Juniper Networks Glossary

END USER LICENSE AGREEMENT

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

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

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

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

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

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

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

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

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

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

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the

---

Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

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

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

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

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

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

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

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

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

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

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

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

Table of Contents

Juniper Networks Glossary

Symbols

(S, G) Source (S) of the multicast packet and the destination multicast group address (G).

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. Data is encrypted with the first key, decrypted with the second key, and encrypted again with the third key. 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* Triple DES.

3G Wireless Third generation of wireless developments, in particular mobile phone standards and technology.

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 IEEE specification for "Q-in-Q" encapsulation and bridging of Ethernet frames.

802.1ah IEEE specification for media access control (MAC) address tunneling encapsulation and bridging of Ethernet frames across a Provider Backbone Bridge (PBB).

802.1p IEEE specification for enabling Layer 2 switches to prioritize traffic and perform dynamic multicast filtering.

802.1Q IEEE specification for adding virtual local area network (VLAN) tags to an Ethernet frame.

802.1X IEEE specification defining a mechanism that allows a supplicant (client) to connect to a wireless access point or wired switch (authenticator) so that the supplicant can provide authentication credentials that can be verified by an authentication server.

802.3ad IEEE specification that enables grouping of Ethernet interfaces at the physical layer to form a single link layer interface. *Also known as* a link aggregation group (LAG) or LAG bundle.

802.3ah IEEE specification defining Ethernet between the subscriber and the immediate service provider. *Also known as* Ethernet in the first or last mile.

A

AAA authentication, authorization, and accounting. Process framework used to standardize the control of access to computer resources, enforcement of policies, audit of usage, and ability to report. Authentication determines who the user is and whether to grant that user access to the network. Authorization determines what the user can do by giving you the ability to limit network services to different users. Accounting tracks the user's activities and provides an audit trail that can be used for billing for connection time or resources used. *See also* redirected authentication.

AAA profile Set of characteristics or commands that you can assign to domain names to control access for an incoming Point-to-Point Protocol (PPP) subscriber. You can create an AAA profile and map it between a PPP client's domain name and certain AAA services on given interfaces and control such things as domain name access to AAA authentication, use of domain name aliases, and other features. If no AAA profile is used, AAA continues as normal. The user's name and domain name are not changed as a result of an AAA profile mapping.

AAL Asynchronous Transfer Mode (ATM) Adaptation Layer. A collection of protocols that defines the conversion of user information into cells by segmenting upper-layer information into cells at the transmitter and reassembling them at the receiver. These protocols enable various types of traffic, including voice, data, image, and video, to run over an ATM network.

AAL5 mode ATM Adaptation Layer 5. One of four AALs recommended by the International Telecommunication Union—Telecommunication Standardization Sector (ITU-T), AAL5 is used predominantly for the transfer of classical IP over ATM, and 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. *See also* cell-relay mode, Layer 2 circuits, standard AAL5 mode, trunk mode.

ABR • area border router. Router that belongs to more than one area, with interfaces in the OSPF boundary between two or more areas. Both sides of any link always belong to the same OSPF area. *See also* OSPF.

• available bit rate. Rate used in ATM for traffic sources that demand low loss ratios but can accept larger delays. ABR uses bandwidth not used by constant bit rate (CBR) and variable bit rate (VBR). ABR uses best effort to send the maximum number of cells but does not guarantee cell delivery. *See also* CBR, VBR.

absolute URL URL that points to the exact location of a file or directory on the Internet, by name. *See also* relative URL.

AC access concentrator. Device that receives and forwards data for a network point of presence (POP). It often acts as a server that supports multiple T1 or E1 lines over one port, for example, a Juniper Networks E Series Broadband Services Router that acts as a server in a Point-to-Point Protocol over Ethernet (PPPoE) session.

access challenge Authentication method used to prove the identity of a user logging in to the network. When a user logs in, the network access server, wireless access point, or authentication server creates a "challenge," typically a random number sent to the client machine. The client software uses its password or a secret key to encrypt the challenge, using an encryption algorithm or a one-way hash function and sends the result back to the network (the "response"). The authentication system also performs the same cryptographic process on the challenge and compares its result to the response from the client. If they match, the authentication system has verified that the user has the correct password.

access concentrator AC. Device that receives and forwards data for a network point of presence (POP). It often acts as a server that supports multiple T1 or E1 lines over one port, for example, a Juniper Networks E Series Broadband Services Router that acts as a server in a Point-to-Point Protocol over Ethernet (PPPoE) session.

access lists Sequential collection of permit and deny conditions used to filter inbound or outbound routes. Files that provide filters that can be applied to route maps or distribution lists. They enable policies to be created, such as a policy to prevent forwarding of specified routes between the BGP-4 and IS-IS routing tables.

access messages Authorization and authentication (AA) messages that identify subscribers before the RADIUS server grants or denies them access to the network or network services. When an application requests user authentication, the request must have certain authenticating attributes, such as a user's name, password, and the particular type of service the user is requesting. This information is sent in the authentication request, using the RADIUS protocol, to the RADIUS server. In response, the RADIUS server grants or denies the request. *See also* accounting messages.

Access Node Control Protocol ANCP. Based on a subset of the General Switch Management Protocol (GSMP) in which IGMP is no longer terminated or proxied at the access node. Instead, IGMP passes through the access node transparently. *Also known as* Layer 2 control (L2C).

access point AP. Device that serves as a communication hub to connect 802.1X wireless clients to a wired network.

access point name APN. An element in the header of a GPRS tunneling protocol (GTP) packet that provides information about how to reach a network. It is composed of two elements: a network ID and an operator ID. 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.

ACCM asynchronous control character map. A 32-bit mask that represents control characters with ASCII values 0 through 31. It is an option negotiated by the Link Control Protocol (LCP) and used on asynchronous links such as telephone lines to identify control characters that must be escaped (replaced by a specific two-character sequence) to avoid being interpreted by equipment used to establish the link. *See also* APN.

accounting messages	Messages that identify service provisions and use on a per-user basis. They keep track of when a particular service is initiated and terminated for a specific user. RADIUS attributes are used by each group of accounting messages. *See also* access messages.
accounting, accounting services	In RADIUS, the process and method of tracking what the user did and when he did it. Accounting is used for collecting network data related to resource usage, as for an audit trail or for billing for connection time or resources used. *See also* broadcast accounting server, duplicate accounting server.
ACFC	Address and Control Field Compression. Compression method that 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, *The Point-to-Point Protocol (PPP). See also* PFC.
Activate Device wizard	Feature in the Juniper Networks Network and Security Manager (NSM) user interface that guides you through activating a modeled device.
active constituent	Constituent that is monitored or controlled by the shared shaper mechanism. *See also* constituent, inactive constituent.
active route	Route chosen from all routes in the routing table to reach a destination. Active routes are installed into the forwarding table.
active state	State of a switch route processor (SRP) module whereby data that was synchronized from the active SRP module to the standby SRP module during initialization remains synchronized through mirroring updates. *See also* SRP.
adaptive services	Set of services or applications that you can configure on an Adaptive Services PIC (AS PIC), including stateful firewall, Network Address Translation (NAT), intrusion detection service (IDS), Internet Protocol Security (IPsec), Layer 2 Tunneling Protocol (L2TP), and voice services. *See also* tunneling protocol.
Adaptive Services Module	ASM. On a Juniper Networks M7i Multiservice Edge Router, provides the same functionality as the AS PIC.
Add Device wizard	Feature in the NSM user interface that guides you through importing or modeling a new device.
add/drop multiplexer	ADM. SONET functionality that allows lower-level signals to be dropped from a high-speed optical connection.
Address and Control Field Compression	ACFC. Compression method that 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, *The Point-to-Point Protocol (PPP). See also* PFC.

address family identifier	AFI. Number assigned by IANA used to identify the protocol associated with an address family. In an MP-BGP update message, AFI is used with SAFI to identify the network layer protocol associated with the network address of the next hop and the semantics of the NLRI that follows. *See also* SAFI.
address match conditions	Use of an IP address as a match criterion in a routing policy or a firewall filter.
address object	Represents a component such as a workstation, router, switch, subnetwork, or any other object connected to the network. Use address book objects to specify the network components you want to protect.
address pool	In a NAT context, a group of IP addresses from which a NAT router obtains an address when dynamically creating a new translation.
Address Resolution Protocol	ARP. Protocol for mapping IPv4 addresses to media access control (MAC) addresses; dynamically binds the IP address (the logical address) to the correct MAC address. *See also* NDP.
address scope	Value used in some unicast and multicast IPv6 addresses that identifies the application suitable for the address. *See also* scope.
address shifting	Mechanism for creating a one-to-one mapping between any original address in one range of addresses and a specific translated address in a different range.
address spoofing	Technique for creating packets with a source IP address that is not the actual interface address. Attackers can use a spoofed IP address to perform DoS attacks while disguising their true address, or to take advantage of a trusted relationship between two hosts.
adjacency	Relationship between a pair of selected neighboring routers for exchanging routing information. Not every pair of neighboring routers is adjacent. A given router can have multiple adjacencies, but each adjacency consists of only two routers connected by one media segment. Packets that go between them do not have to pass through any other network devices. *See also* neighbor.
Adjacency-RIB-In	Logical software table that contains BGP routing information bases received from a specific neighbor.
Adjacency-RIB-Out	Logical software table that contains BGP routing information bases 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.
administrative distance	Integer (in the range 0–255) that is associated with each route known to a router. The distance represents how reliable the source of the route is considered to be. A lower value is preferred over a higher value. An administrative distance of 255 indicates no confidence in the source; routes with this distance are not installed in the routing table.

admission control	Accounting mechanism that tracks resource information on a router-wide basis. Prevents requests from being accepted when sufficient resources are not available. Admission control determines whether a setup request can be honored for an MPLS LSP with traffic parameters.
ADSL	asymmetrical digital subscriber line. Technology that allows 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	Juniper Networks Physical Interface Module (PIM) that supports Annex A, the portion of ITU-T Rec. G.992.1 that defines how ADSL works over twisted-pair copper (POTS) lines. *See* ITU-T Rec. G.992.1, ADSL interface.
ADSL Annex B PIM	Juniper Networks Physical Interface Module (PIM) that supports Annex B, the portion of ITU-T Rec. G.992.1 that defines how ADSL works over ISDN lines. *See* ITU-T Rec. G.992.1, ADSL interface.
ADSL interface	asymmetrical digital subscriber line interface. Physical WAN interface that connects a router to a digital subscriber line access multiplexer (DSLAM). The 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. The ADSL2 interface 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 and 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	AES. Defined in Federal Information Processing Standards (FIPS) PUB 197, the AES algorithm uses keys of 128, 192, or 256 bits to encrypt and decrypt data in blocks of 128 bits. Use AES in your VPNs when you need greater interoperability with other network security devices.
advertisement	Method used by a router to transmit basic information about itself, including IP address, network mask, and other data, to other devices on the network.
AES	Advanced Encryption Standard. Defined in Federal Information Processing Standards (FIPS) PUB 197. The AES algorithm uses keys of 128, 192, or 256 bits to encrypt and decrypt data in blocks of 128 bits. Use AES in your VPNs when you need greater interoperability with other network security devices.
AF	assured forwarding. A DiffServ component that determines the degree of reliability given a packet within the DiffServ domain. AF values are set as part of per-hop behavior (PHB) groups. *See also* PHB.

AFI
- authority and format identifier. Number that identifies the format and type of address being used.

- address family identifier. Number assigned by IANA used to identify the protocol associated with an address family. In an MP-BGP update message, AFI is used with SAFI to identify the network layer protocol associated with the network address of the next hop and the semantics of the NLRI that follows. *See also* SAFI.

AFR
assured flow rate. A Media Flow Controller option that, when enabled, ensures that video or other media content is delivered at a rate that is minimally needed for the media to play smoothly.

agent
SNMP agent. A managed device, such as a router, that collects and stores management information. The SNMP agent (SNMPv3) recognizes up to 32 usernames that can have one of the following security levels: no authentication and no privacy, authentication only, authentication and privacy.

aggregate route
Single entry in a routing table that represents a combination of groups of routes that have common addresses.

aggregate state
State of a router when it is one of multiple virtual BGP routing instances bundled into one address.

aggregated interface
Logical bundle of physical interfaces 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.

aggregation
Process of accumulating data or logical interfaces into a single, larger bundle (for example, higher-speed connections). The process of combining several different routes in such a way that only a single route advertises itself. This technique minimizes the size of the routing table for the router.

aggregator
Object used to bundle multiple routes under one common route generalized according to the value of the network mask.

aggressive aging
Mechanism to accelerate the timeout process when the number of sessions in the session table exceeds a specified high-watermark threshold. When the number of sessions in the table goes below a specified low-watermark threshold, the timeout process returns to normal.

aggressive mode
Internet Key Exchange (IKE) phase 1 negotiation mode that is faster than main mode because fewer messages are exchanged between peers and it enables support for fully qualified domain names when the router uses preshared keys. However, aggressive mode is less secure than main mode because it exposes identities of the peers to eavesdropping.*See also* main mode.

AH
authentication header. Component of the IPsec protocol used to verify that the data integrity of a packet has not changed, and to validate the identity of the sender. *See also* ESP.

AIS	alarm indication signal. Signal transmitted instead of the normal signal to maintain transmission continuity and to indicate to the receiving equipment that a transmission interruption (fault) has occurred either at the equipment originating the AIS signal or upstream of that equipment.
AIS cell	alarm indication signal cell. Type of ATM cell used to indicate a fault to the downstream endpoint.
alarm	Signal alerting you to conditions that might prevent normal operation. On the front of the chassis, the alarm signal is the yellow ALARM LED (when lit).
alarm condition	Failure event that triggers an alarm.
alarm indication signal	AIS. Signal transmitted instead of the normal signal to maintain transmission continuity and to indicate to the receiving equipment that a transmission interruption (fault) has occurred either at the equipment originating the AIS signal or upstream of that equipment.
alarm severity	Seriousness of an alarm. The level of severity of an alarm can be either major (red) or minor (yellow).
ALG	application layer gateway, application-level gateway. Security component in a firewall or Network Address Translation (NAT) used to enable certain legitimate applications to pass through a firewall or between NAT realms without being stopped by security checks. It intercepts and analyzes the specified traffic, allocates resources, and defines dynamic policies to permit the traffic to pass securely through the security device.
ALI	ATM line interface. Interface between ATM and 3G systems. *See also* ATM.
alternate priority queuing	APQ. 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. Because the other configured queues share the remaining 50 percent of the service time, queue starvation is usually avoided. *See also* SPQ.
American National Standards Institute	ANSI. Private organization that coordinates the development and use of voluntary consensus standards in the United States and is the United States' representative to the International Organization for Standardization (ISO). *See also* ISO.
American Standard Code for Information Interchange	ASCII. A code for representing English characters as numbers, with each letter assigned a number in the range 0–127.
AMT	Automatic Multicast Tunneling. Protocol that provides dynamic multicast connectivity between multicast-enabled networks across islands of unicast-only networks. AMT is described in detail in draft-ietf-mboned-auto-multicast-10.txt: *See also* Automatic IP Multicast Without Explicit Tunnels.
analyzer device	Device that receives mirrored traffic from E Series routers during packet mirroring. *Also called* the mediation device.

analyzer port	IP interface in analyzer mode on E Series routers used to direct mirrored traffic to the analyzer device during packet mirroring.
ANCP	Access Node Control Protocol. Based on a subset of the General Switch Management Protocol (GSMP) in which IGMP is no longer terminated or proxied at the access node. Instead, IGMP passes through the access node transparently. *Also known a*s Layer 2 control (L2C).
Annex M	TU-DMT-BIS Standard G.992.3 and ADSL2PLUS Standard G.992.5 that extends the capability of basic ADSL2 by doubling the number of upstream bits.
ANSI	American National Standards Institute. Private organization that coordinates the development and use of voluntary consensus standards in the United States and is the United States' representative to the International Organization for Standardization (ISO). *See also* ISO.
antispam	Any software, hardware, or process used to combat the proliferation of unsolicited bulk e-mail (spam) or to keep spam from entering a system.
antivirus	Software used to detect, delete, or neutralize computer-based viruses or other malware.
antivirus scanning	Method for detecting and blocking viruses in File Transfer Protocol (FTP), Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP)—including HTTP webmail—and Post Office Protocol version 3 (POP3) traffic. Juniper Networks offers an internal antivirus scanning solution.
any-source multicast	ASM. Method of allowing a multicast receiver to listen to all traffic sent to a multicast group, regardless of its source.
anycast address	Type of address in IPv6 used to send a packet to one recipient out of a set of recipients or interfaces on different nodes. An anycast transmission sends packets to only one of the interfaces associated with the address, not to all of them; typically to the closest interface, as defined by the routing protocol.
AP	access point. Device that serves as a communication hub to connect 802.1X wireless clients to a wired network.
API	application programming interface. A set of routines, protocols, and tools for building software applications.
APN	access point name. An element in the header of a GPRS tunneling protocol (GTP) packet that provides information about how to reach a network. It is composed of two elements: a network ID and an operator ID. 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 layer
- Seventh and highest level in the seven-layer OSI reference model for network protocol design that manages communication between application processes. This layer is the main interface for users to interact with application programs such as electronic mail, database managers, and file-server software. *See also* OSI.

- Fifth and highest level in the five-layer TCP/IP stack. This layer is used by most programs for network communication. Data is passed from the program in an application-specific format, then encapsulated into a transport layer protocol.

application layer gateway, application-level gateway
ALG. Security component in a firewall or Network Address Translation (NAT) used to enable certain legitimate applications to pass through a firewall or between NAT realms without being stopped by security checks. It intercepts and analyzes the specified traffic, allocates resources, and defines dynamic policies to permit the traffic to pass securely through the security device.

application programming interface
API. A set of routines, protocols, and tools for building software applications.

application-specific integrated circuit
ASIC. Specialized processor that performs specific functions on the router.

AppSecure
A suite of next-generation security capabilities for Juniper Networks SRX Series Services Gateways that utilize advanced application identification and classification to deliver greater visibility, enforcement, control, and protection over the network.

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. *See also* 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. *See also* ADM.

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.

- An OSPF area divides the internetwork into smaller, more manageable constituent pieces, reducing the amount of information each router must store and maintain about all other routers. When a router in the area needs information about another device in or out of the area, it contacts a special router that stores this information, called the Area Border Router (ABR).

- 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
ABR. Router that belongs to more than one area, with interfaces in the OSPF boundary between two or more areas. Both sides of any link always belong to the same OSPF area. *See also* OSPF.

area range
Sequence of IP addresses defined by a lower limit and an upper limit, indicating a series of addresses of devices existing within an area.

ARP	Address Resolution Protocol. Protocol for mapping IPv4 addresses to media access control (MAC) addresses; dynamically binds the IP address (the logical address) to the correct MAC address. *See also* NDP.
AS	autonomous system. Set of routers that use the same routing policy while running under a single technical administration (a routing domain). An AS runs interior gateway protocols (IGPs) such as RIP, OSPF, and IS-IS within its boundaries. ASs use exterior gateway protocols (EGPs) to exchange routing information with other ASs. Assigned a globally unique autonomous system number. *See also* AS number.
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 number	autonomous system number. A globally unique number assigned by the IANA that is used to identify an autonomous system (AS). The AS number enables an AS to exchange exterior routing information with neighboring ASs.
AS path	autonomous system path. In BGP, the route to a destination. It consists of the AS numbers of all routers that a packet must go through to reach a destination.
AS path access list	Access list used by a BGP routing instance to permit or deny packets sent by neighbor routing instances to the current virtual routing instance.
AS path attribute class	One of four classes of BGP path attributes: Well-Known Mandatory, Well-Known Discretionary, Optional Transitive, and Optional Non-Transitive.
AS path string	An identifier for an AS path, it is configured alongside an AS path access list ID.
AS PIC	Adaptive Services Physical Interface Card. The physical card on which you can configure a set of adaptive services or applications, including stateful firewall, Network Address Translation (NAT), intrusion detection service (IDS), Internet Protocol Security (IPsec), Layer 2 Tunneling Protocol (L2TP), and voice services.
ASBR	autonomous system boundary router. In OSPF, a router that exchanges routing information with routers in other ASs. The ASBR redistributes routing information received from other ASs throughout its own AS.
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. *See also* ASBR.
ASCII	American Standard Code for Information Interchange. A code for representing English characters as numbers, with each letter assigned a number in the range 0–127.
ASIC	application-specific integrated circuit. Specialized processor that performs specific functions on the router.

ASM	• Adaptive Services Module. On a Juniper Networks M7i Multiservice Edge Router, provides the same functionality as the AS PIC.
	• any-source multicast. Method of allowing a multicast receiver to listen to all traffic sent to a multicast group, regardless of its source.
assured flow rate	AFR. A Media Flow Controller option that, when enabled, ensures that video or other media content is delivered at a rate that is minimally needed for the media to play smoothly.
assured forwarding	AF. A DiffServ component that determines the degree of reliability given a packet within the DiffServ domain. AF values are set as part of per-hop behavior (PHB) groups. *See also* PHB.
assured rate	Quality of Service rate at which bandwidth is guaranteed until oversubscribed.
asymmetrical digital subscriber line	ADSL. Physical WAN interface that connects a router to a digital subscriber line access multiplexer (DSLAM). The 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.
asynchronous control character map	ACCM. A 32-bit mask that represents control characters with ASCII values 0 through 31. It is an option negotiated by the Link Control Protocol (LCP) and used on asynchronous links such as telephone lines to identify control characters that must be escaped (replaced by a specific two-character sequence) to avoid being interpreted by equipment used to establish the link. *See also* APN.
Asynchronous Transfer Mode	ATM. A high-speed multiplexing and switching method utilizing fixed-length cells of 53 octets to support multiple types of traffic.
Asynchronous Transfer Mode (ATM) Adaptation Layer	AAL. A collection of protocols that defines the conversion of user information into cells by segmenting upper-layer information into cells at the transmitter and reassembling them at the receiver. These protocols enable various types of traffic, including voice, data, image, and video, to run over an ATM network.
AT commands	Instructions for controlling modems, originally developed by Hayes, Inc. for their modems and sometimes called Hayes commands. Each command line begins with AT (an abbreviation of ATtention), signaling that it is a modem command. This command structure is a de facto industry standard for modems, with specific commands varying by manufacturer.
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 Adaptation Layer	Asynchronous Transfer Mode (ATM) Adaptation Layer or AAL. A collection of protocols that defines the conversion of user information into cells by segmenting upper-layer information into cells at the transmitter and reassembling them at the receiver. These protocols enable various types of traffic, including voice, data, image, and video, to run over an ATM network.

