to capture individual packet information of traffic flow at a specified time period. The sampled traffic information is placed in a file and stored on a server for various types of analysis. <i>See also</i> packet capture.
traffic shaping	Reduces the potential for network congestion by placing packets in a queue with a shaper at the head of the queue. Traffic shaping tools regulate the rate and volume of traffic admitted to the network. <i>See also</i> shaping rate.
transient change	Commit script-generated configuration change that is loaded into the checkout configuration, but not into the candidate configuration. Transient changes are not saved in the configuration if the associated commit script is deleted or deactivated. <i>See also</i> persistent change.
transient interface	Interface that can be configured on a routing platform depending on your network needs. Unlike a permanent interface that is required for router operation, a transient interface can be disabled or removed without affecting basic operation of the router. <i>See also</i> FPC, PIC, and permanent interface.
transit area	In OSPF, an area used to pass traffic from one adjacent area to the backbone, or to another area if the backbone is more than two hops away from an area.
transit router	In MPLS, any intermediate router in the LSP between the ingress router and the egress router.
Transmission Control Protocol	<i>See</i> TCP.

transport mode	IPsec mode of operation in which the data payload is encrypted, but the original IP header is left untouched. The IP addresses of the source or destination can be modified if the packet is intercepted. Because of its construction, transport mode can be used only when the communication endpoint and cryptographic endpoint are the same. VPN gateways that provide encryption and decryption services for protected hosts cannot use transport mode for protected VPN communications. <i>See also</i> tunnel mode.
transport plane	<i>See</i> data plane.
trap	Reports significant events occurring on a network device, most often errors or failures. SNMP traps are defined in either standard or enterprise-specific MIBs.
tricolor marking	<i>See</i> TCM.
triggered updates	Used in a distance-vector protocol to reduce the time for the network to converge. When a router has a topology change, it immediately sends the information to its neighbors instead of waiting for a timer to expire.
Triple Data Encryption Standard	<i>See</i> 3DES.
Trivial Network Protocol	<i>See</i> TNP.
trTCM	Two-rate TCM polices traffic according to the color classification (loss priority) of each packet. Traffic policing is based on two rates: the committed information rate (CIR) and the peak information rate (PIR). Two-rate TCM is defined in RFC 2698, <i>Two Rate Three Color Marker</i> . <i>See also</i> CIR, PIR.
trunk mode	Layer 2 circuit cell-relay transport mode that allows you to send ATM cells between ATM2 IQ interfaces over an MPLS core network. You use Layer 2 circuit trunk mode (as opposed to standard Layer 2 circuit cell-relay mode) to transport ATM cells over an MPLS core network that is implemented between other vendors' switches or routers. The multiple connections associated with a trunk increase bandwidth and provide failover redundancy. <i>See also</i> AAL5 mode, cell-relay mode, Layer 2 circuits, standard AAL5 mode.
Tspec object	RSVP message object that contains information such as the bandwidth request of the LSP as well as the minimum and maximum packets supported.
tunnel	Private, secure path through an otherwise public network.
tunnel endpoint	Last node of a tunnel where the tunnel-related headers are removed from the packet, which is then passed on to the destination network.

tunnel mode	IPsec mode of operation in which the entire IP packet, including the header, is encrypted and authenticated and a new VPN header is added, protecting the entire original packet. This mode can be used by both VPN clients and VPN gateways, and protects communications that come from or go to non-IPsec systems. <i>See also</i> transport mode.
tunnel services interface	Provides the capability of a Tunnel Services PIC on an AS PIC. <i>See</i> Tunnel Services PIC.
Tunnel Services PIC	Physical interface card that allows the router to perform the encapsulation and de-encapsulation of IP datagrams. The Tunnel Services PIC supports IP-IP, GRE, and PIM register encapsulation and de-encapsulation. When the Tunnel Services PIC is installed, the router can be a PIM rendezvous point (RP) or a PIM first-hop router for a source that is directly connected to the router.
tunneling protocol	Network protocol that encapsulates one protocol or session inside another. When protocol A is encapsulated within protocol B, A treats B as though it were a data-link layer. Tunneling can be used to transport a network protocol through a network that would not otherwise support it. Tunneling can also be used to provide various types of VPN functionality such as private addressing.
two-rate TCM	<i>See</i> trTCM.
TX Matrix platform	Routing platform that provides the centralized switching fabric of the routing matrix.
type of service	<i>See</i> ToS.

U

U interface	User reference point interface. A single-pair connection between the local ISDN provider and the customer premises equipment.
UDP	User Datagram Protocol. In TCP/IP, a connectionless transport layer protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols.
UME	UNI management entity. The code residing in the ATM devices at each end of a UNI (user-to-network interface) circuit that functions as an SNMP agent, maintaining network and connection information specified in a MIB.
UMTS	Universal mobile telecommunications system. Provides third-generation (3G), packet-based transmission of text, digitized voice, video, and multimedia, at data rates up to 2 Mbps.
UMTS Terrestrial Radio Access Network	<i>See</i> UTRAN.