ATM Adaptation Layer 5	AAL5 mode. One of four AALs recommended by the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T), AAL5 is used predominantly for the transfer of classical IP over ATM, and 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. *See also* cell-relay mode, Layer 2 circuits, standard AAL5 mode, trunk mode.
ATM cell	Package of information that is always 53 octets long, unlike a frame or packet, which has a variable length.
ATM line interface	ALI. Interface between ATM and 3G systems.
ATM subinterface	Mechanism that enables a single physical ATM interface to support multiple logical interfaces.
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.
atomic aggregate	Object used by a BGP router to inform other BGP routers that the local system selected a generalized route.
atomic configuration	Fail-safe feature for devices running Juniper Networks ScreenOS Software. If the configuration deployment fails for any reason, the device automatically uses the last installed stable configuration. If the configuration deployment succeeds, but the device loses connectivity to the management system, the device rolls back to the last installed configuration. This minimizes downtime and ensures that NSM always maintains a stable connection to the managed device.
attack	An attempt to exploit vulnerabilities in computer hardware and software. Depending on the severity, the attack might completely disable your system, allow access to confidential information, or use your network to attack other networks. *See also* severity.
attack objects	Object that contains patterns of known attacks that can be used to compromise a network. Use attack objects in your firewall rules to enable security devices to detect known attacks and prevent malicious traffic from entering your network.
attenuation	Decrease in signal magnitude between two points, which can be along a radio path or a transmission line or between two devices.

attribute-value pair	AVP. A RADIUS attribute value carried in a RADIUS protocol message. The pair is a combination of a unique attribute—represented by an integer—and a value containing the actual value identified by the attribute.
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.
audit log target	Security device to which an audit log entry sent a directive.
audit log viewer	Module of the NSM user interface that displays records of administrative actions. Each audit log includes the date and time the administrative action occurred, the NSM administrator who performed the action, and the domain (global or a subdomain) in which the action occurred.
authentication	• In RADIUS, the process of determining who the user is, then determining whether to grant that user access to the network. The primary purpose is to bar intruders from networks. RADIUS authentication uses a database of users and passwords.
	• Process that verifies that data is not altered during transmission and ensures that users are communicating with the individual or organization that they believe they are communicating with. *See also* IPsec.
	• Simple Network Management Protocol version 3 (SNMPv3) term related to the user-based security model (USM). Authentication provides the following benefits:
	• Only authorized parties can communicate with each other. Consequently, a management station can interact with a device only if the administrator configured the device to allow the interaction.
	• Messages are received promptly; users cannot save messages and replay them to alter content. This prevents users from sabotaging SNMP configurations and operations. For example, users can change configurations of network devices only if authorized to do so.
authentication center	AUC. Part of the home location register (HLR) in third-generation (3G) systems; performs computations to verify and authenticate a mobile phone user.
authentication header	AH. Component of the IPsec protocol used to verify that the data integrity of a packet has not changed, and to validate the identity of the sender. *See also* ESP.
authentication retry	Feature of SSH that limits the number of times a user can try to correct incorrect information—such as a bad password—in a given connection attempt.
authentication server objects	Used to set a default authentication server for the global domain and each subdomain, or access an external RADIUS or SecurID system to provide authentication for NSM administrators and remote access server (RAS) users on your network.

authentication, authorization, and accounting	AAA. Process framework used to standardize the control of access to computer resources, enforcement of policies, audit of usage, and ability to report. Authentication determines who the user is and whether to grant that user access to the network. Authorization determines what the user can do by giving you the ability to limit network services to different users. Accounting tracks the user's activities and provides an audit trail that can be used for billing for connection time or resources used. *See also* redirected authentication.
authority and format identifier	AFI. Number that identifies the format and type of address being used.
authorization	In RADIUS, the process of determining what the user can do by giving a network administrator the ability to limit network services to different users.
auto-RP	Method of electing and announcing the rendezvous point-to-group address mapping in a multicast network. Junos OS supports this vendor-proprietary specification. *See also* RP.
autodetection	Process that determines the layers of each dynamic interface. Occurs when the router conditionally constructs interface layers based on the encapsulation type of the incoming packet. *Also called* autosensing.
autoinstallation	Automatic configuration of a device over the network from a preexisting configuration file created and stored on a configuration server—typically a Trivial File Transfer Protocol (TFTP) server. Autoinstallation occurs on a device that is powered on without a valid configuration (boot) file or that is configured specifically for autoinstallation. Autoinstallation is useful for deploying multiple devices on a network.
automatic commit mode	Feature of Juniper Networks JunosE Software in which the system automatically saves any change to the system configuration to nonvolatile storage (NVS), without affecting the command-line interface (CLI) prompt.
Automatic Multicast Tunneling	AMT. Protocol that provides dynamic multicast connectivity between multicast-enabled networks across islands of unicast-only networks. AMT is described in detail in Internet draft draft-ietf-mboned-auto-multicast-10.txt, *Automatic IP Multicast Without Explicit Tunnels (AMT)*.
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	APS. Technology used by SONET ADMs to protect against circuit faults between the ADM and a router and to protect against failing routers. *See also* ADM.
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	AS. Set of routers that use the same routing policy while running under a single technical administration (a routing domain). An AS runs interior gateway protocols (IGPs) such as RIP, OSPF, and IS-IS within its boundaries. ASs use exterior gateway protocols (EGPs) to exchange routing information with other ASs. Assigned a globally unique autonomous system number. *See* AS number.
autonomous system boundary router	ASBR. In OSPF, a router that exchanges routing information with routers in other ASs. The ASBR redistributes routing information received from other ASs throughout its own AS.
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.
available bit rate	ABR. Rate used in ATM for traffic sources that demand low loss ratios but can accept larger delays. ABR uses bandwidth not used by constant bit rate (CBR) and variable bit rate (VBR). ABR uses best effort to send the maximum number of cells but does not guarantee cell delivery. *See also* CBR, VBR.
AVP	attribute value pair. A RADIUS attribute value carried in a RADIUS protocol message. The pair is a combination of a unique attribute—represented by an integer—and a value containing the actual value identified by the attribute.

B

B-channel	bearer channel. A 64-Kbps channel used for voice or data transfer on an ISDN interface. *See also* D-channel.
B-MAC	Backbone source and destination MAC address fields found in the IEEE 802.1ah provider MAC encapsulation header.
B-RAS	broadband remote access server. Application responsible for aggregating the output from digital subscriber line access multiplexers (DSLAMs), providing user PPP sessions and PPP session termination, enforcing QoS policies, and routing traffic into an ISP's backbone network.
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. *See also* S-TAG.
B-VID	Specific VLAN identifier carried in a B-TAG.
BA classifier	behavior aggregate classifier. 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. *See also* 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 network	Central network; a network that connects other networks together.
backbone router	OSPF router with all operational interfaces within area 0.0.0.0.
backdoor	A mechanism installed on a host computer that facilitates unauthorized access to the system. Attackers who have already compromised a system can install a backdoor to make future attacks easier.
backdoor link	Private link between two routers. OSPF backdoor links typically serve as backup paths, providing a way for traffic to flow from one VPN site to the other only if the path over the backbone is broken. However, when the OSPF backdoor link connects two sites that are in the same OSPF area, the undesired result is that the path over the OSPF backdoor link is always preferred over the path over the backbone.
backplane	Hardware component that physically separates front and rear cavities inside the chassis, distributes power from the power supplies, and transfers packets and signals between router components that plug into it. *See also* redundancy midplane, midplane.
backup designated router	OSPF router on a broadcast segment that monitors the operation of the designated router (DR) and takes over its functions if the designated router fails.
backup router	Virtual Router Redundancy Protocol (VRRP) router available to take forwarding responsibility if the current master router fails. *See also* master router.
backward explicit congestion notification	BECN. 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. *See also* FECN.
baffle	Individual dividers and partitions inside a chassis that force cooling air to flow through the device in the optimal manner. A baffle is designed to direct cooling air to where it is needed most.
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 management	Policy management that rate-limits a classified packet flow at ingress to enforce ingress data rates below the physical line rate of a port. When the user configures a rate-limit profile, packets are tagged with a drop preference.
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* flexible bandwidth allocation.
	• 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.
bandwidth oversubscription	Feature of JunosE Software that enables line modules to operate at a rate dependent on the resources available rather than having all line modules operate at full line rate performance. Oversubscription enables a much more extensive combination of line modules in the router. *See also* oversubscription.
base station controller	BSC. Key network node in third-generation (3G) systems that supervises the functioning and control of multiple base transceiver stations.
base station subsystem	BSS. Composed of the base transceiver station (BTS) and base station controller (BSC).
Base Station System GPRS Protocol	BSSGP. Processes routing and quality-of-service (QoS) information for the base station subsystem (BSS).
base transceiver station	BTS. Mobile telephony equipment housed in cabinets and colocated with antennas. *Also known as* a radio base station.
Base64	Method used to encode digital certificate requests and certificates before they are sent to or from the certificate authority (CA).
baseline statistics	Starting point for statistics collection after resetting protocol or application statistics and counters to zero. *See also* statistics baseline.
basic NAT	Least secure type of traditional Network Address Translation (NAT). Provides translation for IP addresses only and places the mapping into a NAT table. *See also* NAT.
Basic Rate Interface	BRI. ISDN service intended for home and small enterprise applications. ISDN BRI consists of two 64-Kbps B-channels to carry voice or data and one 16-Kbps D-channel for control and signaling.
bastion host	Special purpose computer on a network specifically set up to withstand attacks, generally a hardened system configured with minimal software to support a single network service.
BBD	blade bay data. 60-byte text string stored in the JCS1200 management module nonvolatile random access memory (NVRAM) that conveys configuration information to the Routing Engines (blades) in the JCS1200 chassis.
BBL	bearer bandwidth limit. Maximum bandwidth available for voice traffic on an interface when dynamic call admission control is configured on the interface. *See also* dynamic CAC.
bearer bandwidth limit	BBL. Maximum bandwidth available for voice traffic on an interface when dynamic call admission control is configured on the interface. *See also* dynamic CAC.

bearer channel | B-channel. A 64-Kbps channel used for voice or data transfer on an ISDN interface. *See also* D-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. *See also* FECN.

behavior aggregate classifier | BA classifier. 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. *See also* multifield classifier.

Bellcore | Bell Communications Research. 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.

BER | bit error rate. Percentage of received bits in error compared to the total number of bits received.

BERT | bit error rate test. 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.

best effort | Traffic class in which the network forwards as many packets as possible in as reasonable a time as possible. By default, packets that are not assigned to a specific traffic class are assigned to the best-effort traffic class.

best path | When multiple routes to a given destination exist, BGP must determine which of these routes is the best. BGP puts the best path in its routing table and advertises that path to its BGP neighbors. If only one route exists to a particular destination, BGP installs that route. If multiple routes exist for a destination, BGP uses tie-breaking rules to decide which one of the routes to install in the BGP routing table.

best-effort queue | Queue associated with the best-effort traffic class for a logical interface.

best-effort scheduler node | Scheduler node associated with a logical interface and traffic class group pair, and where the traffic class group contains the best-effort traffic class. *Also known as* best-effort node.

BFD | Bidirectional Forwarding Detection. Protocol that uses control packets and shorter detection time limits to more rapidly detect failures in a network.

BGP | Border Gateway Protocol. Exterior gateway protocol (EGP) used to exchange routing information among routers in different autonomous systems. Can act as a label distribution protocol for MPLS.

BGP messages Routing information that BGP speakers exchange with each other over a BGP session. BGP uses five message types:

- Open BGP messages—Used to establish and negotiate certain parameters for the BGP session after the underlying TCP session has been established.

- Update messages—Used to announce routes to prefixes that the speaker can reach and to withdraw routes to prefixes that it can no longer reach. The most important message in the BGP protocol.

- Keepalive messages—Periodic messages to determine whether the underlying TCP connection is still up.

- Notification messages—Sent to a BGP peer to terminate a BGP session (either because the speaker has been configured to do so or because it has detected some error condition).

- Route-refresh messages—Sent to BGP peers that advertise their route-refresh capability, enabling the BGP speaker to apply modified or new policies to the refreshed routes.

BGP neighbor Another device on the network that is running BGP. There are two types of BGP neighbors:

- Internal neighbors—in the same autonomous system

- External neighbors—in different autonomous systems

A reliable connection is required between neighbors and is achieved by creating a TCP connection between the two. The handshake that occurs between the two prospect neighbors evolves through a series of phases or states before a true connection can be made.

BGP peer BGP neighbor that has been explicitly configured for a BGP speaker. BGP peers do not have to be directly connected to each other to share a BGP session.

BGP peer group Two or more BGP peers that share a common set of update policies. They are grouped together to reduce configuration overhead and to conserve system resources when updates are generated.

BGP route Prefix and a set of path attributes. Sometimes referred to as a path, although that term technically refers to one of the path attributes of that route.

BGP session TCP connection over which routing information is exchanged according to the rules of the BGP protocol. When two BGP speakers are in the same autonomous system, the BGP session is an internal BGP session, or IBGP session. When two BGP speakers are in different autonomous systems, the BGP session is an external BGP session, or EBGP session. BGP uses the same types of message on IBGP and EBGP sessions, but the rules for when to send and how to interpret each message differ slightly. *See also* IBGP session, EBGP session.

BGP speaker Router configured to run the BGP routing protocol. Unlike some other routing protocols, BGP speakers do not automatically discover each other and begin exchanging information. Instead, each BGP speaker must be explicitly configured with a set of BGP peers with which it exchanges routing information.

Bidirectional Forwarding Detection	BFD. Protocol that uses control packets and shorter detection time limits to more rapidly detect failures in a network.
bidirectional NAT	Type of NAT that adds support for DNS to basic NAT, allowing public hosts to initiate sessions into the private network, usually to reach servers intended for public access.
binding	Collection of configuration parameters, including at least an IP address, assigned by a DHCP server to a DHCP client. A binding can be dynamic (temporary) or static (permanent). Bindings are stored in the DHCP server's binding database.
bit error rate	BER. Percentage of received bits in error compared to the total number of bits received.
bit error rate test	BERT. 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.
bit field match conditions	Use of fields in the header of an IP packet as match criteria in a firewall filter.
bit rate	A data rate expressed as the number of bits transmitted per second: Kbps (kilobits per second). One bit is 1,024 bytes, so bit rate can also be expressed as KB/s (kilobytes per second).
BITS	Building Integrated Timing Source (or Supply, or System). Dedicated timing source that synchronizes all equipment in a particular building; a method for distributing precise timing synchronization among telecommunications equipment.
blacklist	Profile of checklist attributes that cause an AAA server to reject an authentication request. For example, a blacklist profile might cause the rejection of calling station phone numbers or IP addresses that are blocked by the AAA server.
blade	Routing Engine in the Juniper Networks JCS1200 Control System chassis that runs the Junos OS. The JCS1200 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 JCS1200 management module nonvolatile random access memory (NVRAM) that conveys configuration information to the Routing Engines (blades) in the JCS1200 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.
BMA	broadcast multiaccess. Network on which broadcast or multicast packets can be sent, enabling each device on a network segment to communicate directly with every other device on that segment. *See also* NBMA.

BOOTP	bootstrap protocol. 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 loader	Program that loads the operating system for a device at startup.
bootstrap protocol	BOOTP. 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 router	Single router in a multicast network responsible for distributing candidate rendezvous point information to all PIM-enabled routers.
Border Gateway Protocol	BGP. Exterior gateway protocol (EGP) used to exchange routing information among routers in different autonomous systems. Can act as a label distribution protocol for MPLS.
BPDU	bridge protocol data unit. 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 service intended for home and small enterprise applications. ISDN BRI consists of two 64-Kbps B-channels to carry voice or data and one 16-Kbps D-channel for control and signaling.
bridge	• 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. *See also* switch. • 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. *See also* broadcast domain, VLAN.
bridge group	Collection of bridge interfaces stacked on Ethernet layer 2 network interfaces (ports) to form a broadcast domain. Each bridge group has its own set of forwarding tables and filters and functions as a logical transparent bridging device.
bridge group interface	Association of one or more network interfaces with a bridge group. *Also called* a bridge interface.
bridge protocol data unit	BPDU. Spanning Tree Protocol hello packet that is sent out at intervals to exchange information across bridges and detect loops in a network topology.

bridged Ethernet interface	Link layer protocol that allows multiple upper-layer interface types (IP, PPPoE, and CBF) to be simultaneously multiplexed over the same interface.
bridged IP	Link layer protocol used to manage IP packets that are encapsulated inside an Ethernet frame running over a permanent virtual circuit (PVC).
broadband remote access server	B-RAS. Application responsible for aggregating the output from digital subscriber line access multiplexers (DSLAMs), providing user PPP sessions and PPP session termination, enforcing QoS policies, and routing traffic into an ISP's backbone network.
broadband services router	BSR. A router used for subscriber management and edge routing.
broadcast	Operation of sending network traffic from one network node to all other network nodes.
broadcast accounting server	In RADIUS, server that sends the accounting information to a group of virtual routers. An accounting virtual router group can contain up to four virtual routers, and the E Series router supports a maximum of 100 virtual router groups. The accounting information continues to be sent to the duplicate accounting virtual router, if one is configured. You might use broadcast accounting to send accounting information to a group of your private accounting servers. *See also* duplicate accounting server.
broadcast address	IPv4 type of address that enables a device to send a packet to all hosts on a subnetwork.
broadcast circuits	Circuits that use designated routers and are represented as virtual nodes in the network topology. They require periodic database synchronization. By default, IS-IS treats the broadcast link as LAN media and tries to bring up the LAN adjacency even when the interface is configured as unnumbered or only a single neighbor exists on that link. *See also* point-to-point circuits.
broadcast domain	Logical division of a computer network, in which all nodes can reach each other by broadcast at the data link layer.
broadcast multiaccess	BMA. Network on which broadcast or multicast packets can be sent, enabling each device on a network segment to communicate directly with every other device on that segment. *See also* NBMA.
broadcast network	Network of many routers that can send, or broadcast, a single physical message to all the attached routers. Pairs of routers on a broadcast network are assumed to be able to communicate with each other. On broadcast networks, the OSPF router dynamically detects its neighbor routers by sending hello packets to the multicast address 224.0.0.5. The hello protocol elects a designated router and a backup designated router for the network. Ethernet is an example of a broadcast network.
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 radio base station.
buffer	Memory space for handling data in transit. Buffers compensate for differences in processing speed between network devices by temporarily handling bursts of data until they can be processed by slower devices.
buffer overflow	Event that occurs when a program or process attempts to store more data in a buffer than the buffer was intended to hold. Buffers provide temporary data storage and are designed to contain a finite amount of data; any additional data can overflow the buffer zone and attempt to enter nearby buffers, corrupting or overwriting that buffer's existing data.
Building Integrated Timing Source (or Supply, or System)	BITS. Dedicated timing source that synchronizes all equipment in a particular building; a method for distributing precise timing synchronization among telecommunications equipment.
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 OS 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.
bypass tunnel	Single label-switched path (LSP) used to back up a set of LSPs by bypassing specific links in the LSP. In the event of a failure in any link of the protected RSVP-TE LSP (the primary LSP), MPLS redirects traffic to the associated bypass tunnel in tens of milliseconds.

C

C-VLAN	customer VLAN. A stacked VLAN, defined by IEEE 802.1ad, that contains an outer tag corresponding to the S-VLAN and an inner tag corresponding to the C-VLAN. A C-VLAN often corresponds to customer premises equipment (CPE). Scheduling and shaping is often used on a C-VLAN to establish minimum and maximum bandwidth limits for a customer. *See also* S-VLAN.
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 (MPLS). Bandwidth and bandwidth-related resource monitoring and accounting facility that determines whether a setup request can be honored for an MPLS LSP with traffic parameters.

- connection admission control (ATM). Set of actions that the network takes during connection setup or renegotiation. ATM networks use CAC to determine whether to accept a connection request, based on whether allocating the connection's requested bandwidth would cause the network to violate the traffic contracts of existing connections.

CAIDA
Cooperative Association for Internet Data Analysis. 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
CAC. Bandwidth and bandwidth-related resource monitoring and accounting facility that determines whether a setup request can be honored for an MPLS LSP with traffic parameters.

Call Detail Record
CDR. Contains data unique to a specific call, such as origination, termination, length, and time of day.

callback
Alternative feature to dial-in that enables a device to call back the caller from the remote end of a backup ISDN connection. Instead of accepting a call from the remote end of the connection, the router rejects the call, waits a configured period of time, and calls a number configured on the router's dialer interface. *See also* 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. During dial-in, the router matches the caller ID of the incoming call against all caller IDs configured on its dialer interfaces, and accepts only those calls whose caller IDs are configured.

CAM
content-addressable memory. Memory chip in which content is compared in each bit cell, allowing for very fast table lookups.

CAMA
centralized automatic message accounting. Recording of toll calls at a central point.

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 OS 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 (RP). This information is unicast to the bootstrap router for the multicast domain.

capability negotiation
Enables devices to communicate without having prior knowledge of the capabilities of the remote entity. This method is used by BGP peers to determine whether they share the same capabilities, and whether the session will be maintained or terminated, given the respective capabilities of the peers. BGP speakers advertise their capabilities in BGP open messages.

carrier-of-carriers VPN Virtual private network (VPN) service provided to a network service provider that supplies Internet or VPN service to an end customer, establishing a two-tiered relationship between a provider carrier and a customer carrier. The provider carrier provides a VPN backbone network for the customer carrier (Tier 1). The customer carrier, in turn, provides Layer 3 VPN or Internet services to its end customers (Tier 2). For a carrier-of-carriers VPN, the customer's sites are configured within the same autonomous system (AS).

CB Control Board. On a Juniper Networks T640 Core Router 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. *See also* XOR.

CBF connection-based forwarding. A method of forwarding frames in which forwarding decisions are made using only the identity of the ingress interface. No part of a packet's contents is used to determine how a packet should be forwarded.

CBR constant bit rate. An ATM service category that supports a constant and guaranteed rate to transport services such as video or voice, as well as circuit emulation, requiring rigorous timing control and performance parameters. For ATM1 and ATM2 IQ interfaces, data 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.

CC cells continuity check cells. Cells that provide continual monitoring of a connection on a segment or from end to end.

CCC circuit cross-connect. Junos OS 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).

CCITT International Telegraph and Telephone Consultative Committee. Now known as ITU-T (Telecommunication Standardization Sector), organization that coordinates standards for telecommunication on behalf of the ITU (International Telecommunication Union). The ITU is a United Nations specialized agency. ITU-T is a subcommittee of ITU. *See also* ITU-T.

CDMA code division multiple access. Digital cellular technology that uses spread-spectrum techniques for digital transmission of radio signals, for example, between a mobile telephone and a base transceiver station (BTS). Unlike competing systems that use TDMA (time division multiple access), such as GSM (Global System for Mobile Communications), CDMA does not assign a specific frequency to each user. Instead, every channel uses the full available spectrum. Individual conversations are encoded with a pseudo-random digital sequence. CDMA consistently provides better capacity for voice and data communications than other commercial mobile technologies, allowing more subscribers to connect at any given time.

CDMA2000 Radio transmission and backbone technology standards for the evolution to third-generation (3G) mobile networks.

CDN	content delivery network, content distribution network. A system of computers networked together across the Internet that cooperate transparently to deliver content to end users, most often for the purpose of improving performance, scalability, and cost efficiency.
CDR	Call Detail Record. Contains data unique to a specific call, such as origination, termination, length, and time of day.
CDV	cell delay variation. Difference between a cell's expected and actual transfer delay. CDV determines the amount of jitter. (JunosE QoS term)
CDVT	cell delay variation tolerance. Acceptable tolerance of CDV (jitter). (JunosE QoS term)
CE	customer edge. Customer router 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 delay variation	CDV. Difference between a cell's expected and actual transfer delay. CDV determines the amount of jitter. (JunosE QoS term)
cell delay variation tolerance	CDVT. Acceptable tolerance of CDV (jitter). (JunosE QoS term)
cell loss priority	CLP. ATM cell bit that communicates the loss priority of the payload. A value of zero (0) specifies that the cell not be discarded if it encounters congestion as it moves through the network. A value of one (1) specifies that the network can drop the cell when congestion is encountered.
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. *See also* AAL5 mode, Layer 2 circuits, standard AAL5 mode, trunk mode.
Central Management Console	CMC. A feature of the Juniper Networks Media Flow Controller management interface that allows you to push configurations to a number of Media Flow Controllers from a central interface.
central office	CO. Local telephone company building that houses circuit switching equipment used for subscriber lines in a given area.
centralized automatic message accounting	CAMA. Recording of toll calls at a central point.

certificate	Electronic document that binds a person or entity to a public key using a digital signature.
certificate authority	CA. 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).
certificate revocation list	CRL. 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 use of digital certificates and signatures that have been compromised.
CFEB	Compact Forwarding Engine Board. In Juniper Networks M7i and M10i Multiservice Edge Routers, CFEB 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. 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	CHAP. Server-driven, three-step authentication of remote users that depends on a shared secret password that resides on both the server and the client.
change of authorization	CoA. RADIUS messages that dynamically modify session authorization attributes, such as data filters.
channel	Communication circuit linking two or more devices, providing 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. *See also* 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	CSU/DSU. A channel service unit connects a digital phone line to a multiplexer or other digital signal device. A data service unit connects data terminal equipment (DTE) to a digital phone line.
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, with time slot 0 reserved for framing.

channelized interface   Wideband interface divided into many smaller channels to carry different streams of data. It is a subdivision of a larger interface, minimizing the number of 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. Server-driven, three-step authentication of remote users that depends on a shared secret password that resides on both the server and the client.

chassis alarm   Predefined alarm triggered by a physical condition on the device such as a power supply failure, excessive component temperature, or media failure.

chassis daemon   chassisd. Junos OS process responsible for managing the interaction of the router's physical components.

chassisd   chassis daemon. Junos OS process responsible for managing the interaction of the router's physical components.

CHD   computed historical datapoints. Traffic samples that have been computed in some manner, such as summation and averaging.

CIDR   Classless Interdomain Routing. Addressing method that interprets an IP address in two parts: a prefix that identifies the network, followed by notation that indicates the host address and mask; for example, 10.12.8.3/16. CIDR replaces the traditional class structure of IP addresses, in which address allocations were based on octet (8-bit) boundary segments of the 32-bit IP address. In CIDR, the boundary between the network and host portions of an IP address can be on any bit boundary and they have no class restrictions, enabling more efficient use of the IP address space.

CIP   Connector Interface Panel. Panel that contains connectors for the Routing Engines, BITS interfaces, and alarm relay contacts on some M Series and T Series routers.

cipher block chaining   CBC. 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. *See also* XOR.

CIR   committed information rate. Specifies the average rate at which packets are admitted to the network. Each packet is counted as it enters the network. 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. *See also* trTCM, PIR.

circuit cross-connect	CCC. Junos OS 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).
circuit-level proxy	Generic proxy (intermediary cache or relay between a Web client and a Web server) that is not associated with a specific application; instead, a circuit-level proxy can support multiple applications.
Cisco HDLC	Cisco High-Level Data Link Control. Bit-oriented synchronous data-link layer protocol that governs information transfer. Developed by ISO, it specifies a data encapsulation method on synchronous serial links using frame characters and checksums. It is a protocol that has been implemented by many different network equipment vendors. *See also* SLARP.
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.
CISPR	International Special Committee on Radio Interference. An International Electrotechnical Commission (IEC) committee whose principal task is to prepare standards that offer protection of radio reception from interference sources at the higher end of the frequency range (from 9 kHz and above), such as electrical appliances of all types; the electricity supply system; industrial, scientific, and electromedical RF; broadcasting receivers (sound and TV); and IT equipment (ITE).
CIST	common and internal spanning tree. 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. *See also* MSTI.
CLACL	classifier control list. Specifies the criteria by which the router defines a packet flow.
class of service	CoS. 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. *See also* QoS.
Class Selector code point	CSCP. Eight Differentiated Services code point (DSCP) values of the form *xxx*000 (where *x* can be 0 or 1). Defined in RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.
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. *Also known as* a traffic class.
class-of-service process	cosd. Process that enables the routing platform to provide different levels of service to applications based on packet classifications.

classification	Process of taking in a single data stream and sorting it into multiple output substreams. 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. *See also* 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.
classifier control list	CLACL. Specifies the criteria by which the router defines a packet flow.
classifier group	Policy rules that make up a policy list.
Classless Interdomain Routing, classless routing	CIDR. Addressing method that interprets an IP address in two parts: a prefix that identifies the network, followed by notation that indicates the host address and mask; for example, 10.12.8.3/16. CIDR replaces the traditional class structure of IP addresses, in which address allocations were based on octet (8-bit) boundary segments of the 32-bit IP address. In CIDR, the boundary between the network and host portions of an IP address can be on any bit boundary and they have no class restrictions, enabling more efficient use of the IP address space.
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.
clear to send	CTS. Signalling message transmitted in response to an RTS (request to send) message that enables the sender of the RTS message to begin data transfer
cleartext	Unencrypted form of encrypted text. *Also known as* plaintext.
CLEC	competitive local exchange carrier. Company that competes with an 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 entering commands for configuring and monitoring the routing protocol software.
CLI access class	Security level that grants access to specific CLI commands, such as for packet mirroring.
CLI-based packet mirroring	Type of packet mirroring in which an authorized user uses the router CLI commands to configure and manage packet mirroring.
client	Node or software program (front-end device) that requests services from a server. *See also* SNMP client.
client peer	In a BGP route reflection, a member of a cluster that is not the route reflector. *See also* nonclient peer.

CLNP Connectionless Network Protocol. ISO-developed protocol for OSI connectionless network service. A network layer protocol used by CLNS to handle data at the transport layer. CLNP is the OSI equivalent of IP.

CLNS Connectionless Network Service. OSI network layer service that enables data transmission without establishing a circuit and that routes messages independently of any other messages. 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.

CLP cell loss priority. ATM cell bit that communicates the loss priority of the payload. A value of zero (0) specifies that the cell not be discarded if it encounters congestion as it moves through the network. A value of one (1) specifies that the network can drop the cell when congestion is encountered.

cluster Route reflector and its clients (BGP) that have been grouped together. Consists of one system that acts as a route reflector, along with any number of client peers. Clients peer only with a route reflector and do not peer outside their cluster. Route reflectors peer with clients and other route reflectors within a cluster; outside a cluster they peer with other reflectors and other routers that are neither clients nor reflectors. The client peers receive their route information only from the route reflector system. Routers in a cluster do not need to be fully meshed. *See also* route reflector, route reflector client.

cluster list List of paths recorded as a packet travels through a BGP route reflector cluster.

CMC Central Management Console. A feature of the Juniper Networks Media Flow Controller management interface that allows you to push configurations to a number of Media Flow Controllers from a central interface.

CnS, CNS Control and Status messages. 3G modem messages used to configure, set parameters, query status, receive event notification, and control traffic of event notifications for the 3G modem device.

CO central office. Local telephone company building that houses circuit switching equipment used for subscriber lines in a given area.

CoA change of authorization. RADIUS messages that dynamically modify session authorization attributes, such as data filters.

code division multiple access CDMA. Digital cellular technology that uses spread-spectrum techniques for digital transmission of radio signals, for example, between a mobile telephone and a base transceiver station (BTS). Unlike competing systems that use TDMA (time division multiple access), such as GSM (Global System for Mobile Communications), CDMA does not assign a specific frequency to each user. Instead, every channel uses the full available spectrum. Individual conversations are encoded with a pseudo-random digital sequence. CDMA consistently provides better capacity for voice and data communications than other commercial mobile technologies, allowing more subscribers to connect at any given time.

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.

cold restart
: Result of a standby SRP module becoming active without high availability (HA) being configured (no switchover from active SRP). Similar to a cold start, except:

- The standby SRP becomes active much more quickly because the configuration is already loaded in the standby SRP memory and the device is running.

- Line module software is reloaded, so it takes additional time for the newly active SRP to become fully operational.

See also graceful restart, warm restart.

color-aware rate limit
: Type of rate limit that can change the algorithm used, depending on the color of the incoming packet.

color-based thresholding
: Process that assigns precedence to packets in JunosE QoS. Packets within the router are tagged with a drop precedence: committed—green; conformed—yellow; exceeded—red. When the queue fills above the exceeded threshold, the router drops red packets, but still queues yellow and green packets. When the queue fills above the conformed drop threshold, the router queues only green packets.

color-blind rate limit
: Type of rate limit that runs the same algorithm for all packets, regardless of their color. *See also* rate-limit hierarchy.

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 privileges
: Feature of the CLI in E Series routers. Command privileges fall within one of the following levels:

- 0—Allows you to execute the help, enable, disable, and exit commands.

- 1—Allows you to execute commands in User Exec mode plus commands at level 0.

- 5—Allows you to execute Privileged Exec show commands plus the commands at levels 1 and 0.

- 10—Allows you to execute all commands except support commands (provided by Juniper Networks Customer Service), or the privilege command to assign privileges to commands.

- 15—Allows you to execute support commands and assign privileges to commands.

command-line interface
: CLI. Interface provided for entering commands for configuring and monitoring the routing protocol software.

commit
: Junos OS 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	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 OS.
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 OS configuration statements that execute your intended operation.
committed action	In a rate-limit profile, action that drops, transmits, marks (IP and IPv6), or marks-exp (MPLS) when traffic flow does not exceed the rate. The mark value is not supported for hierarchical rate limits, and the transmit values-—conditional, unconditional, and final-—are supported only on hierarchical rate limits.
committed information rate	CIR. Specifies the average rate at which packets are admitted to the network. Each packet is counted as it enters the network. 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. *See also* trTCM, PIR.
common and internal spanning tree	CIST. 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. *See also* MSTI.
Common Criteria	International standard (ISO/IEC 15408) for computer security. *See also* EAL3.
Common Criteria Evaluation Assurance Level 3	EAL3. Compliance requirement defined by Common Criteria. Higher levels have more stringent requirements. *See also* Common Criteria.
Common Language Equipment Identifier	CLEI. Inventory code used to identify and track telecommunications equipment.
Common Open Policy Service	COPS. A query-and-response protocol used to exchange policy information between a policy server and its clients.
Common Open Policy Service usage for policy provisioning	COPS-PR. An IETF standard where the policy enforcement point (PEP) requests policy provisioning when the operational state of the interface and DHCP addresses change.
Common Vulnerabilities and Exposures	CVE. Dictionary of publicly known information security vulnerabilities and exposures that is international in scope and free for public use.

community	• In BGP, a logical group of prefixes or destinations that share a common attribute; used to simplify a routing policy. Community members can be on different networks and in different autonomous systems. BGP allows you to define the community to which a prefix belongs. A prefix can belong to more than one community. The community attribute lists the communities to which a prefix belongs. Community information is included as one of the path attributes in BGP update messages.
	• 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.
community list	Sequential collection of permit and deny conditions. Each condition describes the community number to be matched. The router tests the community attribute of a route against the conditions in a community list one by one. The first match determines whether the router accepts (the route is permitted) or rejects (the route is denied) a route having the specified community. Because the router stops testing conditions after the first match, the order of the conditions is critical. If no conditions match, the router rejects the route.
Compact Forwarding Engine Board	CFEB. In Juniper Networks M7i and M10i Multiservice Edge Routers, CFEB provides route lookup, filtering, and switching to the destination port.
CompactFlash drive	Nonvolatile memory card in Juniper Networks M Series, MX Series, T Series, and J Series platforms used for storing a copy of the Junos OS and the current and most recent router configurations. It also typically acts as the primary boot device.
competitive local exchange carrier	CLEC (pronounced "*see*-lek"). Company that competes with an already-established local telecommunications business by providing its own network and switching.
complete sequence number PDU	CSNP. Packet that contains a complete list of all the LSPs in the IS-IS database.
compound explicit shared shaper	One of four types of shared shapers, in which the software selects constituents based on the shared priority and shared weight configured using a JunosE command. If no attributes are specified, the software supplies a shared priority consistent with the legacy scheduler configuration. *See also* compound implicit shared shaper, simple explicit shared shaper, simple implicit shared shaper, CSNP.
compound implicit shared shaper	One of four types of shared shapers, in which the software selects constituents automatically. If a node exists in a given traffic-class group, the node is active and the queues stacked above it are inactive constituents. *See also* compound explicit shared shaper, simple explicit shared shaper, simple implicit shared shaper, CSNP.
compound shared shaping	Hardware-assisted mechanism that controls bandwidth for all scheduler objects associated with the subscriber logical interface. *See also* shared shaping, simple shared shaping.
Compressed Real-Time Transport Protocol	CRTP. 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, *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*.

computed historical datapoints	CHD. Traffic samples that have been computed in some manner, such as summation and averaging.
concurrent routing and bridging	CRB. Mechanism whereby an E Series router can route a protocol among a group of interfaces in one bridge group and concurrently bridge the same protocol among a separate group of interfaces in a different bridge group on the router.
Concurrent Versions System	CVS. Widely used version control system for software development or data archives.
confederation	In BGP, group of systems that appears to external autonomous systems as a single autonomous system. A set of sub-ASs is established within an AS to reduce mesh overhead. BGP peers within each sub-AS are fully meshed, but the sub-ASs do not have to be fully meshed within the AS. *See also* route reflection.
configlet	Small, static configuration file that contains information about how a security device can connect to NSM.
configuration caching	Mechanism that prevents the system from being partially configured with changes in the event of a reset. When a script or macro begins execution, the resulting configuration changes are automatically cached in system RAM rather than being committed to nonvolatile storage (NVS). When the script or macro completes execution, the cache is flushed as a background operation, saving the configuration changes to NVS.
configuration group	Collection of configuration statements whose inheritance can be directed in the rest of the device configuration. The same group can be applied to different sections of the configuration, and different sections of one group's configuration statements can be inherited in different places in the configuration.
configuration management server	Remote server used to configure Juniper Networks routers when using the NETCONF XML Management Protocol or the Junos XML Management Protocol.
configuration mode	Junos OS mode that allows a user to alter the router's current configuration.
conflict	Problem that occurs when an address within the IP address pool is being used by a host that does not have an associated binding in the DHCP server's database. Addresses with conflicts are removed from the pool and logged in a conflicts list until you clear the list.
conformed action	In a rate-limit profile, an action that drops, transmits, marks (IP and IPv6), or marks-exp (MPLS) when traffic flow exceeds the rate but not the excess burst. The mark value is not supported for hierarchical rate limits, and the transmit values-—conditional, unconditional, and final-—are supported only on hierarchical rate limits.
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.
connection admission control	CAC. Bandwidth and bandwidth-related resource monitoring and accounting facility that determines whether a setup request can be honored for an MPLS LSP with traffic parameters. *Also known as* call admission control.

connection-based forwarding	CBF. A method of forwarding frames in which forwarding decisions are made using only the identity of the ingress interface. No part of a packet's contents is used to determine how a packet should be forwarded.
connection-oriented protocol	Protocol that exchanges control information with a remote computer to verify that the remote computer is ready to receive data before the originating computer sends the data.
Connectionless Network Protocol	CLNP. ISO-developed protocol for OSI connectionless network service. A network layer protocol used by CLNS to handle data at the transport layer. CLNP is the OSI equivalent of IP.
Connectionless Network Service	CLNS. OSI network layer service that enables data transmission without establishing a circuit and that routes messages independently of any other messages. 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.
connectionless protocol	Protocol, such as IP, that does not exchange control information to establish an end-to-end connection before transmitting data.
connectivity fault management	CFM. 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.
Connector Interface Panel	CIP. Panel that contains connectors for the Routing Engines, BITS interfaces, and alarm relay contacts on some M Series and T Series routers.
constant bit rate	CBR. An ATM service category that supports a constant and guaranteed rate to transport services such as video or voice, as well as circuit emulation, requiring rigorous timing control and performance parameters. For ATM1 and ATM2 IQ interfaces, data 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.
constituent	Scheduler node or queue associated with a logical interface. A shared shaper is configured for a logical interface; all queues and scheduler nodes associated with that logical interface are constituents of the shared shaper. *See also* active constituent; inactive constituent.
constrained path	In traffic engineering, a path determined by using the CSPF algorithm. The Explicit Route Object (ERO) carried in the RSVP packets contains the constrained path information. *See also* ERO.
Constrained Shortest Path First	CSPF. MPLS algorithm modified to take into account specific restrictions when calculating the shortest path across the network.
Constraint-Based Routed Label Distribution Protocol	CR-LDP. Traffic engineering signaling protocol for MPLS IP networks. CR-LDP provides mechanisms for establishing explicitly routed label switched paths (LSPs).
constraint-based routed label-switched path	CR-LSP. Explicitly routed label switched path (LSP) established by means of CR-LDP

constraint-based routing (MPLS)	Mechanism to establish paths based on certain criteria (explicit route, QoS parameters). The standard routing protocols can be enhanced to carry additional information to be used when running the route calculation.
content addressable memory	CAM. Memory chip in which content is compared in each bit cell, allowing for very fast table lookups.
content delivery network	CDN, content distribution network. A system of computers networked together across the Internet that cooperate transparently to deliver content to end users, most often for the purpose of improving performance, scalability, and cost efficiency.
content distribution network	content delivery network, CDN. A system of computers networked together across the Internet that cooperate transparently to deliver content to end users, most often for the purpose of improving performance, scalability, and cost efficiency.
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. *See also* XSLT.
context-sensitive help	Function of the router's command-line interface (CLI) that allows a user to request information about the Junos OS hierarchy. You can access context-sensitive help in both operational and configuration mode.
continuity check cells	CC cells. Cells that provide continual monitoring of a connection on a segment or from end to end.
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 and Status messages	CnS, CNS. 3G modem messages used to configure, set parameters, query status, receive event notification, and control traffic of event notifications for the 3G modem device.
Control Board	CB. On a Juniper Networks T640 Core Router routing node, part of the host subsystem that provides control and monitoring functions for router components.
control plane	Virtual network path used to set up, maintain, and terminate data plane connections. *See also* data plane.
convergence	The time it takes all the routers in a network to receive the information and update their routing tables after a topology change.
Cooperative Association for Internet Data Analysis	CAIDA. 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.

cooperative route filtering	Enables a BGP speaker to send an inbound route filter to a peer and have the peer install it as an outbound filter on the remote end of the session. *Also known as* outbound route filtering, ORF.
Coordinated Universal Time	UTC. 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.
COPS	Common Open Policy Service (Protocol). A query-and-response protocol used to exchange policy information between a policy server and its clients.
COPS-PR	COPS usage for policy provisioning. An IETF standard where the policy enforcement point (PEP) requests policy provisioning when the operational state of the interface and DHCP addresses change.
core	Central backbone of the network.
core dump file	In E Series routers, file that indicates which module has failed by referencing that module's hardware slot number (the slot number designation on the system backplane). This slot number is different from the chassis slot number that appears on the front of the chassis and in screen displays.
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. *See also* QoS.
cosd	Class-of-service process that enables the routing platform to provide different levels of service to applications based on packet classifications.
cost	Unitless number assigned to a path between neighbors, based on throughput, round-trip time, and reliability. The sum of path costs between source and destination hosts determines the overall path cost. OSPF uses the lowest cost to determine the best path.
CPE	customer premises equipment. Telephone, modem, router, or other service provider equipment located at a customer site.
CR-LDP	Constraint-Based Routed Label Distribution Protocol. Traffic engineering signaling protocol for MPLS IP networks. CR-LDP provides mechanisms for establishing explicitly routed label-switched paths (LSPs).
CR-LSP	constraint-based routed label-switched path. Explicitly routed label-switched path (LSP) established by means of CR-LDP.
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.

CRB	concurrent routing and bridging. Mechanism whereby an E Series router can route a protocol among a group of interfaces in one bridge group and concurrently bridge the same protocol among a separate group of interfaces in a different bridge group on the router.
CRC	cyclic redundancy check. Error-checking technique that uses a calculated numeric value to detect errors in transmitted data.
CRC errors	Indicates the number of packets generating a cyclic redundancy code error processed through the security device over the selected interface.
Critical Security Parameter	CSP. On routers running Junos-FIPS software, a collection of cryptographic keys and passwords that must be protected at all times.
CRL	certificate revocation list. 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 use of digital certificates and signatures that have been compromised.
CRTP	Compressed Real-Time Transport Protocol. 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, *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*.
Crypto Accelerator Module	Processor card that speeds up certain cryptographic IP Security (IPsec) services on some Juniper Networks devices. For supported cryptographic algorithms, refer to the product documentation for the devices that support the Crypto Accelerator Module.
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. MPLS algorithm 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 data terminal equipment (DTE) to a digital phone line.
CTS	clear to send (signal). Signalling message transmitted in response to an RTS (request to send) message that enables the sender of the RTS message to begin data transfer.
customer edge	CE. Customer router connected to the service provider network.

customer edge device	CE 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.
customer premises equipment	CPE. Telephone, modem, router, or other service provider equipment located at a customer site.
customer VLAN	C-VLAN. A stacked VLAN, defined by IEEE 802.1ad, that contains an outer tag corresponding to the S-VLAN and an inner tag corresponding to the C-VLAN. A C-VLAN often corresponds to customer premises equipment (CPE). Scheduling and shaping is often used on a C-VLAN to establish minimum and maximum bandwidth limits for a customer. *See also* S-VLAN.
Customized Applications of Mobile Enhanced Logic	CAMEL. An ETSI standard for GSM networks that enhances the provision of Intelligent Network services.
CVE	Common Vulnerabilities and Exposures. Dictionary of publicly known information security vulnerabilities and exposures that is international in scope and free for public use.
CVS	Concurrent Versions System. Widely used version control system for software development or data archives.
cyclic redundancy check	CRC. Error-checking technique that uses a calculated numeric value to detect errors in transmitted data.

D

D-channel	delta channel. 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. *See also* 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 OS, 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 those peers without adversely affecting the route convergence time for stable routes.
data carrier detect	DCD. Hardware signal defined by the RS-232C standard that indicates that the device, usually a modem, is online and ready for transmission.
data circuit-terminating equipment	DCE. Device, such as a modem, that provides the interface between a circuit and data terminal equipment (DTE). *Also known as* data communications equipment.
data communications equipment	DCE. Device, such as a modem, that provides the interface between a circuit and data terminal equipment (DTE). *Also known as* data circuit-terminating equipment.
Data Encryption Standard	DES. Method for encrypting information using a 56-bit key. Considered to be a legacy method and insecure for many applications. *See also* 3DES.

Data Encryption Standard-Cipher Block Chaining	DES-CBC. Method for encrypting single DES keys.
data exchange interface	DXI. Specification developed by the switched megabit data services (SMDS) interest group to define the interaction between internetworking devices and CSUs/DSUs that are transmitting over an SMDS access line.
data link layer	Second level in the seven-layer OSI reference model for network protocol design and in the five-layer TCP/IP protocol stack. This layer provides the functional and procedural means to transfer data between network entities by splitting data into frames to send on the physical layer and receiving acknowledgment frames. It performs error checking and retransmits frames not received correctly. In general, it controls the flow of information across the link, providing an error-free virtual channel to the network layer. *See also* OSI.
data link switching	DLSw. Method of tunneling IBM System Network Architecture (SNA) and NetBIOS traffic over an IP network, used because Junos OS does not support NetBIOS. *See also* tunneling protocol.
data model	DM. In NSM, an XML file that contains configuration data for an individual device. The DM is stored in the NSM Device Server. When you create, update, or import a device, the GUI Server edits the Abstract Data Model (ADM) to reflect the changes, then translates that information to the DM.
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. *See also* control plane.
data service unit	channel service unit, CSU/DSU. A channel service unit connects a digital phone line to a multiplexer or other digital signal device. A data service unit connects data terminal equipment (DTE) to a digital phone line.
data set ready	DSR. One of the control signals on a standard RS-232C connector that indicates whether the DCE is connected and ready to start.
data stream inversion	Collection of data bits in a data stream that are inverted for transmission.
data terminal equipment	DTE. RS-232-C interface that a computer uses to exchange information with a serial device, such as a computer, host, or terminal, that communicates with DCE. At the terminal end of a data transmission, DTE comprises the transmit and receive equipment. *See also* DCE.
data terminal ready signal	DTR signal. Sent over a dedicated wire (RS-232 connection) from a computer (or terminal) to a transmission device to indicate that the computer is ready to receive data.
data-driven multicast distribution tree tunnel	data-MDT. Multicast tunnel created and deleted based on defined traffic loads and designed to ease loading on the default MDT tunnel.
data-link connection identifier	DLCI. 10-bit channel number attached to data frames to inform a Frame Relay network how to route the data in a Frame Relay virtual connection (a logical interface).

data-MDT	data-driven multicast distribution tree (MDT) tunnel. 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.
datagram	Packet format defined by IP.
dcd	device control process. Junos OS interface process (daemon).
DCD	data carrier detect. Hardware signal defined by the RS-232C standard that indicates that the device, usually a modem, is online and ready for transmission.
DCE	data communications equipment, data circuit-terminating equipment. Device, such as a modem, that provides the interface between a circuit and data terminal equipment (DTE).
DCU	destination class usage. 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.
DDoS	distributed denial of service attack. Attack, typically a flood, from multiple source points. A DDoS attack can be more effective in disrupting services than a DoS, because the flood of incoming attacks are coming from multiple sources.
DE	discard-eligible bit. In a Frame Relay network, header bit that notifies devices on the network that traffic can be dropped during congestion to ensure the delivery of higher priority traffic (those without the DE bit set).
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 OS uses a default value of 40 seconds for this timer.
dead peer detection	DPD. Method that recognizes the loss of the primary IPsec Internet Key Exchange (IKE) peer and establishes a secondary IPsec tunnel to a backup peer. It is a keepalive mechanism that enables the E Series router to detect when communication to a remote IPsec peer has been disconnected. DPD enables the router to reclaim resources and to optionally redirect traffic to an alternate failover destination. If DPD is not enabled, traffic continues to be sent to the unavailable destination. *Also known as* IKE keepalive.
Deep Inspection	DI. Firewall methodology that builds on the strength of stateful inspection, integrating intrusion prevention technology to provide application-level attack protection at the network perimeter. The Deep Inspection firewall can efficiently perform network security functions as well as analysis on the application message to determine whether to accept or deny traffic.

Deep Inspection action Action performed by a security device when the permitted traffic matches an attack object specified in the rule. Deep Inspection actions include drop connection, drop packet, close client, and so on.

Deep Inspection profile DI profile. Contains predefined attack object groups (created by Juniper Networks), and your own custom attack object groups. After creating the DI Profile, you add the Profile object in the Rule Option column of a firewall rule.

default address Router address that is used as the source address on unnumbered interfaces.

default configuration Configuration that takes place on a device that cannot locate a configuration (boot) file. You can set up two default configuration files for autoinstallation on the device: **network.conf** to specify IP address-to-hostname mappings for devices on the network, and **router.conf** to provide just enough configuration for your subsequent Telnet access.

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 Difference or discrepancy. For example, in NSM, the difference between the configuration running on the physical device and the configuration in NSM is called the delta.

delta channel D-channel. 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. *See also* B-channel, BRI.

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. *See also* multicast.

demilitarized zone DMZ. Physical or logical subnet used as an additional layer of security between an organization's network and an untrusted network (often the Internet); a neutral zone used to secure a network from external access. An attacker only has access to equipment in the DMZ.

denial of service DoS. System security breach in which network services become unavailable to users.

denial-of-service attack DoS attack. Any attempt to deny valid users access to network or server resources by using up all the resources of the network element or server. Typically, an attacker sends a flood of information to overwhelm a service system's resources, causing the server to ignore valid service requests.

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. *See also* sparse mode.

Dense Port Concentrator DPC. Network interface–specific card that can be installed in the router.

dense wavelength division multiplexing	DWDM. Technology that enables data from different sources to be carried together on an optical fiber, with each signal carried on its own separate wavelength.
DES	Data Encryption Standard. Method for encrypting information using a 56-bit key. Considered to be a legacy method and insecure for many applications. *See also* 3DES.
DES-CBC	Data Encryption Standard-Cipher Block Chaining. Method for encrypting single DES keys.
designated intermediate system	DIS. An IS-IS router that is elected by priority on an interface basis. In the case of a tie, the router with the highest MAC address becomes the DIS. DIS is analogous to the designated router in OSPF, although the election process and adjacencies within multiaccess media differ significantly. DIS assists broadcast routers to synchronize their IS-IS databases.
designated router	DR

- Router on a subnet that is selected to control multicast routes for the sources and receivers on the subnet. If several routers are present, the selected DR is the router with the highest priority. If the DR priorities match, the router with the highest IP address is selected as the DR. The source's DR sends PIM register messages from the source network to the rendezvous point (RP). The receiver's DR sends PIM join and PIM prune messages from the receiver network toward the RP.

- 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 topology databases maintained on the other routers.

destination class usage	DCU. 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.
destination prefix length	Number of bits of the network address used for the host portion of a CIDR IP address.
destination service access point	DSAP. Identifies the destination for which a logical link control protocol data unit (LPDU) is intended.
device administrator	Person who uses an interface to control and manage a network security device.
device control process	dcd. Junos OS interface process (daemon).
device discovery rules	Sets of rules that define subnets or ranges of IP addresses to scan for devices in your network.
Device Management Interface	DMI. In NSM, a common, secure management interface used by all device families. DMI is based on a common protocol and device-specific schemas for configuration, inventory management, logging, and status monitoring. DMI schemas can be updated without the need to upgrade NSM.
Device Monitor	Displays information in NSM about individual devices, their configuration and connection status, and memory usage.