UNI	User-to-network interface. ATM Forum specification that defines an interoperability standard for the interface between a router or an ATM switch located in a private network and the ATM switches located within the public carrier networks. Also used to describe similar connections in Frame Relay networks.
UNI management entity	<i>See</i> UME.
unicast	Operation of sending network traffic from one network node to another individual network node.
uninterruptible power supply	<i>See</i> UPS.
unit	JUNOS software syntax that represents the logical properties of an interface.
universal mobile telecommunications system	<i>See</i> UMTS.
unnumbered interface	Logical interface that is configured without an IP address.
Update message	BGP message that advertises path attributes and routing knowledge to an established neighbor.
update timer	Used in a distance-vector protocol to advertise routes to a neighbor on a regular basis.
UPS	Uninterruptible power supply. A device that sits between a power supply and a router or other device and prevents power-source events, such as outages and surges, from affecting or damaging the device.
upto	JUNOS software routing policy match type representing all routes that share the same most-significant bits and whose prefix length is smaller than the supplied subnet in the route filter.
User Datagram Protocol	<i>See</i> UDP.
UTC	Coordinated Universal Time. Historically referred to as Greenwich mean time (GMT), a high-precision atomic time standard that tracks Universal Time (UT) and is the basis for legal civil time all over the Earth. Time zones around the world are expressed as positive and negative offsets from UTC.
UTRAN	UMTS Terrestrial Radio Access Network. The WCDMA radio network in UMTS.

V

vapor corrosion inhibitor	<i>See</i> VCI.
variable bit rate	<i>See</i> VBR.
VBR	Variable bit rate. For ATM1 and ATM2 intelligent queuing (IQ) interfaces, data that is serviced at a varied rate within defined limits. VBR traffic adds the ability to statistically oversubscribe user traffic.
VC	Virtual circuit. A software-defined logical connection between two network devices that is not a dedicated connection but acts as though it is. It can be either permanent (PVC) or switched (SVC). VCs are used in ATM, Frame Relay, and X.25. <i>See also</i> VPI, VCI, PVC, SVC.
VCI	VCI can be either of the following: <ol style="list-style-type: none"> 1. Vapor corrosion inhibitor. Small cylinder packed with the router that prevents corrosion of the chassis and components during shipment. 2. Virtual circuit identifier. A 16-bit field in the header of an ATM cell that indicates the particular virtual circuit the cell takes through a virtual path. Also called a logical interface. <i>See also</i> VPI.
video on demand	<i>See</i> VOD.
video services router	<i>See</i> VSR.
virtual channel	Enables queuing, packet scheduling, and accounting rules to be applied to one or more logical interfaces. <i>See also</i> virtual channel group.
virtual channel group	Combines virtual channels into a group and then applies the group to one or more logical interfaces. <i>See also</i> virtual channel.
virtual circuit	Represents a logical connection between two Layer 2 devices in a network.
virtual circuit identifier	<i>See</i> VCI.
virtual connection	<i>See</i> VC.
virtual link	In OSPF, a link created between two routers that are part of the backbone but are not physically contiguous.
virtual local area network	<i>See</i> VLAN.
virtual loopback tunnel interface	<i>See</i> VT.

virtual path	Combination of multiple virtual circuits between two devices in an ATM network.
virtual path identifier	<i>See</i> VPI.
virtual private network	<i>See</i> VPN.
Virtual Router Redundancy Protocol	<i>See</i> VRRP.
virtual switch	A routing instance that can contain one or more bridge domains.
VLAN	<p>Virtual local area network. A logical group of network devices that appear to be on the same LAN, regardless of their physical location. VLANs are configured with management software, and are extremely flexible because they are based on logical, rather than physical, connections.</p> <p>VLANs span one or more ports on multiple devices. By default, each VLAN maintains its own Layer 2 forwarding database containing MAC addresses learned from packets received on ports belonging to the VLAN. <i>See also</i> bridge domain.</p>
VLAN-tagged frame	Tagged frame whose tag header carries both VLAN identification and priority information.
VOD	Video on demand. A unicast streaming video offering by service providers that enables the reception of an isolated video session per user with rewind, pause, and similar VCR-like capabilities.
VPI	Virtual path identifier. An 8-bit field in the header of an ATM cell that indicates the virtual path the cell takes. <i>See also</i> VCI.
VPLS	Virtual private LAN service. An Ethernet-based multipoint-to-multipoint Layer 2 VPN service used for interconnecting multiple Ethernet LANs across an MPLS backbone. VPLS is specified in the IETF draft <i>Virtual Private LAN Service</i> .
VPN	Virtual private network. A private data network that uses a public TCP/IP network, typically the Internet, while maintaining privacy with a tunneling protocol, encryption, and security procedures. <i>See also</i> tunneling protocol.
VRF instance	VPN routing and forwarding instance. A VRF instance for a Layer 3 VPN implementation consists of one or more routing tables, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of policies and routing protocols that determine what goes into the forwarding table.
VRF table	Routing instance table that stores VRF routing information. <i>See also</i> VRF instance.
VRRP	Virtual Router Redundancy Protocol. On Fast Ethernet and Gigabit Ethernet interfaces, allows you to configure virtual default routers.