Device Server In NSM, component of the management system that handles communication between the GUI server and the device, collects data from the managed devices on your network, formats configuration information sent to your managed device, and consolidates log and event data.

DF do not fragment (bit). One-bit flag in the IP datagram header that specifies if a datagram should be fragmented. A value of zero (0) indicates to fragment the datagram; a value of one (1) indicates not to fragment the datagram.

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. Mechanism through which hosts using TCP/IP can obtain protocol configuration parameters automatically from a DHCP server on the network; allocates IP addresses dynamically so that they can be reused when no longer needed.

DHCP equal access mode Mode in which a DHCP local server works with the Juniper Networks Service Deployment System (SDX) software to provide an advanced subscriber configuration and management service. In equal access mode, the router enables access to non-PPP users. Non-PPP equal access requires the use of the E Series router DHCP local server and SDX software, which communicates with a RADIUS server.

DHCP external server Server that enables an E Series router not running DHCP relay or DHCP proxy server to monitor DHCP packets and keep information for subscribers based on their IP and MAC addresses. When this server application is used, all DHCP traffic to and from the external server is monitored by the router. The services provided by integrating the E Series router DHCP external server application with SDX software are similar to those provided when the DHCP local server is integrated with SDX software. This application is used with other features of the router to provide subscriber management.

DHCP options Configuration settings sent within a DHCP message from a DHCP server to a DHCP client.

DHCP proxy client Configuration that enables the router to obtain an IP address from a DHCP server for a remote PPP client. Each virtual router (acting as a DHCP proxy client) can query up to five DHCP servers. For PPP users, the router acts as a DHCP client to obtain an address for the user.

DHCP relay client Enhanced component of DHCP relay that manages host routes for DHCP clients, including selecting the single most appropriate offer from multiple DHCP servers.

DHCP server Host that provides an IP address and configuration settings to a DHCP client. A J Series or SRX Series device is a DHCP server.

DHCP standalone mode Mode in which the DHCP local server operates as a basic DHCP server. Clients are not authenticated by default; however, you can optionally configure the DHCP local server to use AAA authentication for the incoming clients.

dhcpd — DHCP process that implements the DHCP client, allowing the device to obtain IP addresses from the network DHCP server, set other configuration parameters, manage TCP/IP settings propagation, and display client-related information.

DI — Deep Inspection. Firewall methodology that builds on the strength of stateful inspection, integrating intrusion prevention technology to provide application-level attack protection at the network perimeter. The DI firewall can efficiently perform network security functions as well as analysis on the application message to determine whether to accept or deny traffic.

DI profile — Deep Inspection profile. Contains predefined attack object groups (created by Juniper Networks), and your own custom attack object groups. After creating the DI Profile, you add the Profile object in the Rule Option column of a firewall rule.

Diagnostic Mode — DM. Qualcomm protocol specification and mechanism used to collect debug logs from Sierra 3G wireless modem firmware.

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 a device to receive calls from the remote end of a backup ISDN connection. The remote end of the ISDN call might be a service provider, a corporate central location, or a customer premises equipment (CPE) branch office. All incoming calls can be verified against caller IDs configured on the router's dialer interface. *See also* callback.

dial-on-demand routing (DDR) backup — Feature that provides a device 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. *See also* dialer filter, dialer watch.

dial-out route — Route definition that contains the dial-out target, as well as a domain name and profile. The domain name is used in the initial Access Request message. The profile is used to create the IP/Point-to-Point Protocol (PPP) stack for the dial-out session.

dial-out session — Control entity for a triggered IP flow that is used to manage the establishment of an associated L2TP session for dial-out.

dial-out target — Virtual router context and an IP address prefix, for which the arrival of an IP packet (a dial-out trigger) initiates a dial-out session.

dial-out trigger — IP packet that initiates a dial-out session.

dialed number identification service — DNIS. If users have a called number associated with them, the router searches the domain map for the called number. If it finds a match, the router uses the matching domain map entry information to authenticate the user. If the router does not find a match, it searches the domain map using normal processing.

dialer filter	Stateless firewall filter that enables dial-on-demand routing backup when applied to a physical ISDN interface and its dialer interface is configured as a passive static route. The passive static route has a lower priority than dynamic routes. If all dynamic routes to an address are lost from the routing table and the router receives a packet for that address, the dialer interface initiates an ISDN backup connection and sends the packet over it. *See also* dial-on-demand routing (DDR) backup, floating static route.
dialer interface	Logical interface for configuring dialing properties and the control interface for a backup ISDN connection.
dialer pool	One or more physical interfaces that are associated with a dialer profile.
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. *See also* dial-on-demand routing (DDR) backup.
DID	direct inward dialing. Feature of a trunk line that allows incoming calls to be routed directly to selected stations without help from an attendant.
Differentiated Services	DiffServ. An architecture that provides assured forwarding and expedited forwarding by classifying packets into one of a small number of aggregated flows or traffic classes for which you can configure different QoS characteristics. The Juniper Networks QoS architecture extends DiffServ to support edge features such as high-density queuing. 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).
Differentiated Services aware	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.
Differentiated Services code point	DSCP, 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.
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 key exchange	Feature of SSH that provides server authentication by protecting against hackers who interject mimics to obtain your password, so that you can be confident that you are connected to your own router. A method of key exchange whereby an 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. An architecture based on RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers* that provides assured forwarding and expedited forwarding by classifying packets into one of a small number of aggregated flows or traffic classes for which you can configure different QoS characteristics. The Juniper Networks QoS architecture extends DiffServ to support edge features such as high-density queuing. 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).
digital signal	DS. Discontinuous signal used in direct sequence spread spectrum modulation, *also known as* direct sequence code division multiple access (DS-CDMA). DS-CDMA is one of two approaches to spread spectrum modulation for digital signal transmission over the airwaves. In direct sequence spread spectrum, the stream of information to be transmitted is divided into small pieces, each of which is allocated across to a frequency channel across the spectrum.
digital signal level 0	DS0. 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.
digital signal level 1	DS1. 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.
digital signal level 3	DS3. 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. *See also* T3.
Digital Signature Algorithm	DSA. Cryptographic standard used for authenticating electronic documents, much as a written signature verifies the authenticity of a paper document.
digital subscriber line	DSL. Technology that increases the digital capacity of standard telephone lines into the home or office and provides always-on Internet operation. *See also* ADSL, SDSL.
digital subscriber line access multiplexer	DSLAM. Network device directly connected to subscriber premises that handles the copper termination and aggregates traffic into a higher-speed uplink. The output from a DSLAM is fed into the router through a DS3 or OC3 link.

Dijkstra algorithm   Search algorithm often used in routing that determines a shortest path tree. *See also* SPF.

DIMM   dual inline memory module. A 168-pin memory module that supports 64-bit data transfer.

DIOD   direct inward and outward dialing. Feature of a trunk line that allows both incoming and outgoing calls to be routed directly without help from an attendant. *See also* direct inward dialing, DID, direct outward dialing, DOD.

direct inward and outward dialing   DIOD. Feature of a trunk line that allows both incoming and outgoing calls to be routed directly without help from an attendant. *See also* direct inward dialing, DID, direct outward dialing, DOD.

direct inward dialing   DID. Feature of a trunk line that allows incoming calls to be routed directly to selected stations without help from an attendant.

direct outward dialing   DOD. Feature of a trunk line that allows outgoing calls to be routed directly to selected stations without help from an attendant.

direct routes   Routes that are in the routing table because an interface has been configured with an IP address. *Also called* interface routes.

direct server access   First authentication or accounting server that you configure in RADIUS. This server is treated as the primary authentication or accounting server, the next server configured is the secondary, and so on. *See also* round-robin server access.

direct server return   DSR. In Juniper Networks Media Flow Controller, a method of handling TCP traffic using a proxy.

directive   In NSM, a command sent to managed devices. Directives include importing, updating, rebooting, and so on. When a command is sent to a device or group of devices, NSM creates a job for that command and displays information about that job in the NSM Job Manager.

DIS   designated intermediate system. An IS-IS router that is elected by priority on an interface basis. In the case of a tie, the router with the highest MAC address becomes the DIS. DIS is analogous to the designated router in OSPF, although the election process and adjacencies within multiaccess media differ significantly. DIS assists broadcast routers to synchronize their IS-IS databases.

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 OS 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	DE. In a Frame Relay network, a header bit that notifies devices on the network that traffic can be dropped during congestion to ensure the delivery of higher priority traffic (those without the DE bit set).*See also* DE.
discrete multitone	DMT. Modulation method used by VDSL2 for separating a digital subscriber line signal so that the usable frequency range is divided into 256 frequency bands (or channels) of 4.3125 KHz each.
disk-on-key	Memory device (stick) that plugs into a USB port to load a complete Junos OS configuration with VoIP onto a Services Router. You must first use an Electronic Preinstallation Worksheet (EPW) to download the configuration to the disk-on-key device. The EPW and disk-on-key device provide an alternative method to configure the router for VoIP.
Distance Vector Multicast Routing Protocol	DVMRP. Dynamically generates IP multicast delivery trees using a technique called reverse-path multicasting (RPM) to forward multicast traffic to downstream interfaces. An interior gateway protocol (IGP) that supports operations within an autonomous system (AS), but not between ASs. The multicast backbone of the Internet uses DVMRP to forward multicast datagrams. DVMRP is a dense-mode multicasting protocol and therefore uses a broadcast-and-prune mechanism. *See also* dense mode.
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.
distance-vector routing	One of two major dynamic routing classes, requires each router to inform its neighbors of its routing table. For each network path, the receiving router picks the neighbor advertising the lowest metric, then adds this entry into its routing table for readvertisement. This method has less computational complexity and less message overhead than the other major class (link-state routing).
distributed denial of service attack	DDoS. Attack, typically a flood, from multiple source points. A DDoS attack can be more effective in disrupting services than a DoS, because the flood of incoming attacks are coming from multiple sources.
distributed port scan	Denial of service attack that uses multiple source addresses to scan ports on a network.
distribution list	List that controls routing information that is accepted or transmitted to peer routers. Distribution lists always use access lists to identify routes for distribution. For example, distribution lists can use access lists to specify routes to advertise. *See also* access lists.
DLCI	data-link connection identifier. 10-bit channel number attached to data frames to inform a Frame Relay network how to route the data in a Frame Relay virtual connection (a logical interface).
DLSw	data link switching. Method of tunneling IBM System Network Architecture (SNA) and NetBIOS traffic over an IP network, used because the Junos OS does not support NetBIOS. *See also* 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 code (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.
DM	• Diagnostic Mode. Qualcomm protocol specification and mechanism used to collect debug logs from Sierra 3G wireless modem firmware.
	• data model. In NSM, an XML file that contains configuration data for an individual device and is stored in the NSM Device Server. When you create, update, or import a device, the GUI Server edits the Abstract Data Model (ADM) to reflect the changes, then translates that information to the DM.
DMI	Device Management Interface. In NSM, a common, secure management interface used by all device families. DMI is based on a common protocol and device-specific schemas for configuration, inventory management, logging, and status monitoring. DMI schemas can be updated without the need to upgrade NSM.
DMT	discrete multitone. Modulation method used by VDSL2 for separating a digital subscriber line signal so that the usable frequency range is divided into 256 frequency bands (or channels) of 4.3125 KHz each.
DMZ	demilitarized zone. Physical or logical subnet used as an additional layer of security between an organization's network and an untrusted network (often the Internet); a neutral zone used to secure a network from external access. An attacker only has access to equipment in the DMZ.
DNIS	dialed number identification service. If users have a called number associated with them, the router searches the domain map for the called number. If it finds a match, the router uses the matching domain map entry information to authenticate the user. If the router does not find a match, it searches the domain map using normal processing.
DNS	Domain Name System. A system that stores information about hostnames and domain names. It provides an IP address for each hostname and lists the e-mail exchange servers accepting e-mail addresses for each domain.
DNS-ALG	Domain Name System-Application Level Gateway. Facilitates name-to-address mapping over bidirectional NAT or twice NAT.
document type definition	DTD. Defines the elements and structure of an Extensible Markup Language (XML) document or data set.
DOD	direct outward dialing. Feature of a trunk line that allows outgoing calls to be routed directly to selected stations without help from an attendant.

domain	Logical grouping of devices, policies, and access privileges that can also contain templates, objects, VPNs, administrators, activities, authentication servers, and groups—a representation of all or a subset of the physical devices and functionality on a network. The domain at a level above a domain is the parent domain, and the domain at a level below a domain is the child domain. Domains at the same level are considered peer domains. Also refers to a collection of routers that use a common interior gateway protocol (IGP).
Domain Menu	In NMS, the pull-down menu above the navigation tree where domains and subdomains are selected.
Domain Name System	DNS. A system that stores information about hostnames and domain names. It provides an IP address for each hostname and lists the e-mail exchange servers accepting e-mail addresses for each domain.
domain-specific part	DSP. Section of the Network Service Access Point (NSAP) address that uniquely identifies a system on the network.
don't fragment (bit)	DF. One-bit flag in the IP datagram header that specifies if a datagram should be fragmented. A value of zero (0) indicates to fragment the datagram; a value of one (1) indicates not to fragment the datagram.
DoS	denial of service. System security breach in which network services become unavailable to users.
DoS attack	denial-of-service attack. Any attempt to deny valid users access to network or server resources by using up all the resources of the network element or server. Typically, an attacker sends a flood of information to overwhelm a service system's resources, causing the server to ignore valid service requests.
downstream-on-demand	Method of label distribution whereby MPLS devices do not signal a FEC-to-label binding until requested to do so by an upstream device. Downstream-on-demand conserves labels by not binding until needed, and the label-switching router (LSR) receives label bindings (*also known as* label mappings) from a neighbor that is the next hop to a destination. It is used when RSVP is the signaling protocol. *See also* downstream-unsolicited, independent control, ordered control.
downstream-unsolicited	Label distribution method whereby MPLS devices do not wait for a request from an upstream device before signaling FEC-to-label bindings. As soon as the LSR learns a route, it sends a binding for that route to all peer LSRs, both upstream and downstream. Downstream-unsolicited does not conserve labels, because an LSR receives label mappings from neighbors that might not be the next hop for the destination; it is used by BGP or LDP when adjacent peers are configured to use the platform label space. *See also* downstream-unsolicited, independent control, ordered control.
DPC	Dense Port Concentrator. Network interface–specific card that can be installed in the router.

DPD   dead peer detection. Method that recognizes the loss of the primary IPsec Internet Key Exchange (IKE) peer and establishes a secondary IPsec tunnel to a backup peer. It is a keepalive mechanism that enables the E Series router to detect when communication to a remote IPsec peer has been disconnected. DPD enables the router to reclaim resources and to optionally redirect traffic to an alternate failover destination. If DPD is not enabled, traffic continues to be sent to the unavailable destination. *Also known as* IKE keepalive.

DR   designated router.

- Router on a subnet that is selected to control multicast routes for the sources and receivers on the subnet. If several routers are present, the selected DR is the router with the highest priority. If the DR priorities match, the router with the highest IP address is selected as the DR. The source's DR sends PIM register messages from the source network to the rendezvous point (RP). The receiver's DR sends PIM join and PIM prune messages from the receiver network toward the RP.

- 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 topology databases maintained on the other routers.

drop probability   Percentage value that expresses the likelihood that an individual packet will be dropped from the network. *See also* drop profile.

drop profile   Template that defines parameters that allow packets to be dropped from the network, controlling the dropping behavior of a set of egress queues. The profile defines the range within the queue where random early detection (RED) operates, the maximum percentage of packets to drop, and the sensitivity to bursts of packets. Weighted random early detection (WRED) is an extension to RED that enables an administrator to assign different RED drop profiles to each color of traffic. When you configure drop profiles, there are two important values: the queue fullness and the drop probability. *See also* drop probability, queue fullness, RED.

DS
- digital signal. Discontinuous signal used in direct sequence spread spectrum modulation, *also known as* direct sequence code division multiple access (DS-CDMA). DS-CDMA is one of two approaches to spread spectrum modulation for digital signal transmission over the airwaves. In direct sequence spread spectrum, the stream of information to be transmitted is divided into small pieces, each of which is allocated across to a frequency channel across the spectrum.

- Differentiated Services (field). The IPv4 header ToS octet or the IPv6 Traffic Class octet used to mark packets to enable differentiated services. *See also* DiffServ.

DS-BGP   dual-stack Border Gateway Protocol router. Router that runs both the IPv4 and the IPv6 protocol stack. DS-BGP routers are typically used to connect IPv6 islands across IPv4 clouds.

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.

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.

DSA   Digital Signature Algorithm. Cryptographic standard used for authenticating electronic documents, much as a written signature verifies the authenticity of a paper document.

DSAP   destination service access point. Identifies the destination for which a logical link control protocol data unit (LPDU) is intended.

DSCP   Differentiated Services code point, 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.

DSI   dynamic subscriber interface. Associated with a primary IP interface and dynamically created in response to an external event, such as packet detection or a DHCP event.

DSL   digital subscriber line. Technology that increases the digital capacity of standard telephone lines into the home or office and provides always-on Internet operation. *See also* ADSL, SDSL.

DSLAM   digital subscriber line access multiplexer. Network device directly connected to subscriber premises that handles the copper termination and aggregates traffic into a higher-speed uplink. The output from DSLAMs is fed into the router through a DS3 or OC3 link.

DSP   domain-specific part. Section of the Network Service Access Point (NSAP) address that uniquely identifies a system on the network.

DSR

- data set ready. One of the control signals on a standard RS-232C connector that indicates whether the DCE is connected and ready to start.

- direct server return. In Juniper Networks Media Flow Controller, a method of handling TCP traffic using a proxy.

DSU   data service unit. 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. *See also* CSU/DSU.

DTCP   Dynamic Tasking Control Protocol. 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, *DTCP: Dynamic Tasking Control Protocol*.

DTD   document type definition. Defines the elements and structure of an Extensible Markup Language (XML) document or data set.

DTE   data terminal equipment. RS-232-C interface that a computer uses to exchange information with a serial device, such as a computer, host, or terminal, that communicates with DCE. At the terminal end of a data transmission, DTE comprises the transmit and receive equipment. *See also* DCE.

DTR signal	data terminal ready signal. Sent over a dedicated wire (RS-232 connection) from a computer (or terminal) to a transmission device to indicate that the computer is ready to receive data.
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.
dual-stack Border Gateway Protocol	DS-BGP. Router that runs both the IPv4 and the IPv6 protocol stack. DS-BGP routers are typically used to connect IPv6 islands across IPv4 clouds.
duplex mode	Transmission and reception of signals in both directions. *See also* full-duplex mode, half-duplex mode.
duplicate accounting server	In RADIUS, a server that sends the accounting information to a particular router. You might use duplicate accounting to send the accounting information to a customer's accounting server. *See also* broadcast accounting server.
DVMRP	Distance Vector Multicast Routing Protocol. Dynamically generates IP multicast delivery trees using a technique called reverse-path multicasting (RPM) to forward multicast traffic to downstream interfaces. An interior gateway protocol (IGP) that supports operations within an autonomous system (AS), but not between ASs. The multicast backbone of the Internet uses DVMRP to forward multicast datagrams. DVMRP is a dense-mode multicasting protocol and therefore uses a broadcast-and-prune mechanism. *See also* dense mode.
DVMRP tunnels	Allow the exchange of IP multicast traffic between routers separated by networks that do not support multicast routing.
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.
DXI	data exchange interface. Specification developed by the switched megabit data services (SMDS) interest group to define the interaction between internetworking devices and CSUs/DSUs that are transmitting over an SMDS access line.
dynamic CAC	Dynamic call admission control application that blocks calls on a WAN interface when the bandwidth is exhausted. *See also* call admission control, CAC.
dynamic encapsulation lockout	Mechanism that temporarily prevents an ATM 1483 subinterface from autodetecting, accepting, and creating dynamic interface columns for a configurable time period.
dynamic flow capture	DFC. 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.
Dynamic Host Configuration Protocol	DHCP. Mechanism through which hosts using TCP/IP can obtain protocol configuration parameters automatically from a DHCP server on the network; allocates IP addresses dynamically so that they can be reused when no longer needed.

dynamic interface	Type of interface created through an external event, typically through the receipt of data over a lower-layer link, such as an ATM virtual circuit. The layers of a dynamic interface are created based on the packets received on the link and can be configured through RADIUS authentication, profiles, or a combination of RADIUS authentication and profiles. *See also* static interface.
dynamic label-switched path (LSP)	MPLS network path established by signaling protocols such as RSVP and LDP.
dynamic oversubscription	Mechanism that enables the router to vary queue thresholds based on the amount of egress buffer memory in use. *See also* bandwidth oversubscription, static oversubscription.
dynamic routing	Method that adjusts to changing network circumstances by analyzing incoming routing update messages. If a message indicates that a network change has occurred, the routing software recalculates routes and sends out new routing update messages, using different routes, based on current conditions of communications circuits. There are two common forms of dynamic routing: distance vector routing and link state routing.
dynamic subscriber interface	DSI. Associated with a primary IP interface and dynamically created in response to an external event, such as packet detection or a DHCP event.
Dynamic Tasking Control Protocol	DTCP. 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, *DTCP: Dynamic Tasking Control Protocol*.
dynamic translation	One of two NAT methods used to assign a translated IP address. This method uses access list rules and NAT address pools. Use it when you want the NAT router to initiate and manage address translation and session flows between address realms on demand.
dynamic tunnel-server ports	Module that supports dynamic tunnel-server ports. It provides both tunnel services and regular access services. *Also known as* shared tunnel-server module.

E

E-carrier	European carrier. 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.
E-LSP	EXP-inferred PSC-LSP. One of two types of LSPs used by MPLS to support differentiated services. The EXP field of the MPLS shim header is used to determine the per-hop behavior applied to the packet. *See also* L-LSP, shim header.
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. Compliance requirement defined by Common Criteria. Higher levels have more stringent requirements. *See also* Common Criteria.

EAP Extensible Authentication Protocol. Industry standard for network access that acts as a transport for multiple authentication methods or types. Defined by RFC 2284, PPP Extensible Authentication Protocol (EAP).

early packet discard EPD. For ATM2 interfaces only, a limit on the number of transmit packets that can be queued. Packets that exceed the limit are dropped. *See also* queue length.

EBGP External Border Gateway Protocol. Configuration in which sessions are established between routers in different autonomous systems (ASs).

EBGP session External Border Gateway Protocol session. Session between two BGP speakers that are in different autonomous systems. EBGP sessions typically exist between peers that are physically connected. *See also* IBGP session.

ECC error checking and correction; error-checking code. 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.

ECMP equal-cost multipath. Traffic load-balancing feature that enables traffic to the same destination to be distributed over multiple paths that have the same cost.

ECP Encryption Control Protocol. Responsible for configuring and enabling data encryption algorithms on both ends of a PPP link.

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

edge cache Appliance between the Internet and the end user, nearer to the end user, that caches and delivers content such as Java scripts, common channel signaling (CSS), images, and so on. This frees up Web servers for other processes. When Media Flow Controller is used as an edge cache, it is effectively a "reverse proxy," that provides these benefits: reduces the network and CPU load on an origin server by servicing previously retrieved content, and enhances the user experience due to a decrease in latency.

edge router In MPLS, the router located at the beginning or end of a label-switching tunnel. When at the beginning of a tunnel, it applies labels to new packets entering the tunnel. When at the end of a tunnel, it 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.

EEPROM electrically erasable programmable read-only memory. Chip used to store small amounts of configuration data.

effective weight	Result of a weight or an assured rate. Users configure the scheduler node by specifying either an assured rate or a weight within a scheduler profile. An assured rate, in bits per second, is translated into a weight, referred to as an effective weight.
EGP	exterior gateway protocol. Distributes routing information to routers that connect separate autonomous systems. *See also* IGP, BGP.
egress	Outbound, referring to packets exiting a device. *See also* ingress.
egress router	In MPLS, the last router in a label-switched path (LSP). *See also* ingress router.
EIA	Electronic Industries Association. 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. Mobile network database that contains information about devices using the network.
electrically erasable programmable read-only memory	EEPROM. Chip used to store small amounts of configuration data.
electromagnetic interference	EMI. Any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the effective performance of electronics or electrical equipment.
Electronic Industries Association	EIA. United States trade group that represents manufacturers of electronic devices and sets standards and specifications.
Electronic Preinstallation Worksheet	EPW. Customized Microsoft Excel spreadsheet used with a disk-on-key USB memory stick to configure VoIP on a Services Router. You download the EPW from an Avaya website.
Electronic Serial Number	ESN. Standardized code that uniquely identifies a mobile device. It can be printed on the device and is also digitally assigned to the device's firmware, and can be displayed by using a command such as **show modem wireless interface firmware**.
electrostatic discharge	ESD. Stored static electricity that can damage electronic equipment and impair electrical circuitry when released.
electrostatic discharge wrist strap	ESD wrist strap. Strap with a metal contact that is tied to the user's wrist in order to channel static electricity to a proper ground when the user handles sensitive computer equipment.
embedded OS software	Software used by a router to operate the physical router components.
embedded system	Special-purpose computer system designed to perform one or a few dedicated functions, usually embedded as part of a complete device that includes hardware and mechanical parts.

emergency transfer relay	ETR. Feature that provides an emergency link between the telephone connected to the first line port on the TGM550 and the trunk connected to the trunk port on the TGM550 if power is disconnected from the Services Router or if the TGM550 becomes unregistered from its Media Gateway Controller (MGC).
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	ESP. 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. *See also* AH.
encryption	Process of changing data into a form that can be read only by the intended receiver. A software mechanism that makes data confidential by making it unreadable to everyone except the sender and the intended recipient. The receiver of the encrypted message must have the correct decryption key to decipher the message.
Encryption Control Protocol	ECP. Responsible for configuring and enabling data encryption algorithms on both ends of a PPP link.
end system	ES. Any nonrouting network node or host in OSI internetworking. *See also* intermediate system.
End System-to-Intermediate System	ES-IS. 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.
endpoint discriminator	LCP negotiation option that identifies the system or device transmitting the packet.
enterprise MIB	SNMP term for a MIB defined by a single vendor. In addition to providing consistency of management data representation across that vendor's product line, the enterprise MIB also accounts for proprietary functions and value-added features not addressed by standard MIBs.
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. *See also* queue length.
EPW	Electronic Preinstallation Worksheet. Customized Microsoft Excel spreadsheet used with a disk-on-key USB memory stick to configure VoIP on a Services Router. You download the EPW from an Avaya website.
equal access mode	Mode in which a DHCP local server works with the Juniper Networks Service Deployment System (SDX) software to provide an advanced subscriber configuration and management service. In equal access mode, the router enables access to non-PPP users. Non-PPP equal access requires the use of the E Series router DHCP local server and SDX software, which communicates with a RADIUS server. *Also known as* DHCP equal access mode.
equal-cost multipath	ECMP. Traffic load-balancing feature that enables traffic to the same destination to be distributed over multiple paths that have the same cost.

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	ECC, error checking code. 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.
error checking code	ECC, error checking and correction. 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.
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	end system. Any nonrouting network node or host in OSI internetworking. *See also* intermediate system.
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.
ESD wrist strap	electrostatic discharge wrist strap. Strap with a metal contact that is tied to the user's wrist in order to channel static electricity to a proper ground when the user handles sensitive computer equipment.
ESN	Electronic Serial Number. Standardized code that uniquely identifies a mobile device. It can be printed on the device and is also digitally assigned to the device's firmware, and can be displayed by using a command such as **show modem wireless interface firmware**.
ESP	Encapsulating Security Payload. 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. *See also* 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 (10BaseT), to Fast Ethernet at 100 Mbps, to Gigabit Ethernet at 1000 Mbps.

Ethernet link aggregation	. Process that enables grouping of Ethernet interfaces at the physical layer to form a single link layer interface. *Also known as* 802.3ad link aggregation, a link aggregation group (LAG), or LAG bundle.
ETR	emergency transfer relay. Feature that provides an emergency link between the telephone connected to the first line port on the TGM550 and the trunk connected to the trunk port on the TGM550 if power is disconnected from the Services Router or if the TGM550 becomes unregistered from its Media Gateway Controller (MGC).
ETSI	European Telecommunications Standardization Institute. Nonprofit organization that produces voluntary telecommunications standards used throughout Europe.
European carrier	E-carrier. 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.
European Telecommunications Standardization Institute	ETSI. Nonprofit organization that produces voluntary telecommunications standards used throughout Europe.
EV-DO	Evolution-Data Optimized. Telecommunications standard for transmitting data through radio signals.
event categories	Classification groups and severity levels for system events that can be used to track system changes. Severity levels (categories) include: Emergency, Alert, Critical, Error, Warning, Notice, Info, and Debug.
event ID	event identifier. System log message code that uniquely identifies a system log message. The code begins with a prefix indicating the software process or library that generated the event.
event MIB	Enables you to create trigger conditions, test those conditions, and determine which action to take when a trigger meets those conditions, for object integers accessible in the SNMP agent, making it possible to monitor any aspect of a device without defining specific notifications. *See also* event table (mteEventTable), objects table (mteObjectsTable), SNMP Server Event Manager, trigger table (mteTriggerTable).
event policy process	eventd. Process that performs configured actions in response to events on a routing platform that trigger system log messages.
event table (mteEventTable)	SNMP term for a table that defines which action you want a device to take when a trigger occurs. This action can be in the form of a notification, setting a specified MIB object, or both. The results of these actions are controlled within two subordinate MIB tables—notification and set. One of the three parts of the Event MIB. *See also* objects table (**mteObjectsTable**), trigger table (**mteTriggerTable**).
eventd	Event policy process that performs configured actions in response to events on a routing platform that trigger system log messages.

events	system events. System changes that can be classified into log event categories and that can be used for tracking purposes.
Evolution-Data Optimized	EV-DO. Telecommunications standard for transmitting data through radio signals.
exact	Junos OS routing policy match type that represents only the route specified in a route filter.
exceeded action	In a rate-limit profile, an action that drops, transmits, marks (IP and IPv6), or marks-exp (MPLS) when traffic flow exceeds the rate. The mark value is not supported for hierarchical rate limits, and the transmit values conditional, unconditional, and final are supported only on hierarchical rate limits.
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.
Exchange Carriers Standards Association	ECSA. Organization created after the divestiture of the Bell System to represent the interests of interexchange carriers.
exclusive or	XOR. Logical operator (exclusive disjunction) in which the operation yields the result of true when one, and only one, of its operands is true.
Exec mode	CLI mode assigned to a user that determines which functions that user can perform when logged in to the system. *See also* Global Configuration mode, Privileged Exec mode, privileged level, User Exec mode
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.
EXP-inferredPSC-LSP	E-LSP. One of two types of LSPs used by MPLS to support differentiated services. The EXP field of the MPLS shim header is used to determine the per-hop behavior applied to the packet. *See also* L-LSP, shim header.
explicit path	*Also known as* signaled path. In traffic engineering, a specific, defined path determined using RSVP signaling. The Explicit Route Object carried in the packets contains the explicit path information.
Explicit Route Object	ERO. 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.
explicit routing	Subset of constraint-based routing where the constraint is an explicit route: the route the LSP takes is defined by the ingress node.

explicit shared shaper	Type of shared shaper in which you select the active constituents in a scheduler profile. A subset of the interface traffic is shaped to the shared rate. *See also* implicit shared shaper, shared shaping.
export	Placing of routes from the routing table into a routing protocol.
export map	Route map applied to a VRF to modify or filter routes exported from the VRF to the global BGP VPN routing information base (RIB) in the parent virtual router (VR). *See also* import map.
export rules	When you have two or more virtual routers on a security device, you can configure export rules that define which routes on one virtual router are allowed to learned by another virtual router. *See also* import rules.
ExStart	OSPF adjacency state in which the neighboring routers negotiate to determine which router is in charge of the synchronization process.
Extensible Authentication Protocol	EAP. Industry standard for network access that acts as a transport for multiple authentication methods or types. Defined by RFC 2284, PPP Extensible Authentication Protocol (EAP).
Extensible Markup Language	XML. 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.
Extensible Stylesheet Language for Transformations	XSLT. 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**.
exterior gateway protocol	EGP. Distributes routing information to routers that connect separate autonomous systems. *See also* IGP, BGP.
External Border Gateway Protocol, external BGP	EBGP. Configuration in which sessions are established between routers in different autonomous systems (ASs).
External Data Representation Standard	XDR. Standard for the description and encoding of data. XDR can be used to transfer data between computers.
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.
external neighbors	Two BGP routers that are peers, and reside in two different autonomous systems.
extranet	Private network that connects two or more intranets, allowing secure sharing of a part of a business's information with users outside the company, for example, allowing two or more companies or users to share resources and communicate over the Internet in their own virtual space. This technology greatly enhances business-to-business communications.

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.
facilities data link	FDL. Type of message that can be used to determine the status of a line and to display statistics for the remote end of a connection.
facility	Group of system log messages that either are generated by the same software process (such as accounting statistics) or that concern a similar condition or activity (such as authentication attempts.)
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. *See also* GRES, switchover.
false positive	Any situation in which benign traffic causes an IDS (intrusion detection system) to generate an alert. *Also known as* false alert.
far-end alarm and control	FEAC. 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.
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. *See also* 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. Filter that classifies packets to determine their forwarding path within a router. FBF is used to redirect traffic for analysis.
FCS	frame check sequence. Calculation 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. 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.

FDL facilities data link. Type of message that can be used to determine the status of a line and to display statistics for the remote end of a connection.

FEAC far-end alarm and control. 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. Set of packets with similar or identical characteristics that are forwarded in the same manner, on the same path, with the same forwarding treatment, and using the same MPLS label. FECs 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. *See also* BECN.

Federal Information Processing Standards FIPS. Defines, among other things, security levels for computer and networking equipment. FIPS is usually applied to military environments.

FIB forwarding information base. In the JunosE Software, the IP routing table. Referred to in the context of BGP.

Fiber Distributed Data Interface FDDI. 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.

field-programmable gate array FPGA. Semiconductor device that contains programmable logic components and interconnects. Also a category of hardware classifier.

field-replaceable unit FRU. Router component that customers can replace onsite.

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 OS interface queues operate in this mode by default.

file system synchronization mode	Default behavior mode for E Series routers that contain redundant SRP modules, and available only to SRP modules. Characteristics of this mode include:

- Files and data in nonvolatile storage (NVS) remain synchronized between the primary (active) SRP module and standby SRP module.

- SRP modules reload all line modules and restart from saved configuration files.

- If the active SRP module switches over to the standby SRP, the router cold-restarts as follows: all line modules are reloaded; user connections are lost; forwarding through the chassis stops until the router SRP module recovers; the standby SRP module boots from the last known good configuration from NVS.

See also high availability mode, switchover.

File Transfer Protocol	FTP. Application protocol that is part of the TCP/IP protocol stack. Used for transferring files between network nodes. FTP is defined in RFC 959, *File Transfer Protocol*.
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. *See also* packet.
filter-based forwarding	FBF. Filter that classifies packets to determine their forwarding path within a router. FBF is used to redirect traffic for analysis.
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 means of controlling access to a network to protect it from misuse and malicious intent from other users (for example, denial-of-service attacks). 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 action	Action performed by a security device when the device receives traffic that matches the direction, source, destination, and service. Firewall actions include permit, deny, reject.
firewall filter	At the firewall, a policy that evaluates the context of connections and permits or denies traffic based on the context, updating 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. *See also* 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	FIFO. Scheduling method in which the first data packet stored in the queue is the first data packet removed from the queue. All Junos OS interface queues operate in this mode by default.
flap damping	Method of reducing the number of update messages sent between BGP peers, thereby reducing the load on those peers without adversely affecting the route convergence time for stable routes. *See also* damping.
flapping	route flapping. Condition of network instability where a route is announced and withdrawn repeatedly, often as the result of an intermittently failing link.
flexible bandwidth allocation	Technique to temporarily provide additional capacity on a link to handle bursts in data, videoconferencing, or other variable bit rate applications. *Also known as* bandwidth on demand.
Flexible PIC Concentrator	FPC. An interface concentrator on which physical interface cards (PICs) are mounted. An FPC is inserted into a slot in a Juniper Networks router. *See also* PIC.
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.
flooding	Distribution and synchronization of the link-state database between OSPF routers.
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 OS 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 tracking	Method of reducing false positives, it correlates multiple TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) connections into a single flow to determine the validity of the traffic.

flow-tap application | 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 for lawfully intercepting data.

flowd | Flow-based packet forwarding process that applies ingress interface filters and policers to packets entering the device. The **flowd** establishes the state of the packet's session and manages the packet as it transits the security flow and associated features, applying output filtering and traffic shaping before transmitting the packet out the egress interface.

forward explicit congestion notification | FECN. 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. *See also* BECN.

forwarding adjacency | FA. RSVP LSP tunnel through which one or more other RSVP LSPs can be tunneled.

forwarding classes | Defined set 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* ordered aggregates in the IETF Differentiated Services architecture.

Forwarding Engine Board | FEB. In M5 and M10 routers, provides route lookup, filtering, and switching to the destination port.

forwarding equivalence class | FEC. Set of packets with similar or identical characteristics that are forwarded in the same manner, on the same path, with the same forwarding treatment, and using the same MPLS label. FECs 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.

forwarding information base | FIB, forwarding table. In the JunosE Software, the IP routing table. Referred to in the context of BGP.

forwarding table | Table of best routes to all destinations reachable by the router. For each destination, the table has only the single best route to the destination selected from the IP routing table. The Junos OS 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.

forwarding table entry | FTE. Of all destinations reachable by the router, the single best route to a given destination selected from the IP routing table.

FPC | Flexible PIC Concentrator. An interface concentrator on which physical interface cards (PICs) are mounted. An FPC is inserted into a slot in a Juniper Networks router. *See also* PIC.

FPGA | field-programmable gate array. Semiconductor device that contains programmable logic components and interconnects. Also a category of hardware classifier.

FQDN | fully qualified domain name. The hostname and domain name for a specific system.

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, allowing service providers to provision part of the 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, fractional T1 channel	Interface that contains one or more of the 24 DS0 time slots that can be reserved from a T1 interface. A DS0 portion of a 24-DS0 T1 line. Fractional T1s enable you to separate out one DS0 line or combine several lines into bundles (usually in multilink PPP).
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. Required when IP must transmit a large packet through a network that transmits smaller packets, or when the MTU size of the other network is smaller. In the Open Systems Interconnection (OSI) reference model, this process is known as segmentation. For Junos OS applications, split Layer 3 packets can then be encapsulated in MLFR or MLPPP for transport.
fragmentation and assembly	• In Frame Relay, a feature that reduces excessive delays of Frame Relay packets by breaking them into smaller fragments that are then interleaved with real-time frames.
	• In the Multilink Point-to-Point Protocol (MLPPP), fragmentation is the process by which a large packet is broken up into multiple smaller fragments for simultaneous transmission across multiple links of an MLPPP bundle. Reassembly is the process by which the destination router reassembles the fragments into the original packets.
frame check sequence	FCS. Calculation added to a frame for error control. FCS is used in HDLC, Frame Relay, and other data-link layer protocols.
Frame Relay	Public, connection-oriented packet service based on the core aspects of the Integrated Services Digital Network. It eliminates all processing at the network layer and greatly restricts data-link layer processing. Frame Relay is an efficient replacement for the older X.25 protocol that does not require explicit acknowledgment of each frame of data. It 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.
Frame Relay Forum	FRF. Technical committee that promotes Frame Relay by negotiating agreements and developing standards.
Frame Relay LMI	Frame Relay local management interface. Provides the operator with configuration and status information relating to the Frame Relay VCs in operation. LMI specifies a polling mechanism to receive incremental and full-status updates from the network. The router can represent either side of the User-to-Network Interface (UNI) and supports unidirectional LMI. Bidirectional support for the Network-to-Network Interface (NNI) is also supported.

frequency-division multiplexed channel	Signals that are carried at different frequencies and transmitted over a single wire or wireless medium.
FRF	Frame Relay Forum. Technical committee that promotes Frame Relay by negotiating agreements and developing standards.
FRF.15	Implementation of MLFR using multiple virtual connections to aggregate logical bandwidth for end-to-end Frame Relay, defined by the Frame Relay Forum in *End-to-End Multilink Frame Relay Implementation Agreement FRF.15*.
FRF.16	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. Defined by the Frame Relay Forum in *Multilink Frame Relay UNI/NNI Implementation Agreement FRF.16.1*.
FRU	field-replaceable unit. Router component that customers can replace onsite.
FTE	forwarding table entry. Of all destinations reachable by the router, the single best route to a given destination selected from the IP routing table.
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, *File Transfer Protocol*.
Full	OSPF adjacency state that represents a fully functional neighbor relationship.
full download	In virtual player functions, an HTTP media delivery method in which the entire media file is downloaded before playback, in contrast with other methods such as progressive download, which partially downloads before initiating playback, or streaming modes that simultaneously download and play back in real time. *See also* progressive download.
full-duplex mode	Transmission mode that supports transmission and reception of signals in both directions simultaneously. *See also* duplex mode, half-duplex mode.
full-mesh VPN	VPN in which each site in the VPN can communicate with every other site in that same VPN. *See also* hub-and-spoke VPN, overlapping VPN.
fully-qualified domain name	FQDN. The hostname and domain name for a specific system.
fwauthd	Firewall authentication process that implements and manages user authentication configuration, and authenticates users who access the firewall.
fxp0	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. *See also* permanent interface.
fxp1	Junos OS permanent interface used for communications between the Routing Engine and the Packet Forwarding Engine. This interface is not present in all routers.

fxp2	Junos OS 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-PDU	User data message sent in a path. It consists of a T-PDU plus a GTP header.
G.992.1	ITU-T Rec. G.992.1. International ITU-T 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. .
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 incorporates features of other DSL technologies such as asymmetrical DSL (ADSL). *See also* 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.
gateway	Program or device that converts one protocol or format to another, or acts as a go-between two or more networks that use the same protocols. In this case, the gateway functions as an entry/exit point to the network. Also, an older term for a router.
gateway GPRS support node	GGSN. Router that serves as a gateway between mobile networks and packet data networks.
gateway router	Device that passes DHCP messages between DHCP clients and DHCP servers. *Also known as* a relay agent.
GBIC	Gigabit Interface Connector. Interface module card used on some security devices for connecting to a fiber optic network.
general community	Convenient way to categorize groups of routes to facilitate the use of routing policies. *Also called* private community or local-use community.
General Packet Radio Service	GPRS. Packet-switched service that enables high-speed wireless Internet and other data communications, allowing full mobility and wide-area coverage as information is sent and received across a mobile network. Using a packet data service, subscribers are always connected and always online so services are easy and quick to access.
Generalized Multiprotocol Label Switching	GMPLS. 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.
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	GRE. 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. *See also* tunneling protocol.
generic token card	GTC. Carries user-specific token cards for authentication.
GGSN	gateway GPRS support node. Router that serves as a gateway between mobile networks and packet data networks.
GGSN call detail record	G-CDR. Collection of charges in ASN.1 format that is eventually billed to a mobile station user.
GI interface	Interface between a GSN and an external network or the Internet.
Gigabit Backplane Physical Interface Module	GPIM. SRX mid-range services gateway network interface card (NIC) that includes standard GPIMs installed in a single-high, single-wide GPIM slot and has gigabit connectivity to the system backplane.
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. *See also* Ethernet, Fast Ethernet.
global AS	Autonomous system (AS) consisting of multiple subautonomous systems (sub-ASs).
Global Configuration mode	Privileged Exec mode from which you can set parameters or enable features. Within Global Configuration mode, you can apply features globally to a router, enable a feature or function, disable a feature or function, and configure a feature or function. *See also* Privileged Exec mode, User Exec mode.
global domain	Top level, or root domain, that contains all subdomains (logical groupings of devices, policies, and access privileges). *See also* domain.
global export map	Route map applied to a VRF to modify and filter routes exported by the VRF to the global BGP non-VPN RIB in the parent VR. *See also* export map, global import map, import map.
global import map	Route map applied to a VRF to modify and filter routes imported to the the BGP RIB of the VRF from the global BGP non-VPN RIB in the parent VR. *See also* export map, global export map, import map.
global routing table	Database maintained by IP on E Series router SRP modules. Contains at most one route per protocol to each prefix in the table. *See also* local routing table, forwarding table, routing table.
Global System for Mobile Communications	GSM. A second-generation (2G) mobile wireless networking standard defined by ETSI that uses TDMA technology and operates in the 900-MHz radio band. *See also* TDMA.
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	Greenwich Mean Time, 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.
Gn interface	Interface between two GSNs within the same Public Land Mobile Network (PLMN).
Gp interface	Interface between two GSNs located in different Public Land Mobile Networks (PLMNs).
GPIM	Gigabit Backplane Physical Interface Module. SRX mid-range services gateway network interface card (NIC) that includes standard GPIMs installed in a single-high, single-wide GPIM slot and has gigabit connectivity to the system backplane.
GPRS	General Packet Radio Service. Packet-switched service that enables high-speed wireless Internet and other data communications, allowing full mobility and wide-area coverage as information is sent and received across a mobile network. Using a packet data service, subscribers are always connected and always online so services are easy and quick to access.
GPRS Roaming Exchange	GRX. Acts as a hub for GPRS connections from roaming users, removing the need for a dedicated link between each GPRS service provider.
GPRS tunneling protocol	GTP. Transports IP packets between an SGSN and a GGSN. *See also* tunneling protocol.
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. Implementation varies by protocol. *Also called* nonstop forwarding. *See also* cold restart, warm restart.
graceful Routing Engine switchover	GRES. 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.
graceful switchover	Junos OS 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. 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. *See also* tunneling protocol.
GRE tunnel	IP tunnel that uses GRE-encapsulated IP packets to enable data transmission. The resulting encapsulated packet contains a GRE header and a delivery header. Consequently, the packet requires more processing than an IP packet, and GRE can be slower than native routing protocols. GRE tunnels can be secured with IPsec.

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 that organizes previously created devices into user-defined groups, making it easier for you to configure and manage devices in your domain. Groups enable you to execute certain NSM operations on multiple security devices at the same time.
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.
group expression object	Represents a statement that sets conditions for authentication requirements that enable you to combine multiple external user objects. You can create group expressions using the operator OR, AND, or NOT to combine user objects, user group objects, or other group expressions.
group node	Scheduler node associated with a {port interface, traffic-class group} pair. Because the logical interface is the port, only one such scheduler node can exist for each traffic-class group above the port. This node aggregates all traffic for traffic classes in the group.
group preshared keys	Secure remote access method that uses L2TP/IPsec when connecting to networks that do not use a certificate authority (CA) to issue certificates. A group preshared key is associated with a local IP address in the E Series router and is used to authenticate L2TP/IPsec clients that target this IP address as their VPN server address. Group preshared keys are not fully secure; they open to man-in-the-middle attacks. Digital certificates are preferred instead.
GRX	GPRS Roaming Exchange. Acts as a hub for GPRS connections from roaming users, removing the need for a dedicated link between each GPRS service provider.
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. *See also* TDMA.
GTC	generic token card. Carries user-specific token cards for authentication.
GTP	GPRS tunneling protocol. Transports IP packets between an SGSN and a GGSN. *See also* tunneling protocol.
GTP tunnel	Tunnel in the GTP-U plane defined for each PDP context in the GSNs. A GTP tunnel in the GTP-C plane is defined for all PDP contexts with the same PDP address and APN (for Tunnel Management messages) or for each MS (for messages not related to Tunnel Management). A GTP tunnel is identified in each node with a TEID, an IP address, and a UDP port number. A GTP tunnel is necessary to forward packets between an external network and an MS user.
GTP-C	GGSN tunneling protocol, control. Allows an SGSN to establish packet data network access for a mobile station. *See also* tunneling protocol.

GTP-C message   Control messages exchanged between GSN pairs in a path to transfer GSN capability information between the pairs, to create, update and delete GTP tunnels, and for path management.

GTP-PDU   GTP Protocol Data Unit. Either a GTP-C message or a GTP-U message.

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

GTP-U message   GTP-User Data message. Messages exchanged between GSN pairs or GSN/RNC pairs in a path to carry user data packets, and used as signaling messages for path management and error indication.

GUI Server   Manages the system resources in NSM and data that drives NSM functionality. It contains the NSM databases and centralizes information for devices, their configurations, attack and server objects, and policies.

H

H.323   ITU–T recommendation that describes packet-based multimedia communications over networks that do not guarantee class of service, such as IP networks, providing a widely-used standard for VoIP and conferencing that is modeled on ISDN PRI. It is implemented as an Application Layer Gateway (ALG) that provides secure VoIP communication between terminal hosts, such as IP phones and multimedia devices, in which the gatekeeper devices manage call registration, admission, and call status for VoIP calls. The gatekeepers can reside in the two different zones, or in the same zone.

HA   high availability. Configuring pairs of security devices to ensure service continuity in the event of a network outage or device failure. Used to provide fault detection and correction procedures to maximize the availability of critical services and applications. When applied to the E Series router, high availability provides both hardware-specific and software-specific methods to ensure minimal downtime and ultimately improve the performance of your network. *See also* high availability mode.

half-duplex mode   Transmission mode that supports transmission and reception of signals in both directions, but not at the same time. *See also* duplex mode, full-duplex mode.

handshake   Process of exchanging signaling information between two communications devices to establish the method and transmission speed of a connection.

HAR   hierarchical assured rate. Calculation process that dynamically adjusts bandwidth for scheduler nodes—a more powerful and efficient method of configuring assured rates than static assured rates. *See also* SHA-1, MD5.

hard disk drives   HDD. Refers to system storage media used for caching functions and installation procedures.

hardened system   Secure server with all appropriate security patches and bug fixes. These systems are designed to resist penetration.