- VSR** Video services router. A router used in a video services network to rout video streams between an access network and a metro or core network. The VSR is any M-series or MX-series router that supports the video routing package provided with JUNOS software Release 8.3 or later.
- VT** Virtual loopback tunnel interface. VT interface that loops packets back to the Packet Forwarding Engine for further processing, such as looking up a route in a VRF routing table or looking up an Ethernet MAC address. A virtual loopback tunnel interface can be associated with a variety of MPLS and VPN-related applications, including VRF routing instances, VPLS routing instances, and point-to-multipoint LSPs.

W

- WAN PHY** Wide Area Network Physical Layer Device. A physical layer device that allows 10-Gigabit Ethernet wide area links to use fiber-optic cables and other devices intended for SONET/SDH. *See also* LAN PHY and PHY.
- WAP** Wireless Application Protocol. A standard protocol that enables mobile users to access the Internet in a limited fashion if WAP is supported and enabled on the mobile device, server, and wireless network. WAP users can send and receive e-mail and access Web sites in text format only (WAP does not support graphics).
- warm standby** Method that enables one backup Adaptive Services (AS) PIC to support multiple active AS PICs, without providing guaranteed recovery times.
- wavelength-division multiplexing** *See* WDM.
- WCDMA** Wideband Code Division Multiple Access. Radio interface technology used in most third-generation (3G) systems.
- WDM** Wavelength-division multiplexing. Technique for transmitting a mix of voice, data, and video over various wavelengths (colors) of light.
- weighted round-robin** *See* WRR.
- Wideband Code Division Multiple Access** *See* WCDMA.
- Windows Internet Name Service** *See* WINS.
- WINS** Windows Internet Name Service. A Windows name resolution service for network basic input/output system (NetBIOS) names. WINS is used by hosts running NetBIOS over TCP/IP (NetBT) to register NetBIOS names and resolve NetBIOS names to Internet Protocol (IP) addresses.

WRR Weighted round-robin. Scheme used to decide the queue from which the next packet should be transmitted.

X

XENPAK Standard that defines a type of pluggable fiber-optic transceiver module that is compatible with the 10-Gigabit Ethernet (10 GbE) standard.

XENPAK module 10-Gigabit Ethernet fiber-optic transceiver. XENPAK modules are hot-insertable and hot-removable. *See also* MSA.

XENPAK Multisource Agreement *See* MSA.

**XENPAK-SR
10GBASE-SR XENPAK** Media type that supports a link length of 26 meters on standard Fiber Distributed Data Interface (FDDI) grade multimode fiber (MMF). Up to 300-meter link lengths are possible with 2000 MHz/km MMF (OM3).

**XENPAK-ZR
10GBASE-ZR XENPAK** Media type used for long-reach, single-mode (80–120 km) 10-Gigabit Ethernet metro applications.

XFP 10-Gigabit small form-factor pluggable transceiver. A transceiver that provides support for fiber-optic cables. XFPs are hot-insertable and hot-removable. *See also* SFP.

XML Extensible Markup Language. Language used for defining a set of markers, called tags, that define the function and hierarchical relationships of the parts of a document or data set.

XML Path Language *See* XPath.

XML schema Definition of the elements and structure of one or more Extensible Markup Language (XML) documents. Similar to a document type definition (DTD), but with additional information and written in XML.

XOR Exclusive or. A logical operator (exclusive disjunction) in which the operation yields the result of true when one, and only one, of its operands is true.

XPath Standard used in XSLT to specify and locate elements in the input document's XML hierarchy. XPath is fully described in the W3C specification at <http://w3c.org/TR/xpath>.

XSLT Extensible Stylesheet Language for Transformations. A standard for processing XML data developed by the World Wide Web Consortium (W3C). XSLT performs XML-to-XML transformations, turning an input XML hierarchy into an output XML hierarchy. The XSLT specification is on the W3C Web site at <http://www.w3c.org/TR/xslt>.

Z

zeroize Process of removing all sensitive information, such as cryptographic keys and user passwords, from a router running JUNOS-FIPS.