Hashed Message Authentication Code	HMAC. 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*.
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, it used to validate that the contents of a message have not been altered in transit. The Secure Hash Algorithm (especially SHA-1) and Message Digest 5 (MD5) are commonly used hashes. *See also* SHA-1, MD5.
HDD	hard disk drives. Refers to system storage media used for caching functions and installation procedures.
HDLC	High-Level Data Link Control. 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 OS 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 OS 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.
hello messages	Messages used to detect adjacent peers and maintain adjacency.
hello packet	Message sent out to the current network to announce the presence of the current routing instance to the network. Hello packets aid in the discovery of neighbors and in a router being able to connect to other devices on the network. When an OSPF interface is created, the interface sends Hello packets to the network to announce itself.
hello protocol	Establishes and maintains neighbor relationships; communication between neighbors is bidirectional. The hello protocol also dynamically discovers neighboring routers on broadcast or point-to-point networks.
hierarchical assured rate	HAR. Calculation process that dynamically adjusts bandwidth for scheduler nodes—a more powerful and efficient method of configuring assured rates than static assured rates. *See also* SHA-1, MD5.
hierarchical round-robin	HRR. Scheme for allocating bandwidth to queues in proportion to their weights.

high availability	HA. Configuring pairs of security devices to ensure service continuity in the event of a network outage or device failure. Used to provide fault detection and correction procedures to maximize the availability of critical services and applications. When applied to the E Series router, high availability provides both hardware-specific and software-specific methods to ensure minimal downtime and ultimately improve the performance of your network. *See also* high availability mode.
high availability mode	Ensures rapid SRP module recovery following a switchover. High availability mode uses an initial bulk file transfer and subsequent, transaction-based mirroring. *Also known as* stateful SRP switchover. In addition to keeping the contents of NVS, high availability mode keeps state and dynamic configuration data from the SRP memory synchronized between the primary and standby SRP modules.
High Speed Downlink Packet Access	HSDA. Enhanced 3G mobile communications protocol.
high-density Ethernet	Process by which a module allows oversubscription of Ethernet packets. The module manages oversubscription by prioritizing and dropping certain packets.
high-density keepalive mode	Mode whereby, when the keepalive timer expires, the interface first verifies whether any frames were received from the peer in the prior keepalive timeout interval. If so, the interface does not send an LCP echo request (keepalive). Keepalive packets are sent only if the peer is silent (if no traffic was received from the peer during the previous keepalive timeout interval). *Also known as* smart keepalive. *See also* low-density keepalive mode.
High-Level Data Link Control	HDLC. International Telecommunication Union (ITU) standard for a bit-oriented data-link layer protocol on which most other bit-oriented protocols are based.
High-Speed Circuit Switched Data	HSCSD. Circuit-switched wireless data transmission for mobile users, at data rates up to 38.4 Kbps.
high-speed serial interface	HSSI. Interface that supports high-speed WAN switching services such as Frame Relay and Switched Multimegabit Data Service (SMDS) trunk encapsulation. You can configure an interface to act as data communications equipment (DCE) or data terminal equipment (DTE).
histogram	Vertical graph that represents different amounts by thin, color-coded bands or bars. These bars represent a frequency distribution; heights of the bars represent observed frequencies.
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. 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*.

HMAC MD5 authentication	Method for IS-IS that prevents unauthorized routers from injecting false routing information into your network or forming adjacencies with your router. The router creates secure digests of the packets, encrypted according to the HMAC MD5 message-digest algorithms. The digests are inserted into the packets from which they are created. Depending on the commands you issue, the digests can be inserted into hello packets, link-state PDUs, complete sequence number PDUs, and partial sequence number PDUs. *Also called* MD5 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. In OSPF, the maximum amount of time between instances of initiating Shortest Path First (SPF) computations.
Home Location Register	HLR. Database containing information about a subscriber and the current location of a subscriber's mobile station.
hop count	Number of routers that data packets must traverse between RIP networks. *See also* RIP metric.
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	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).
host-specific configuration	Configuration that takes place on a device for which you have created a host-specific autoinstallation configuration file (**hostname.conf**). The **hostname.conf** file contains all the information necessary for configuring the named host device. *See also* **hostname.conf.**
hostname.conf	Host-specific configuration file for autoinstallation on a device that contains all the information necessary for configuring the device. In the filename, **hostname** is replaced with the **hostname** that you are assigning to the device.
hot content	Media content that is often requested. Media Flow Controller caches content hierarchically according to how "hot" it is: short tail video (a few videos requested often by many clients) can be cached closer to the subscriber, while long tail video (videos seldom requested) can be kept deeper in the network.

hot fix One or more files that update an operational E Series router. Hot fixes can do any of the following: address one or more specific, critical software issues by replacing or adding functionality to one or more software components; enable the delivery of software updates without having to load an entire software release; or deploy debugging code to collect data that facilitates troubleshooting of software issues.

hot standby In the Junos OS, method used with link services intelligent queuing interfaces (LSQ) to enable rapid switchover between primary and secondary (backup) PICs. *See also* warm standby.

HRR hierarchical round-robin. Scheme for allocating bandwidth to queues in proportion to their weights.

HRR scheduler One part of the integrated scheduler used to extend ATM QoS functionality on all E Series router ASIC-enabled line modules. *See also* SAR scheduler.

HSCSD High-Speed Circuit Switched Data. Circuit-switched wireless data transmission for mobile users, at data rates up to 38.4 Kbps.

HSDA High Speed Downlink Packet AccessEnhanced 3G mobile communications protocol.

HSSI high-speed serial interface. Interface that supports high-speed WAN switching services such as Frame Relay and Switched Multimegabit Data Service (SMDS) trunk encapsulation. You can configure an interface to act as data communications equipment (DCE) or data terminal equipment (DTE).

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.

hub-and-spoke VPN Type of VPN in which spoke sites in the VPN can communicate only with the hub sites; they cannot communicate with other spoke sites. *See also* full-mesh VPN, overlapping VPN.

Hypertext Transfer Protocol HTTP. Method used to publish and receive information on the Web, such as text and graphic files.

Hypertext Transfer Protocol over Secure Sockets Layer HTTPS. 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.

I

I-DAS integrated DHCP access server. Feature that enables you to use RADIUS start and stop attributes to track user events such as the lifetime of an IP address.

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	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 adapter	IOA, Input/output adapter. Physical interface that pairs with line modules to provide connectivity to E120 and E320 routers. *See also* I/O module.
I/O Manager ASIC	Juniper Networks ASIC responsible for segmenting data packets into 64-byte J-cells and for queuing result cells before transmission.
I/O module	• Physical interface that pairs with line modules to provide connectivity to an ERX router. *See also* IOA. • In Juniper IDP series, it contains the traffic interfaces that receive and send network traffic and is a field-replaceable unit (FRU).
IANA	Internet Assigned Numbers Authority. Regulatory group that maintains all assigned and registered Internet numbers, such as IP and multicast addresses. *See also* NIC.
IAPP	Inter Access Point Protocol. IEEE 802.11F recommendation that describes optional extensions to IEEE 802.11, which defines wireless access-point communications among multivendor systems.
IBGP	Internal Border Gateway Protocol. BGP configuration in which sessions are established between routers in the same autonomous system (AS). *See also* EBGP.
IBGP session	Session between two BGP speakers that are in the same autonomous system (AS). IBGP requires that BGP speakers within an autonomous system be fully meshed, meaning that there must be a BGP session between each pair of peers within the AS. IBGP does not require that all the peers be physically connected. *See also* EBGP session.
ICMP	Internet Control Message Protocol. Network layer protocol that provides a query and response system for a router or destination host to report an error in data traffic processing to the original source of the packet. Used in router discovery, ICMP allows router advertisements that enable a host to discover addresses of operating routers on the subnet. An ICMP echo request is *also known as* a ping.
ICMP flood	Type of Denial of Service attack that sends ICMP pings so large or so numerous that they overload a system with echo requests, causing the system to expend all its resources responding until it can no longer process valid network traffic. *Also known as* ping flood or smurf attack.
ICMP Router Discovery Protocol	IRDP. Used by DHCP clients that enables a host to determine the address of a router that it can use as a default gateway.
IDE	Integrated Drive Electronics. Type of hard disk on a Routing Engine.

IDEA International Data Encryption Algorithm. One of the methods at the heart of Pretty Good Privacy (PGP), it uses a 128-bit key. IDEA is patented by Ascom Tech AG and is popular in Europe.

IDI initial domain identifier. Part of an ATM address format that contains the address fields describing the address allocation and issuing authority.

Idle Initial BGP neighbor state in which the local router refuses all incoming session requests.

IDP
- initial domain part. Portion of a CLNS address that consists of the AFI and IDI. *See also* AFI, IDI.
- Intrusion Detection and Prevention. Name of a Juniper product line of security devices that run the IDP OS (operating system).

IDS intrusion detection service. Inspects all inbound and outbound network activity and identifies suspicious patterns that might indicate a network or system attack from someone attempting to break into or compromise a system.

IEC International Electrotechnical Commission. International standards organization that deals with electrical, electronic, and related technologies. *See* ISO.

IEEE Institute of Electrical and Electronics Engineers. International professional society for electrical engineers.

IEEE 802.1p IEEE standard for a Layer 2 frame structure that supports VLAN identification and CoS traffic classification.

IEEE 802.3af IEEE standard that defines a method for powering network devices through an Ethernet cable. *Also known as* Power over Ethernet (PoE), this standard enables remote devices (such as VoIP telephones) to operate without a separate, external power source.

IETF Internet Engineering Task Force. 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 physical interface. (A Juniper Networks internal use acronym.) Port on a Physical Interface Card (PIC) or Physical Interface Module (PIM).

IFF protocol families. (A Juniper Networks internal use acronym.) Grouping of logical properties within an interface configuration, for example, the inet, inet4, and mpls protocol families.

IFL logical interface. (A Juniper Networks internal use acronym.) 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.

IGMP	Internet Group Management Protocol. Host-to-router signaling protocol for IPv4 to report multicast group memberships to neighboring routers and determine whether group members are present during IP multicasting. Similarly, multicast routers, such as E Series routers, use IGMP to discover which of their hosts belong to multicast groups and to determine whether group members are present.
IGMP proxy	Method by which a router issues IGMP host messages on behalf of hosts that the router discovered through standard IGMP interfaces. The router acts as a proxy for its hosts.
IGP	interior gateway protocol. Distributes routing information to routers within an autonomous system, such as IS-IS, OSPF, or RIP. *See also* EGP.
IKE	Internet Key Exchange. Part of IPsec that provides ways to exchange keys for encryption and authentication securely over an unsecured medium such as the Internet. IKE enables a pair of security gateways to:

- Dynamically establish a secure tunnel over which security gateways can exchange tunnel and key information.
- Set up user-level tunnels or SAs, including tunnel attribute negotiations and key management. These tunnels can also be refreshed and terminated on top of the same secure channel.

IKE employs Diffie-Hellman methods and is optional in IPsec (the shared keys can be entered manually at the endpoints).

IKE endpoint	IP address of the entity that is one of two endpoints in an IKE/ISAKMP SA.
IKE policies	Policies that define a combination of security parameters to be used during the IKE SA negotiation. IKE policies are configured on both security gateway peers, and there must be at least one policy on the local peer that matches a policy on the remote peer. If that is not the case, the two peers are not able to successfully negotiate the IKE SA, and no data flow is possible.
IKE proposal object	In NSM, a representation of an IKE proposal, which is a set of encryption keys and authentication algorithms used to negotiate a VPN connection.
iked	IKE process that implements tunnel management for IPsec VPNs, provides authentication of endpoint entities, and generates keys for packet authentication and encryption.
ILEC	incumbent local exchange carrier. Any commercial telecom company that was in business after the breakup of AT&T in 1984 and before the Telecommunications Act of 1996.
ILMI	Integrated Local Management Interface. 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. Unique code used to identify an individual mobile station to a GSM network.

implicit shared shaper	Type of shared shaper in which the system automatically selects the active constituents. A shared-shaping rate is configured on the best-effort node or queue, and QoS locates the other constituents automatically. *See also* explicit shared shaper, shared shaping.
import	Installation of routes from the routing protocols into a routing table.
import map	Route map applied to a VRF to modify and filter routes imported to the BGP RIB of the VRF from the global BGP VPN RIB in the parent VR. *See also* export map, global import map.
import rules	When you have two or more virtual routers on a security device, you can configure import rules on one virtual router that define which routes are allowed to be learned from another virtual router. If you do not configure any import rules for a virtual router, all routes that are exported to that virtual router are accepted. *See also* export rules.
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.
in-device policy management	In NSM, mode of policy management performed on a single device, using the NSM Device Editor. If this method is selected to manage a J Series or SRX Series device, then the NSM Policy Manager, the Object Manager, and the VPN Manager are all disabled for that device.
inactive constituent	Constituent that is ignored by the shared shaper mechanism. *See also* active constituent, constituent.
InARP	Inverse Address Resolution Protocol. Way of determining the IP address of the device at the far end of a circuit.
inbound traffic (IPsec)	In the context of a secure interface, already secured traffic arriving on that interface (identified based on its SPI). This traffic is cleared and checked against the security parameters set for that interface.
incumbent local exchange carrier	ILEC. Any commercial telecom company that was in business after the breakup of AT&T in 1984 and before the Telecommunications Act of 1996.
independent control	MPLS label distribution method whereby the LSR sending the label acts independently of its downstream peer. It does not wait for a label from the downstream LSR before it sends a label to peers. *See also* ordered control.
inet.0	Default Junos OS routing table for IPv4 unicast routers.
inet.1	Default Junos OS routing table for storing the multicast cache for active data streams in the network.

inet.2	Default Junos OS routing table for storing unicast IPv4 routes specifically used to prevent forwarding loops in a multicast network.
inet.3	Default Junos OS routing table for storing the egress IP address of an MPLS label-switched path.
inet.4	Default Junos OS routing table for storing information generated by the Multicast Source Discovery Protocol (MSDP).
inet6.0	Default Junos OS 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.
Infranet Controller	Policy management component of a Juniper Networks UAC solution.
Infranet Enforcer	Policy enforcement point or firewall within a Juniper Networks UAC solution.
ingest	Data that has been placed on a Media Flow Controller and analyzed and queued for deployment.
ingress	Inbound, referring to packets entering a device. *See also* egress.
ingress router	In MPLS, the first router in a label-switched path (LSP). *See also* egress router.
Init	OSPF adjacency state in which the local router has received a hello packet but bidirectional communication is not yet established.
initial domain identifier	IDI. Part of an ATM address format that contains the address fields describing the address allocation and issuing authority.
initial domain port	IDP. Portion of a CLNS address that consists of the AFI and IDI. *See also* AFI, IDI.
input policy	Policy that evaluates a condition before the normal route lookup. *See also* output policy, policy, secondary input policy.
input/output adapter	IOA. Physical interface that pairs with line modules to provide connectivity to E120 and E320 routers. *See also* I/O module.
input/output module	IOA. Physical interface that pairs with line modules to provide connectivity to E120 and E320 routers. *See also* I/O adapter.
insert	Junos OS command that allows a user to reorder terms in a routing policy or a firewall filter, or to change the order of a policy chain.
inside global address	In a NAT context, IP translated address of an inside host as seen by an outside host and network.
inside local address	In a NAT context, configured IP address that is assigned to a host on the inside network.

inside network	In a NAT context, the local portion of a network that uses private, not publicly routable, IP addresses that you want to translate.
inside source translation	Commonly used NAT configuration, in which an inside host sends a packet to the outside network and the NAT router translates the source information. Then, in the inbound direction, the NAT router restores the original information. For outbound traffic, the NAT router translates the inside local address into the inside global address.
instance.inetflow.0	Routing table that shows route flows through BGP.
Institute of Electrical and Electronics Engineers	IEEE. International professional society for electrical engineers.
Integrated DHCP access server	I-DAS. Feature that enables you to use RADIUS start and stop attributes to track user events such as the lifetime of an IP address.
Integrated Drive Electronics	IDE. Type of hard disk on a Routing Engine.
Integrated IS-IS	Extended version of IS-IS that supports the routing of datagrams by means of IP or CLNS. Without the extensions, IS-IS routes datagrams only by means of CLNS.
Integrated Local Management Interface	ILMI. 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).
integrated routing and bridging	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.
integrated scheduler	QoS scheduler that provides extended ATM QoS functionality. The integrated scheduler consists of two schedulers in series—the hierarchical round robin (HRR) scheduler and the segmentation and reassembly (SAR) scheduler.
Integrated Services Digital Network	ISDN. 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.
intelligent queuing	IQ. 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.
Inter Access Point Protocol	IAPP. IEEE 802.11F recommendation that describes optional extensions to IEEE 802.11, which defines wireless access-point communications among multivendor systems.
inter-AS routing	Routing of packets among different autonomous systems (ASs). *See also* EBGP.

inter-AS services	Services that support VPNs across AS boundaries.
interactive traffic	Network traffic that indicates human involvement in a normally automated process, such as a user typing commands. It appears different from other traffic because one end of the connection is manually controlled. For example, in an automated process, TCP packets can be batched and sent in bulk. However, in a connection between a program and a user, packets are sent when they become available; characters display as they are typed (not after the word is complete). Interactive programs transmit several short IP packets containing individual keystrokes and their echoes, reflecting the real-time actions of a user (or attacker).
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). *See also* route reflection.
interface alarm	Alarm triggered by the state of a physical link on a fixed or installed PIM, such as a link failure or a missing signal. Interface alarms are triggered by conditions on a T1 (DS1), Fast Ethernet, serial, or T3 (DS3) physical interface or by conditions on the sp-0/0/0 adaptive services interface for stateful firewall filter, NAT, IDP, or IPsec services. To enable an interface alarm, you must explicitly set an alarm condition.
interface cost	Value added to all received routes in a distance-vector network before they are placed into the routing table. The Junos OS uses a cost of 1 for this value.
interface label space	Configurable pool of labels from which multiple smaller pools (ranges) of labels can be created. Interfaces are configured to use labels only from a particular pool.
interface preservation	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* link-state replication.
interface routes	Routes that are in the routing table because an interface has been configured with an IP address. *Also called* direct routes.
interface sampling	Packet sampling method used by packet capture, in which entire IPv4 packets flowing in the input or output direction, or both directions, are captured for analysis.
interface set	A logical group of interfaces that describe the characteristics of a set of service VLANs, logical interfaces, or customer VLANs, including the members of the set and the name of the traffic control profiles. *See also* S-VLAN.
interface specifier	Label used in JunosE Software to identify both the physical location (such as chassis slot and port number) of a particular interface type on the router and the logical interface, such as a channelized T3 interface. Used in conjunction with an interface type to uniquely identify the interface on the router. *See also* interface type.
interface type	Label used in JunosE Software to identify the type of interface you are configuring on the router. For example, gigabitEthernet indicates a Gigabit Ethernet interface. Used in conjunction with an interface specifier to uniquely identify the interface on the router. *See also* interface specifier.

interfaces	Physical and logical channels on the router that define how data is transmitted to and received from lower layers in the protocol stack. *See also* subinterface.
interior gateway protocol	IGP. Distributes routing information to routers within an autonomous system, such as IS-IS, OSPF, or RIP. *See also* EGP.
intermediate system	In IS-IS, the network entity that sends and receives packets and can also route packets. A router in OSI internetworking. *See also* ES.
Intermediate System-to-Intermediate System	IS-IS. Link-state, interior gateway routing protocol for IP networks that uses the shortest-path-first (SPF) algorithm to determine routes.
Internal Border Gateway Protocol	IBGP. BGP configuration in which sessions are established between routers in the same autonomous system (AS). *See also* EBGP.
International Data Encryption Algorithm	IDEA. One of the methods at the heart of Pretty Good Privacy (PGP), it uses a 128-bit key. IDEA is patented by Ascom Tech AG and is popular in Europe.
International Electrotechnical Commission	IEC. International standards organization that deals with electrical, electronic, and related technologies. *See* ISO.
International Mobile Station Equipment Identity	IMEI. Unique code used to identify an individual mobile station to a GSM network.
International Mobile Subscriber Identity	IMSI. Information that identifies a particular subscriber to a GSM network.
International Mobile Telecommunications-2000	IMT-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.
International Organization for Standardization	ISO. Worldwide federation of standards bodies that promotes international standardization and publishes international agreements as International Standards.
International Special Committee on Radio Interference	CISPR. An International Electrotechnical Commission (IEC) committee whose principal task is to prepare standards that offer protection of radio reception from interference sources at the higher end of the frequency range (from 9 kHz and above), such as electrical appliances of all types; the electricity supply system; industrial, scientific, and electromedical RF; broadcasting receivers (sound and TV); and IT equipment (ITE).
International Telecommunication Union— Telecommunication Standardization	ITU-T. Group supported by the United Nations that makes recommendations and coordinates the development of telecommunications standards for the entire world. Formerly known as the CCITT.

International Telegraph and Telephone Consultative Committee	Now known as ITU-T (Telecommunication Standardization Sector), organization that coordinates standards for telecommunication on behalf of the ITU (International Telecommunication Union). The ITU is a United Nations specialized agency. ITU-T is a subcommittee of ITU. *See also* ITU-T, CCITT.
Internet Assigned Numbers Authority	IANA. Regulatory group that maintains all assigned and registered Internet numbers, such as IP and multicast addresses. *See also* NIC.
Internet Control Message Protocol	ICMP. Network layer protocol that provides a query and response system for a router or destination host to report an error in data traffic processing to the original source of the packet. Used in router discovery, ICMP allows router advertisements that enable a host to discover addresses of operating routers on the subnet. An ICMP echo request is *also known as* a ping.
Internet Engineering Task Force	IETF. International community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
Internet Group Management Protocol	IGMP. Host-to-router signaling protocol for IPv4 to report multicast group memberships to neighboring routers and determine whether group members are present during IP multicasting. Similarly, multicast routers, such as E Series routers, use IGMP to discover which of their hosts belong to multicast groups and to determine whether group members are present.
Internet Key Exchange	IKE. Part of IPsec that provides ways to exchange keys for encryption and authentication securely over an unsecured medium such as the Internet. IKE enables a pair of security gateways to: • Dynamically establish a secure tunnel over which security gateways can exchange tunnel and key information. • Set up user-level tunnels or SAs, including tunnel attribute negotiations and key management. These tunnels can also be refreshed and terminated on top of the same secure channel. IKE employs Diffie-Hellman methods and is optional in IPsec (the shared keys can be entered manually at the endpoints).
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	IP. Used for sending data from one point to another on the Internet, it provides the functions necessary to deliver blocks of data (datagrams) from a source to a destination over an interconnected system of networks, where sources and destinations are identified by fixed length addresses. *See also* IP address, IPv6.
Internet Protocol Control Protocol	IPCP. Establishes and configures IP over the Point-to-Point Protocol (PPP).
Internet Protocol over Asynchronous Transfer Mode	IPoA. Interface stacking configuration supported on E Series routers. An IPoA interface is IP over ATM 1483 over ATM AAL5 over ATM.

Internet Protocol Security	IPsec. Provides security to IP flows through the use of authentication and encryption: • Authentication verifies that data is not altered during transmission and ensures that users are communicating with the individual or organization that they believe they are communicating with. • Encryption makes data confidential by making it unreadable to everyone except the sender and intended recipient. 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).
Internet Protocol version 4	IPv4. Network Layer (Layer 3) connectionless protocol for the routing of datagrams through gateways connecting networks and subnetworks. It is used on packet switched internetworks, for example, Ethernet.
Internet Protocol version 6	IPv6. *Also known as* IPng (for IP next generation), IPv6 is the next planned version of the IP address system, to eventually supersede IP version 4 (IPv4). While IPv4 uses 32-bit addresses, IPv6 uses 128-bit addresses, which increases the number of possible addresses exponentially. For example, IPv4 allows 4,294,967,296 addresses to be used (2^32). IPv6 allows for over 340,000,000,000,000,000,000,000,000,000,000,000,000 IP addresses. It can be installed as a normal software upgrade in Internet devices and is interoperable with the current IPv4.*See also* IP address.
Internet Security Association and Key Management Protocol	ISAKMP. 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.
Internet service provider	ISP. Company that provides access to the Internet and related services.
Internet-based Over-the-Air	IOTA. Activation method used by cellular network providers such as Sprint for CDMA EV-DO 3G wireless modem cards. **See also** Over-the-Air Service Provisioning, OTASP.
interprovider services	inter-AS services. Services that support VPNs across AS boundaries.
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). *See also* IBGP.
Intrusion Detection and Prevention	IDP. Name of a Juniper product line of security devices that run the IDP OS (operating system).
intrusion detection service	IDS. Inspects all inbound and outbound network activity and identifies suspicious patterns that might indicate a network or system attack from someone attempting to break into or compromise a system.

Inverse Address Resolution Protocol	InARP. Way of determining the IP address of the device at the far end of a circuit.
IOA	Input/output adapter. Physical interface that pairs with line modules to provide connectivity to E120 and E320 routers. *See also* I/O module.
IOTA	Internet-based Over-the-Air. Activation method used by cellular network providers such as Sprint for CDMA EV-DO 3G wireless modem cards. **See also** Over-the-Air Service Provisioning, OTASP.
IP	Internet Protocol. Used for sending data from one point to another on the Internet, it provides the functions necessary to deliver blocks of data (datagrams) from a source to a destination over an interconnected system of networks, where sources and destinations are identified by fixed length addresses. *See also* IP address, IPv6.
IP address	Unique decimal dot format address that devices use to identify and communicate with each other across a network. IPv4 uses 32-bit (4 byte) addresses in a dotted-decimal notation (for example, 192.168.50.4). IPv6 uses 128-bit addresses in a hexadecimal notation of eight 16-bit components separated by colons (for example, 2001:DB8:0:0:8:822:210C:447F). *See also* IPv6.
IP address classes	Four classes that lend themselves to different network configurations, depending on the desired ratio of networks to hosts:

- Class A—The leading bit is set to 0, a 7-bit number, and a 24-bit local host address. Up to 125 class A networks can be defined, with up to 16,777,214 hosts per network.

- Class B—The two highest-order bits are set to 1 and 0, a 14-bit network number, and a 16-bit local host address. Up to 16,382 class B networks can be defined, with up to 65,534 hosts per network.

- Class C—The three leading bits are set to 1, 1, and 0, a 21-bit network number, and an 8-bit local host address. Up to 2,097,152 class C networks can be defined, with up to 254 hosts per network.

- Class D—The four highest-order bits are set to 1, 1, 1, and 0. Class D is used as a multicast address.

IP address pool	Collection of IP addresses maintained by the DHCP server for assignment to DHCP clients and associated with a subnet on either a logical or a physical interface.
IP Control Protocol	IPCP. Establishes and configures IP over the Point-to-Point Protocol (PPP).
IP defragmentation and TCP reassembly	Method of reducing false positives, it reconstructs fragmented traffic. *See also* TCP/IP.
IP gateway	IP gateway is a program or a special-purpose device that transfers IP datagrams from one network to another until the final destination is reached. *Also called* a router.
IP multicast	Internet transmission method that enables a device to send packets to a group of hosts, rather than to a list of individual hosts. Routers use multicast routing algorithms to determine the best route and transmit datagrams throughout the network.

IP pool object   IP pool object represents a range of IP addresses. Use IP pool objects to configure DHCP servers for your managed devices.

IP reassembly   Method of encapsulating and de-encapsulating packets as they enter and leave a tunnel.

IP Security   IPsec. Provides security to IP flows through the use of authentication and encryption:

- Authentication verifies that data is not altered during transmission and ensures that users are communicating with the individual or organization that they believe they are communicating with.

- Encryption makes data confidential by making it unreadable to everyone except the sender and intended recipient.

  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).

IP spoofing   Mimicking the source address of an IP packet. Every IP packet includes the destination address (where the packet is going) and the source address (where the packet came from). The routers that provide Internet communication between distant computers determine the best route for the IP packet using only the destination address and typically ignore the source address. An attacker can fake the source address of a malicious IP packet by modifying the packet headers so that the packet appears to come from a trusted system.

IP sweep   Denial-of-service attack in which attackers send ICMP echo requests (or pings) to different destination addresses and wait for replies that indicate the IP address of a target. If a remote host pings 10 addresses in 0.3 seconds, the security device flags the event as an IP sweep attack and drops the connection to prevent replies. An IP sweep is similar to a port scan attack.

IP television   IPTV. System using the Internet Protocol to deliver digital television service over a network.

IP tracking   Method of monitoring configured IP addresses to see if they respond to ping or ARP requests. You can configure IP tracking with NSRP to determine device or VSD group failover, or to determine if the interface is up or down.

IP tunnels   Secure method of transporting datagrams between routers separated by networks that do not support all the protocols that those routers support. To configure an IP tunnel, you must first configure a TSM interface.

IP version 4   Internet Protocol version 4, IPv4. Network Layer (Layer 3) connectionless protocol for the routing of datagrams through gateways connecting networks and subnetworks. It is used on packet switched internetworks, for example, Ethernet.

IP version 6	Internet Protocol version 6, IPv6. *Also known as* IPng (for IP next generation), IPv6 is the next planned version of the IP address system, to eventually supersede IP version 4 (IPv4). While IPv4 uses 32-bit addresses, IPv6 uses 128-bit addresses, which increases the number of possible addresses exponentially. For example, IPv4 allows 4,294,967,296 addresses to be used (2^{32}). IPv6 allows for over 340,000,000,000,000,000,000,000,000,000,000,000,000 IP addresses. It can be installed as a normal software upgrade in Internet devices and is interoperable with the current IPv4. *See also* IP address.
IPCP	Internet Protocol Control Protocol. Establishes and configures IP over the Point-to-Point Protocol (PPP).
IPoA	Internet Protocol over Asynchronous Transfer Mode. Interface stacking configuration supported on E Series routers. An IPoA interface is IP over ATM 1483 over ATM AAL5 over ATM.
IPsec	Internet Protocol Security. Provides security to IP flows through the use of authentication and encryption:

- Authentication verifies that data is not altered during transmission and ensures that users are communicating with the individual or organization that they believe they are communicating with.

- Encryption makes data confidential by making it unreadable to everyone except the sender and intended recipient.

  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).

IPsec endpoint	ISM. IPsec service module. Receives data from and transmits data to line modules that have ingress and egress ports. Does not pair with a corresponding I/O module that provides ingress and egress ports.
IPsec service module	IP address of the entity that is one of two endpoints in an IPsec SA.
IPTV	IP television. System using the Internet Protocol to deliver digital television service over a network.
IPv4	Internet Protocol version 4. Network Layer (Layer 3) connectionless protocol for the routing of datagrams through gateways connecting networks and subnetworks. It is used on packet switched internetworks, for example, Ethernet.
IPv6	Internet Protocol version 6. *Also known as* IPng (for IP next generation), IPv6 is the next planned version of the IP address system, to eventually supersede IP version 4 (IPv4). While IPv4 uses 32-bit addresses, IPv6 uses 128-bit addresses, which increases the number of possible addresses exponentially. For example, IPv4 allows 4,294,967,296 addresses to be used (2^{32}). IPv6 allows for over 340,000,000,000,000,000,000,000,000,000,000,000,000 IP addresses. It can be installed as a normal software upgrade in Internet devices and is interoperable with the current IPv4. *See also* IP address.

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 routing and bridging. 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. Used by DHCP clients 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. 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. 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. 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.

ISDN BRI ISDN Basic Rate Interface. ISDN interface intended for home and small enterprise applications, it consists of two 64-Kbps B-channels to carry voice or data, and one 16-Kbps D-channel for control and signaling. *See also* B-channel, D-channel.

ISM IPsec service module. Receives data from and transmits data to line modules that have ingress and egress ports. Does not pair with a corresponding I/O module that provides ingress and egress ports.

ISO International Organization for Standardization. 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.

IT power system In an IT power system, the distribution system has no connection to earth or has only a high impedance connection. In such systems, an insulation monitoring device is used to monitor the impedance.

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 world.

ITU-T G.991.2
International standard recommendation that describes a data transmission method for SHDSL for data transport in telecommunications access networks. The standard also describes the functionality required for interoperability of equipment from various manufacturers.

ITU-T G.992.1
International standard recommendation that describes ADSL. Annex A defines how ADSL works over twisted-pair copper (POTS) lines. Annex B defines how ADSL works over ISDN lines.

ITU-T G.993.2
International standard recommendation that describes a data transmission method for VDSL2 transceivers.

ITU-T G.994.1
International standard recommendation that describes the types of signals, messages, and procedures exchanged between DSL equipment when the operational modes of equipment need to be automatically established and selected.

ITU-T G.997.1
International standard recommendation that describes the physical layer management for ADSL transmission systems, including the means of communication on a transport transmission channel defined in the physical layer recommendations. The standard also describes the content and syntax of network elements for configuration, fault management, and performance management.

ITU-T H.248
International standard recommendation that describes communication between a gateway controller and a media gateway.

ITU-T H.323
International standard recommendation that describes packet-based multimedia communications over networks that do not guarantee class of service, such as IP networks, providing a widely-used standard for VoIP and conferencing that is modeled on ISDN PRI. It is implemented as an Application Layer Gateway (ALG) that provides secure VoIP communication between terminal hosts, such as IP phones and multimedia devices, in which the gatekeeper devices manage call registration, admission, and call status for VoIP calls. The gatekeepers can reside in the two different zones, or in the same zone.

J

J-cell
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-Flow
Method of collecting IP traffic flow statistics from routing devices. J-Flow does not require any special protocol for connection setup, and does not require any external changes to networked traffic, packets, or any other devices in the network.

J-Web
Graphical Web browser interface to the Junos OS 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 OS package containing updates to the kernel.

jbundle
Junos OS package containing all possible software package files.

JCS	Juniper Control System. 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.
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.
JDBC	Java Database Connectivity. API that provides a standard means of database-independent connectivity between the Java platform and a wide range of databases.
jdocs	Junos OS 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 OS package containing the basic components of the software.
Job Manager	Module of the NSM user interface that tracks the status of major administrative tasks, such as importing or updating a device, as commands travel to the device and back to the management server.
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 OS package containing the embedded OS software for operating the Packet Forwarding Engine.
jroute	Junos OS package containing the software used by the Routing Engine.
JSF	Juniper Services Framework.
JSRP	Junos Services Redundancy Protocol. A process that controls chassis clustering of Junos OS devices.
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

kB   *See* kilobyte, KiB. Represents approximately 1000 bytes, depending on whether a decimal (kB) or a binary (KiB) system of measurement is being used. When dealing with network capacity, the decimal version (kB) is the standard, with each kB representing 1000 bytes. However, in storage devices, the binary value of 1024 bytes is used, and sometimes expressed using the abbreviation KiB, although this term is not yet standard in common usage. When precise calculations of storage or network capacity are required, it is important to use an appropriate value for kilobytes.

keepalive   Signal sent at predefined intervals to determine that the connection between two links or routers is still active (up). Parameters important to keepalive include time, interval, and retry.

keepalive message   Sent between network devices to inform each other that they are still active. Keepalive messages are used to identify inactive or failed connections.

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

kernel forwarding table   Table of best routes to all destinations reachable by the router. For each destination, the table has only the single best route to the destination selected from the IP routing table. The Junos OS 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. *Also known as* forwarding table.

key   Commonly used way to protect the integrity and privacy of information is to rely upon the use of secret information for signing and encryption. These pieces of secret information are known as keys.

key management   Method used in a security system to create and manage security keys, including selection, exchange, storage, certification, expiration, revocation, changing, and transmission of keys. Most of the work in managing information security systems lies in the key management.

key management daemon   kmd. Process that provides IPsec authentication services for encryption PICs.

KiB   kilobyte, kB. Represents approximately 1000 bytes, depending on whether a decimal (kB) or a binary (KiB) system of measurement is being used. When dealing with network capacity, the decimal version (kB) is the standard, with each kB representing 1000 bytes. However, in storage devices, the binary value of 1024 bytes is used, and sometimes expressed using the abbreviation KiB, although this term is not yet standard in common usage. When precise calculations of storage or network capacity are required, it is important to use an appropriate value for kilobytes.

kilobyte   kB, KiB. Represents approximately 1000 bytes, depending on whether a decimal (kB) or a binary (KiB) system of measurement is being used. When dealing with network capacity, the decimal version (kB) is the standard, with each kB representing 1000 bytes. However, in storage devices, the binary value of 1024 bytes is used, and sometimes expressed using the abbreviation KiB, although this term is not yet standard in common usage. When precise calculations of storage or network capacity are required, it is important to use an appropriate value for kilobytes.

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

L

L-LSP	label-only-inferred-PSC LSP. One of two types of LSPs employed by MPLS to support differentiated services. The per-hop behavior applied to the packet is determined from the packet label and the EXP field of the MPLS shim header. *See also* E-LSP, shim header.
L2C	Layer 2 control. *Also known as* Access Node Control Protocol, ANCP. Based on a subset of the General Switch Management Protocol (GSMP) in which IGMP is no longer terminated or proxied at the access node. Instead, IGMP passes through the access node transparently.
L2TP	Layer 2 Tunneling Protocol. 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.
L2TP access concentrator	LAC. Device that receives packets from a remote client and forwards them to an L2TP network server (LNS) on a remote network.
L2TP dial-out	Method for corporate virtual private networks (VPNs) that use a Broadband Remote Access Server (B-RAS) to dial out to remote offices that have only narrowband dial-up access.
L2TP network server	LNS. Node that acts as one side of an L2TP tunnel endpoint and is a peer to the LAC. The logical termination point of a PPP connection that is being tunneled from the remote system by the LAC.
L2TP tunnel switching	Router configuration that enables you to switch packets between one session terminating at an L2TP LNS and another session originating at an L2TP LAC. A tunnel-switched LAC differs from a conventional LAC because it uses two interface columns: one for the incoming session (LNS) and one for the outgoing session (LAC). The router forwards traffic from the incoming session to the outgoing session and vice versa.
Label Distribution Protocol	LDP. 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.
label edge router	LER. Label-switching router serving as an ingress node or an egress node.
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 that each router along the path of an LSP 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	Multiprotocol Label Switching, MPLS. Mechanism for engineering network traffic patterns that functions by assigning short labels to network packets that describe how to forward them through the network. *See also* traffic engineering, TE.
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	LSI. Logical interface supported by the Junos OS that provides VPN services (such as VPLS and Layer 3 VPNs) normally provided by a Tunnel Services PIC.
label-switched path	LSP. Sequence of routers that cooperatively perform MPLS operations for a packet stream; the path traversed by a packet that is routed by MPLS. An LSP is a unidirectional, point-to-point, half-duplex connection carrying information downstream from the ingress (first) router to the egress (last) router. The ingress and egress routers cannot be the same router.
label-switching router	LSR, label-switching router. Router on which MPLS is enabled and that can process label-switched packets; an MPLS node that can forward Layer 3 packets based on their labels.
LAC	L2TP access concentrator. Device that receives packets from a remote client and forwards them to an L2TP network server (LNS) on a remote network.
LACP	Link Aggregation Control Protocol. Mechanism for exchanging port and system information to create and maintain LAG bundles.
LAG	link aggregation group. Two or more network links bundled together to appear as a single link. Distributes MAC clients across the link layer interface and collects traffic from the links to present to the MAC clients of the LAG. *Also known as* a bundle.
LAN	local area network. Covers a local area, like a home, office, or small group of buildings such as a campus.
LAN PHY	Local Area Network Physical Layer Device. Allows 10-Gigabit Ethernet wide area links to use existing Ethernet applications. *See also* PHY and WAN PHY.
land attack	Denial-of-service attack in which the attacker may send spoofed SYN packets containing the IP address of the target as both the destination and source IP address, creating an empty connection. These connections flood the target system, overwhelming it.
latency	Delay in the transmission of a packet through a network from beginning to end.
launch pad	In NSM, an otherwise blank user interface pane that provides access to commonly used functionality within the associated NSM module.

Layer 1 *Also known as* physical layer. First and lowest level in the seven-layer OSI reference model for network protocol design and in the five-layer TCP/IP protocol stack. This layer defines all the electrical and physical specifications for devices and provides the transmission of bits over the network medium. It includes the physical media: cables, microwaves, and networking equipment such as hubs and repeaters.

Layer 2 Second level in the seven-layer OSI reference model for network protocol design and in the five-layer TCP/IP protocol stack. This layer provides the functional and procedural means to transfer data between network entities by splitting data into frames to send on the physical layer and receiving acknowledgment frames. It performs error checking and retransmits frames not received correctly. In general, it controls the flow of information across the link, providing an error-free virtual channel to the network layer. *Also known as* data link layer. *See also* OSI.

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. *See also* AAL5 mode, cell-relay mode, standard AAL5 mode, trunk mode.

Layer 2 control L2C. *Also known as* Access Node Control Protocol, ANCP. Based on a subset of the General Switch Management Protocol (GSMP) in which IGMP is no longer terminated or proxied at the access node. Instead, IGMP passes through the access node transparently.

Layer 2 Tunneling Protocol L2TP. 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.

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 *Also known as* network layer. The third level in the seven-layer OSI reference model for network protocol design and in the five-layer TCP/IP protocol stack. This layer performs the basic task of routing data across the network (getting packets of data from source to destination).

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.

Layer 4 *Also known as* transport layer. The fourth level in the seven-layer OSI reference model for network protocol design and in the five-layer TCP/IP protocol stack. This layer provides communication between applications residing in different hosts and reliable transparent data transfer between end users. It is the first layer to address reliability.

Layer 5	*Also known as* application layer, session layer. The fifth and highest level in the five-layer TCP/IP stack. This layer is used by most programs for network communication. Data is passed from the program in an application-specific format, then encapsulated into a transport layer protocol.
Layer 6	*Also known as* presentation layer. The sixth level in the seven-layer OSI reference model for network protocol design. This layer transforms data to provide a standard interface for the application layer.
Layer 7	*Also known as* application layer. The seventh and highest level in the seven-layer OSI reference model for network protocol design that manages communication between application processes. This layer is the main interface for users to interact with application programs such as electronic mail, database managers, and file-server software. *See also* OSI.
LCC	line-card chassis. Term used by the Junos OS command-line interface (CLI) to refer to a T640 routing node in a routing matrix.
LCP	Link Control Protocol. 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.
LDP MD5 authentication	Method of providing protection, using a shared secret (password), against spoofed TCP segments that can be introduced into the connection streams for LDP sessions. Authentication is configurable for both directly connected and targeted peers. Any given pair of peers must share the same password.
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.
lease	Period of time during which an IP address is allocated, or bound, to a DHCP client. A lease can be temporary (dynamic binding) or permanent (static binding).
LER	label edge router. Label-switching router serving as an ingress node or an egress node.
level 1 routing	Refers to routing *within* an area; a level 1 router:

- (or intermediate system) tracks all the individual links, routers, and end systems within a level 1 area.
- does not know the identity of routers or destinations outside its area.
- forwards all traffic for destinations outside its area to the nearest level 2 router within its area.

level 2 routing	Refers to routing *between* areas; a level 2 router:

- knows the level 2 topology and which addresses are reachable through each level 2 router.

- tracks the location of each level 1 area.

- is not concerned with the topology within any level 1 area (for example, the details internal to each level 1 area).

- can identify when a level 2 router is also a level 1 router within the same area.

- is the only router type that can exchange packets with external routers located outside its routing domain.

LFI	link fragmentation and interleaving. 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. Method used to detect problems on links and spans on an Ethernet network defined in IEEE 802.3ah. *See also* OAM.
liblicense	Library that includes messages generated for routines for software license management.
libpcap	Implementation of the **pcap** application programming interface. Used by a program to capture packets traveling over a network. *See also* pcap.
Lightweight Directory Access Protocol	LDAP. Software protocol used for locating resources on a public or private network.
limited operational environment	Term used to describe the restrictions placed on FIPS-certified equipment. *See* FIPS.
line layer	For a channelized OCx/STMx interface, the layer that manages the transport of SONET/SDH payloads, which are embedded in a sequence of STS/STM frames in the physical medium. This layer is responsible for multiplexing and synchronization. *See also* path layer, section layer.
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 module	LM. Acts as a frame forwarding engine for the physical interfaces (I/O modules and IOAs) and processes data from different types of network connections.
line module redundancy	Configuration in which an extra line module in a group of identical line modules provides redundancy if one of the modules fails. The process by which the router switches to the spare line module is called switchover. The requirements for line module redundancy depend on the type of router that you have.
line-card chassis	LCC. Term used by the Junos OS command-line interface (CLI) to refer to a T640 routing node in a routing matrix.

link	Communication path between two neighbors. A link is up when communication is possible between the two end points.
Link Aggregation Control Protocol	LACP. Mechanism for exchanging port and system information to create and maintain LAG bundles.
link aggregation group	802.3ad link aggregation, LAG. Two or more network links bundled together to appear as a single link. Distributes MAC clients across the link layer interface and collects traffic from the links to present to the MAC clients of the LAG. *Also known as* a bundle.
Link Control Protocol	LCP. Traffic controller used to establish, configure, and test data-link connections for the Point-to-Point Protocol (PPP).
link fault management	LFM. Method used to detect problems on links and spans on an Ethernet network defined in IEEE 802.3ah. *See also* OAM.
link fragmentation and interleaving	LFI. 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.
Link Integrity Protocol	LIP. Runs on the member links of a Multilink Frame Relay (MLFR) bundle. Several types of LIP messages allow member links to join and leave the bundle.
link layer	Data Link Layer. The second level in the seven-layer OSI reference model for network protocol design and in the five-layer TCP/IP protocol stack. This layer provides the functional and procedural means to transfer data between network entities by splitting data into frames to send on the physical layer and receiving acknowledgment frames. It performs error checking and retransmits frames not received correctly. In general, it controls the flow of information across the link, providing an error-free virtual channel to the network layer. *See also* OSI.
Link Management Protocol	LMP. Part of GMPLS, a protocol used to define a forwarding adjacency between peers and to maintain and allocate resources on the traffic engineering links.
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	LSQ. Interfaces configured on the Adaptive Services PIC or ASM that support MLPPP and MLFR traffic and also fully support Junos OS class-of-service (CoS) components.
link-state	link-state routing. One of two main classes of routing protocols used in packet-switched networks for computer communications; the other main class is distance-vector. The basic concept of link-state routing is that every node constructs a map of the connectivity of the network, determining which nodes are connected to which other nodes. Each node then independently calculates the best next hop from it to every possible destination in the network, using the Shortest Path First (SPF) algorithm. The collection of best next hops forms the node's routing table. Examples of link-state routing protocols include OSPF and IS-IS.

link-state acknowledgment	OSPF data packet used to inform a neighbor that a link-state update packet has been successfully received.
link-state advertisement	LSA. OSPF data structure that is advertised in a link-state update packet. Each LSA uniquely describes a portion of the OSPF network, containing information about neighbors and path costs. LSAs are used by the receiving routers to maintain their routing tables.
link-state database	LSDB. Contains all routing knowledge in a link-state network. Each router runs the SPF algorithm against this database to locate the best network path to each destination in the network.
link-state PDU	LSP. Packet that contains information about the state of adjacencies to neighboring systems.
link-state protocol	LSP. Routing protocol, such as OSPF and IS-IS, where each router shares information with other routers (by flooding information about itself to every reachable router in the routing area) to determine the best path. Link-state protocols use characteristics of the route such as speed and cost, as well as current congestion, to determine the best path. In link-state routing, every node receives a map of the connectivity of the network, then independently calculates the best next hop for every possible destination in the network. The collection of best next hops forms the routing table for the node. Link state information is transmitted only when something has changed in the network. *See also* routing table.
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* interface preservation.
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 routing	One of two main classes of routing protocols used in packet-switched networks for computer communications; the other main class is distance-vector. The basic concept of link-state routing is that every node constructs a map of the connectivity of the network, determining which nodes are connected to which other nodes. Each node then independently calculates the best next hop from it to every possible destination in the network, using the Shortest Path First (SPF) algorithm. The collection of best next hops forms the node's routing table. Examples of link-state routing protocols include OSPF and IS-IS.
link-state update	OSPF data packet that contains one of multiple LSAs. It is used to advertise routing knowledge into the network.

linktrace message
LTM. Used by one maintenance end point (MEP) to trace the path to another MEP or maintenance intermediate point (MIP) in the same domain. It is needed for loopback (ping). All MIPs respond with a linktrace response to the originating MEP. After decreasing the TTL by one, 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. *See also* MIP, MEP.

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
LTR. *Also known as* link trace message, LTM. Used by one maintenance end point (MEP) to trace the path to another MEP or maintenance intermediate point (MIP) in the same domain. It is needed for loopback (ping). All MIPs respond with a linktrace response to the originating MEP. After decreasing the TTL by one, 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.

LIP
Link Integrity Protocol. Runs on the member links of a Multilink Frame Relay (MLFR) bundle. Several types of LIP messages allow member links to join and leave the bundle.

LLC
logical link control. Data-link layer protocol used on a LAN. The LLC is responsible for managing communications links and handling frame traffic. LLC1 provides connectionless data transfer, and LLC2 provides connection-oriented data transfer. *See also* data link layer, OSI.

LLC frame
Unit of data that contains specific information about the LLC layer and identifies line protocols associated with the layer. *Also called* LLC.

LM
line module. Acts as a frame forwarding engine for the physical interfaces (I/O modules and IOAs) and processes data from different types of network connections.

LMI
Local Management Interface. Enhancements to the basic Frame Relay specifications, providing support for the following:

- 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.
LNS	L2TP network server. Node that acts as one side of an L2TP tunnel endpoint and is a peer to the LAC. The logical termination point of a PPP connection that is being tunneled from the remote system by the LAC.
lo0	loopback interface. Logical interface that emulates a physical interface on the security device, but 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. *See also* unnumbered interface.
load balancing	Method used to distribute workload to processors to improve the throughput of concurrent connections. Basically, it 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* per-packet load balancing.
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 address pool alias	Alternate name for an existing local address pool. It consists of an alias name and a pool name.
local address server	Server that allocates IP addresses from a pool of addresses stored locally on the router. A local address server is defined in the context of a virtual router. Local address servers exist as long as the virtual router exists or until you remove them by deleting all configured pools.
local area network	LAN. Covers a local area, like a home, office, or small group of buildings such as a campus.local area network. Covers a local area, like a home, office, or small group of buildings such as a campus.
Local Area Network Physical Layer Device	LAN PHY. Allows 10-Gigabit Ethernet wide area links to use existing Ethernet applications. *See also* PHY and WAN PHY.
local ATM passthrough	Ability of the router to emulate packet-based ATM switching. Useful for customers who run IP in most of their network but still have to carry a small amount of native ATM traffic.
local authentication server	AAA server that enables the E Series router to provide local PAP and CHAP user authentication for subscribers. The router also provides limited authorization, using the IP address, IP address pool, and operational virtual router parameters. When a subscriber logs in to the E Series router that is using local authentication, the subscriber is authenticated against user entries in a local user database; the optional parameters are assigned to subscribers after the subscriber is authenticated.
local loopback	Ability to loop the data back toward the router on supported line modules. Also sends an alarm indication signal out toward the network.

Local Management Interface	LMI. Enhancements to the basic Frame Relay specifications, providing support for the following: • 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.
local packet	Chunk of data destined for or sent by the Routing Engine.
local preference	Optional BGP path attribute (**LOCAL_PREF**) 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 routing table	Database local to the protocol that contains all the routes known by that protocol to the prefixes in the table. *Also known as* a routing information base, or RIB. *See also* global routing table, routing table.
local significance	Concept used in an MPLS network where the label values are unique only between two neighbor routers.
local-use community	Convenient way to categorize groups of routes to facilitate the use of routing policies. *Also called* private community or general community.
lockout	Object state during which the object cannot be edited.
log	Grouping of log entries, which are the systematic recording of specific types of data processing events.
log category	Term to describe the log type, such as alarm, config, traffic, and so on.
log ID	Unique identifier label for a log, derived from a combination of the date and log number.
Log Investigator	Module of the NSM user interface that has tools for analyzing log entries in depth. Use the Log Investigator to manipulate and change constraints on log information, correlate log entries visually and rapidly, and filter log entries while maintaining the broader picture.
Log Viewer	Module of the NSM user interface that displays the entries of traffic logs for devices on your network.
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
LLC. Data-link layer protocol used on a LAN. The LLC is responsible for managing communications links and handling frame traffic. LLC1 provides connectionless data transfer, and LLC2 provides connection-oriented data transfer. *See also* data link layer, OSI.

logical operator
Characters used in a firewall filter to represent a Boolean AND or OR operation.

logical router
Also called 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.

logical system
Logical routing device that is partitioned from an M Series, MX 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 OS 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
Also called local loopback, network loopback, remote loopback. Ability to loop the data back toward the router on supported line modules. Also sends an alarm indication signal out toward the network.

loopback address
IP address type used by a node to send a packet to itself (specially designated for the software loopback interface of a device). The loopback interface has no hardware associated with it and is not physically connected to a network.

loopback interface
lo0. Logical interface that emulates a physical interface on the security device, but 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. *See also* 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.) *See also* strict hop.

loose-source routing
MPLS routing method that specifies a set of hops that the packet must traverse. The specified hops do not need to be adjacent, and the routing does not need to include every hop in the path. *See also* strict-source routing.

loss-priority map
Maps the loss priority of incoming packets based on code point values.

low-density keepalive mode
Mode in which, when the keepalive timer expires, the interface always sends an LCP echo request, regardless of whether the peer is silent. *See also* high-density keepalive mode.

lower-speed IQ interfaces
E1, NxDS0, and T1 interfaces configured on an IQ PIC.

LPDU
LLC protocol data unit. Unit of data that contains specific information about the LLC layer and identifies line protocols associated with the layer (LLC frame) on a DLSw network.

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, containing information about neighbors and path costs. LSAs are used by the receiving routers to maintain their routing tables.

LSDB link-state database. Computerized representation of the topology of an autonomous system. *See also* AS.

LSI label-switched interface. Logical interface supported by the Junos OS 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 path traversed by a packet that is routed by MPLS. An LSP is a unidirectional, point-to-point, half-duplex connection carrying information downstream from the ingress (first) router to the egress (last) router. The ingress and egress routers cannot be the same router.

- link-state PDU (protocol data unit). In IS-IS, a broadcast by link-state protocols containing information about neighbors and path costs that is used to maintain routing tables. *See also* link-state advertisement.

- link-state protocol. Routing protocol, such as OSPF and IS-IS, where each router shares information with other routers (by flooding information about itself to every reachable router in the routing area) to determine the best path. Link-state protocols use characteristics of the route such as speed and cost, as well as current congestion, to determine the best path. In link-state routing, every node receives a map of the connectivity of the network, then independently calculates the best next hop for every possible destination in the network. The collection of best next hops forms the routing table for the node. Link state information is transmitted only when something has changed in the network. *See also* routing table.

LSP priority level Relative importance of an LSP that determines which LSPs can preempt other LSPs. Priorities are in the range 0–7 in order of decreasing priority.

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 OS class-of-service (CoS) components.

LSR label-switching router. Router on which MPLS is enabled and that can process label-switched packets; an MPLS node that can forward Layer 3 packets based on their labels.

LTM linktrace message. Used by one maintenance end point (MEP) to trace the path to another MEP or maintenance intermediate point (MIP) in the same domain. It is needed for loopback (ping). All MIPs respond with a linktrace response to the originating MEP. After decreasing the TTL by one, 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. *Also known as* linktrace message, LTM. Used by one maintenance end point (MEP) to trace the path to another MEP or maintenance intermediate point (MIP) in the same domain. It is needed for loopback (ping). All MIPs respond with a linktrace response to the originating MEP. After decreasing the TTL by one, 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. |

M

MA	maintenance association. Combined set of nodes (MEPs and MIPs) within a maintenance domain. *See also* LTR, linktrace message, LTR, linktrace response.
MAC	• media access control (address). A unique code assigned to every piece of hardware that connects to the network. 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. *See also* MAC address.
	• Message Authentication Code. In cryptography, a short piece of information used to authenticate a message. A MAC algorithm accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC, or a tag. Sometimes called message integrity code (MIC) to distinguish the MAC function from the MAC (media access control) address.
MAC address	media access control address. Serial number permanently stored in a device adapter to uniquely identify the device. *See also* MAC.
MAC address validation	Verification process performed on each incoming packet to prevent spoofing on IP Ethernet-based interfaces, including bridged Ethernet interfaces.
magic number	Randomly generated number that identifies one end of a point-to-point connection. Each side negotiates its magic number, taking note of the other's magic number. If both sides discover that the magic numbers they are negotiating are the same, each side attempts to change its magic number. If they are not successful, and the magic numbers remain the same, the session terminates because of the loopback that is detected.
main mode	Mode of IKE phase 1 negotiations that protects the identities of the peers during negotiations and enables greater proposal flexibility than aggressive mode. Main mode is more time-consuming than aggressive mode because more messages are exchanged between peers. (Six messages are exchanged in main mode.) *See also* aggressive mode.
maintenance association	MA. Combined set of nodes (MEPs and MIPs) within a maintenance domain. *See also* LTR, linktrace message, LTR, linktrace response.
maintenance association end point	MEP, maintenance end point. End point (beginning or ending) of a maintenance domain. *See also* LTR, linktrace message, LTR, linktrace response.

maintenance association ID	Identifier associated with the maintenance association.
maintenance association intermediate point	MIP. Intermediate node within the maintenance domain. *See also* LTM, linktrace message, LTR, linktrace response.
maintenance data link	MDL. Type of message that can be used to determine the status of a line and to display statistics for the remote end of a connection.
maintenance domain	Part of the network where connectivity fault detection is performed.
maintenance end point	MEP. End point (beginning or ending) of a maintenance domain. *See also* LTM.
maintenance point	MP. A MEP or a MIP is a maintenance point.
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	mgd. Junos OS process responsible for managing all user access to the router.
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. *See also* permanent interface.
Management Information Base	MIB. Definition of an object that can be managed by SNMP.
Management Module, JCS	JCS Management Module. Chassis management hardware and software used to access and configure the Juniper Control System (JCS) platform.
Manual Commit Mode	Feature of JunosE Software where configuration changes affect only the current system configuration (the running configuration), without affecting the CLI prompt.
manual secure IP interfaces	Interfaces that use a preconfigured set of SA parameters to secure traffic flowing through a secure IP interface. If these are not used, the interface drops all traffic it receives. The router keeps statistics for dropped traffic. Both peer security gateways must contain a manually provisioned secure IP tunnel. *See also* signaled secure IP interface.
map tag	Unique string used to identify a route map.
mapped IP address	MIP. Direct one-to-one mapping of traffic destined for one IP address to another IP address.
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 OS does not allow martian routes in the **inet.0** routing table.
MAS	mobile network access subsystem. GSN application subsystem that contains the access server.
mask	*Also called* subnet mask. Number of bits of the network address used to separate the network information from the host information in a Class A, Class B, or Class C IP address, allowing the creation of subnetworks. In binary notation, a series of 1s followed by a series of contiguous 0s. The 1s represent the network number; the 0s represent the host number. Use of masks can divide networks into subnetworks by extending the network portion of the address into the host portion. Subnetting increases the number of subnetworks and reduces the number of hosts.
master	Router in control of the OSPF database exchange during an adjacency formation.
master router	VRRP router that takes the responsibility of forwarding packets sent to the IP addresses associated with the virtual router, and that answers ARP requests for these IP addresses. If the IP address owner is available, it always becomes the master. *See also* backup router.
match	Logical concept used in a routing policy or firewall filter, it denotes the criteria used to find a route or IP packet before an action is performed.
match clause	Portion of a route map that specifies the attribute values that determine whether a route matches the route map. A route that has the same attribute values passes the match condition. Routes that pass all the match conditions match the route map.
match policy list	Similar to a route map but contains only match clauses and no set clauses. *See also* policy list.
match type	Junos OS syntax used in a route filter to better describe the routes that should match the policy term.
MAU	medium attachment unit. Small device that converts signals between an attachment unit interface (AUI) and coaxial cable.
maximum allocation bandwidth constraints model	MAM. 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.
maximum received reconstructed unit	MRRU. Similar to the maximum transmission unit (MTU), but is specific to link services interfaces such as MLPPP. *See also* MTU.
maximum transmission unit	MTU. Size in bytes of the largest protocol data unit that can be passed on in a link. The standard MTU for an Ethernet link is 1500.

MB megabyte, MiB. Represents approximately 1,000,000 bytes, depending on whether a decimal (MB) or a binary (MiB) system of measurement is being used. In storage devices, the standard value for one megabyte (MB) is 1,000,000 bytes. For computer memory, however, one megabyte is typically 1,048,576 (1024 x 1024) bytes. When precise calculations of storage capacity or memory capacity are required, it is important to use an appropriate value for megabytes.

Mb megabit, Mbit. Unit used in measuring digital transmission (data transfer rates), one megabit is equal to 1,000,000 bits. Not to be confused with megabytes, the megabit base unit is an 8-bit-sized byte, so one megabit is equal to 125,000 bytes.

MBGP Multicast Border Gateway Protocol, MP-BGP. *Also called* Multiprotocol Border Gateway Protocol. Extensions to BGP that permit the configuration of a multicast routing topology within and between BGP ASs. A BGP unicast routing protocol that allows different types of addresses (known as address families) to be distributed in parallel. This allows information about the topology of IP multicast-capable routers to be exchanged separately from the topology of normal unicast routers.

Mbit megabit, Mb. Unit used in measuring digital transmission (data transfer rates), one megabit is equal to 1,000,000 bits. Not to be confused with megabytes, the megabit base unit is an 8-bit-sized byte, so one megabit is equal to 125,000 bytes.

MBone multicast backbone. 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.

MCC Mobile Country Code. Used to identify the country in which a mobile station is located. The MCC is part of the International Mobile Subscriber Identity (IMSI) number, which uniquely identifies a particular subscriber in a mobile network.

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. One-way hashing algorithm that produces a 128-bit hash used for generating message authentication signatures. MD5 is used in AH and ESP. *See also* hashing, SHA-1.

MD5 authentication HMAC MD5 authentication. Method for IS-IS that prevents unauthorized routers from injecting false routing information into your network or forming adjacencies with your router. The router creates secure digests of the packets, encrypted according to the HMAC MD5 message-digest algorithms. The digests are inserted into the packets from which they are created. Depending on the commands you issue, the digests can be inserted into hello packets, link-state PDUs, complete sequence number PDUs, and partial sequence number PDUs.

MDL maintenance data link. Type of message that can be used to determine the status of a line and to display statistics for the remote end of a connection.

MDRR modified deficit round robin. Method for selecting queues to be serviced. *See also* queue.

MDT	multicast distribution tree. Path between the sender (host) and the multicast group (receiver or listener).
mean time between failures	MTBF. Measure of hardware component reliability.
MED	multiple exit discriminator. 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.
media access control (address)	MAC address. A unique code assigned to every piece of hardware that connects to the network. 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.
Media Gateway Control Protocol	MGCP. Text-based, application layer protocol used for call set up and control. The protocol is based on a master/slave call control architecture: the media gateway controller (call agent) maintains call control intelligence, and media gateways carry out the instructions from the call agent.
Media Gateway Controller	MGC. Avaya media server that controls the parts of the call state that pertain to connection control for media channels in a media gateway. The MGC is the controlling entity in an ITU-T H.248 relationship.
mediation device	Device that receives mirrored traffic from E Series routers during packet mirroring. *Also called* the analyzer device.
medium attachment unit	MAU.medium attachment unit. Small device that converts signals between an attachment unit interface (AUI) and coaxial cable.
megabit	Mbit or Mb. Unit used in measuring digital transmission (data transfer rates), one megabit is equal to 1,000,000 bits. Not to be confused with megabytes, the megabit base unit is an 8-bit-sized byte, so one megabit is equal to 125,000 bytes.
megabyte	MB or MiB. Represents approximately 1,000,000 bytes, depending on whether a decimal (MB) or a binary (MiB) system of measurement is being used. In storage devices, the standard value for one megabyte (MB) is 1,000,000 bytes. For computer memory, however, one megabyte is typically 1,048,576 (1024 x 1024) bytes. When precise calculations of storage capacity or memory capacity are required, it is important to use an appropriate value for megabytes.
member AS	Name of the autonomous system being included in a BGP confederation.
MEP	maintenance end point. End point (beginning or ending) of a maintenance domain. *See also* LTM, link trace message.
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 Authentication Code	MAC. In cryptography, a short piece of information used to authenticate a message. A MAC algorithm accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC, or a tag. Sometimes called message integrity code (MIC) to distinguish the MAC function from the MAC (media access control) address.
Message Digest 5	MD5. One-way hashing algorithm that produces a 128-bit hash used for generating message authentication signatures. MD5 is used in AH and ESP. *See also* hashing, SHA-1.
metric	Value associated with a route that the virtual router uses to select the active route when there are multiple routes to the same destination network with the same preference value. The metric value for connected routes is always 0. The default metric value for static routes is 1, but you can specify a different value when defining a static route.
MGC	Media Gateway Controller. Avaya media server that controls the parts of the call state that pertain to connection control for media channels in a media gateway. The MGC is the controlling entity in an ITU-T H.248 relationship.
MGCP	Media Gateway Control Protocol. Text-based, application layer protocol used for call set up and control. The protocol is based on a master/slave call control architecture: the media gateway controller (call agent) maintains call control intelligence, and media gateways carry out the instructions from the call agent.
mgd	management daemon. Junos OS process responsible for managing all user access to the router.
MiB	megabyteMB. Represents approximately 1,000,000 bytes, depending on whether a decimal (MB) or a binary (MiB) system of measurement is being used. In storage devices, the standard value for one megabyte (MB) is 1,000,000 bytes. For computer memory, however, one megabyte is typically 1,048,576 (1024 x 1024) bytes. When precise calculations of storage capacity or memory capacity are required, it is important to use an appropriate value for megabytes.
MIB	Management Information Base. Definition of an object that can be managed by SNMP.
MIC	Modular Interface Card. Network interface–specific card that can be installed on an MPC in the router.
Microcom Networking Protocol	MNP. Protocol that provides error correction and data compression for asynchronous modem transmission
midplane	Hardware component that physically separates front and rear cavities inside the chassis, distributes power from the power supplies, and transfers packets and signals between router components that plug into it. *See also* redundancy midplane.

Mini-Physical Interface Module	Mini-PIM. Circuit board designed for use with Juniper Networks devices. The board enables easy addition or modification of physical interfaces on a device.
Mini-PIM	Mini-Physical Interface Module. Circuit board designed for use with Juniper Networks devices. The board enables easy addition or modification of physical interfaces on a device.
MIP	• maintenance intermediate point. Intermediate node within the maintenance domain. *See also* LTM, linktrace message, LTR, linktrace response.
	• mapped Internet Protocol (IP) address. Direct one-to-one mapping of traffic destined for one IP address to another IP address.
mirrored interface	Statically or dynamically configured interface on which traffic is being mirrored during packet mirroring on E Series routers.
mirrored user	User whose traffic is being mirrored during packet mirroring on E Series routers.
Miscellaneous Control Subsystem	MCS. On the M40e and M160 routers, provides control and monitoring functions for router components and SONET clocking for the router.
MLD	Multicast Listener Discovery. Protocol that manages the membership of hosts and routers in multicast groups. An IPv6 protocol that hosts use to report their multicast group memberships to neighboring routers. Similarly, multicast routers, such as E Series routers, use MLD to discover which of their hosts belong to multicast groups.
MLD proxy	Method by which the router issues MLD host messages on behalf of hosts that the router discovered through standard MLD interfaces. The router acts as a proxy for its hosts.
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. *See also* PPP.
MM	Juniper Control System (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. *See also* single-mode fiber.
MNC	Mobile Network Code. Unique identifier assigned to a mobile operator/carrier. It is used in conjunction with the MCC to specify carrier and country.
MNP	Microcom Networking Protocol. Protocol that provides error correction and data compression for asynchronous modem transmission.

Mobile Country Code	MCC. Used to identify the country in which a mobile station is located. The MCC is part of the International Mobile Subscriber Identity (IMSI) number, which uniquely identifies a particular subscriber in a mobile network.
mobile network access subsystem	MAS. GSN application subsystem that contains the access server.
Mobile Network Code	MNC. Unique identifier assigned to a mobile operator/carrier. It is used in conjunction with the MCC to specify carrier and country.
mobile point-to-point control subsystem	MPS. GSN application subsystem that controls all functionality associated with a particular connection.
Mobile Station	MS. Mobile device, such as a cellular phone or a mobile personal digital assistant (PDA).
Mobile Station Integrated Services Digital Network Number	MSISDN. Number that callers use to reach a mobile services subscriber.
Mobile Switching Center	MSC. Provides origination and termination functions to calls from a mobile station user.
mobile transport subsystem	MTS. GSN application subsystem that implements all the protocols used by the GSN.
modeling	In NSM, process of creating a non-deployed device configuration.
modified deficit round robin	MDRR. Method for selecting queues to be serviced. *See also* queue.
Modular Interface Card	MIC. Network interface–specific card that can be installed on an MPC in the router.
Modular Port Concentrator	MPC. Interface concentrator on which modular interface cards (MICs) are mounted. An MPC is inserted into a slot in a Juniper Networks router. *See also* MIC.
module	In NSM, first-level element in the NSM navigation tree.
mOhm	Unit of mechanical mobility for sound waves. The reciprocal of the mechanical ohm unit of impedance.
MP-BGP	Multiprotocol Border Gateway Protocol. *Also called* Multicast Border Gateway Protocol. Extensions to BGP that enable it to carry routing information for multiple network layer protocols instead of only for IP, including the ability to carry multicast routing information.
MPC	Modular Port Concentrator. Interface concentrator on which modular interface cards (MICs) are mounted. An MPC is inserted into a slot in a Juniper Networks router. *See also* MIC.
MPLS	Multiprotocol Label Switching. Mechanism for engineering network traffic patterns that functions by assigning short labels to network packets that describe how to forward them through the network. *Also called* label switching. *See also* traffic engineering, TE.

MPLS edge node	MPLS node that connects an MPLS domain with a node outside the domain that either does not run MPLS or is in a different domain.
MPLS egress node	MPLS edge node that handles traffic as it leaves an MPLS domain.
MPLS EXP classifier	Class-of-service (CoS) behavior classifier for classifying packets based on the MPLS experimental bit. *See also* EXP bits.
MPLS FEC	Set of packets that are all forwarded in the same manner by a given LSR.
MPLS forwarding table	Maps MPLS labels to next hops. MPLS looks up the outermost label in a received packet in the forwarding table to determine what labels to push on the packet's label stack and where to send the packet.
MPLS ingress node	Edge node that handles traffic as it enters an MPLS domain.
MPLS node	Router running MPLS; it is aware of MPLS control protocols, operates one or more Layer 3 routing protocols, and is capable of forwarding packets based on labels. Optionally, an MPLS node can be capable of forwarding native Layer 3 packets.
MPLS traffic engineering	Ability to establish LSPs according to particular criteria (constraints) in order to meet specific traffic requirements rather than relying on the path chosen by the conventional IGP. The constraint-based IGP examines the available network resources and calculates the shortest path for a particular tunnel that has the resources required by that tunnel. Traffic engineering enables you to make the best use of your network resources by reducing overuse and underuse of certain links.
MPS	mobile point-to-point control subsystem. GSN application subsystem that controls all functionality associated with a particular connection.
mroute	Multicast traffic flow entry used for forwarding multicast traffic.
MRRU	maximum received reconstructed unit. Similar to the maximum transmission unit (MTU), but is specific to link services interfaces such as MLPPP. *See also* MTU.
MS	Mobile Station. Mobile device, such as a cellular phone or a mobile personal digital assistant (PDA).
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. 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).

MSIN	Mobile Subscriber Identification Number. A unique number to identify subscribers in a mobile network, used within the International Mobile Subcriber Identity (IMSI).
MSISDN	Mobile Station Integrated Services Digital Network Number. Number that callers use to reach a mobile services subscriber.
MST	multiple spanning-tree. A region or area within the Multiple Spanning Tree Protocol (MSTP). Spanning-tree protocols are used to prevent loops in bridge configurations. Unlike other types of STPs, MSTP can block ports selectively by VLAN. *See also* MSTP, RSTP.
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, common and internal spanning tree.
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. GSN application subsystem that implements all the protocols used by the GSN.
MTU	maximum transmission unit. Size in bytes of the largest protocol data unit that can be passed on in a link. The standard MTU for an Ethernet link is 1500.
multicast	Operation of sending network traffic from one network node to multiple network nodes.
multicast address	Type of IPv4 and IPv6 address used for sending packets to multiple destinations. Improves network efficiency by enabling a host to transmit a packet to a targeted group of receivers.
multicast backbone	MBone. 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.
Multicast Border Gateway Protocol	MBGP, P-BGP. *Also called* Multiprotocol Border Gateway Protocol. Extensions to BGP that permit the configuration of a multicast routing topology within and between BGP ASs. A BGP unicast routing protocol that allows different types of addresses (known as address families) to be distributed in parallel. This allows information about the topology of IP multicast-capable routers to be exchanged separately from the topology of normal unicast routers.
multicast distribution tree	MDT. Path between the sender (host) and the multicast group (receiver or listener).
Multicast Listener Discovery	MLD. Protocol that manages the membership of hosts and routers in multicast groups. An IPv6 protocol that hosts use to report their multicast group memberships to neighboring routers. Similarly, multicast routers, such as E Series routers, use MLD to discover which of their hosts belong to multicast groups.

Multicast Source Discovery Protocol	MSDP. 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).
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, *The Multi-Class Extension to Multi-Link PPP*.
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. *See also* BA classifier, classification.
multihoming	Network topology that uses multiple connections between customer and provider devices to provide redundancy.
Multilink Frame Relay	MLFR. 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.
Multilink Point-to-Point Protocol	MLPPP. 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, *The PPP Multilink Protocol (MP)*. *See also* PPP.
multimode fiber	MMF. 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. *See also* single-mode fiber.
multinetting	Method for adding more than one IP address to an IP interface—that is, a primary address and one or more secondary addresses.
multiple exit discriminator	MED. 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.
Multiple Spanning Tree Protocol	MSTP. 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.

multiple spanning-tree instance	MSTI. 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 bridges of that MST region. *See also* CIST, common and internal spanning tree.
multipoint connection	Single-source end system connected to multiple destination end systems. Multipoint indicates a nonbroadcast multiaccess (NBMA) interface.
Multiprotocol Border Gateway Protocol	MP-BGP. *Also called* Multicast Border Gateway Protocol. Extensions to BGP that enable it to carry routing information for multiple network layer protocols instead of only for IP, including the ability to carry multicast routing information.
Multiprotocol Label Switching	MPLS. Mechanism for engineering network traffic patterns that functions by assigning short labels to network packets that describe how to forward them through the network. *Also called* label switching. *See also* traffic engineering, TE.
multisource agreement	MSA. Specification of a fiber-optic transceiver module that conforms to the 10-Gigabit Ethernet standard. *See also* XENPAK module.
munged QoS profile	Set of rules used for a given forwarding interface. This set results from a process in which rules from all the QoS profiles are combined.

N

n-selector	Last byte of a nonclient peer address.
named path	Junos OS 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.
namespace	In Media Flow Controller, a defined collection of delivery policies for different categories of content or domains.
NAPT	Network Address Port Translation. 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. *See also* NAT.
NAS	network access server. Device that provides connections to a single user, to a network or subnetwork, and to interconnected networks. In reference to TACACS+, the NAS is the E Series router.
NAT	Network Address Translation. Method of concealing a set of host addresses on a private network behind a pool of public addresses. Using NAT allows conservation of registered IP addresses within private networks, simplifies IP address management through a form of transparent routing, and increases network privacy by hiding internal IP addresses from external networks. It can be used as a security measure to protect the host addresses from direct targeting in network attacks. *See also* bidirectional NAT, traditional NAT, twice NAT.

NAT object	Global object that contains references to device-specific NAT configurations, enabling multiple devices to share a single object. In NSM, use the Device Manager to configure NAT for each device, then create a global NAT object that includes the device-specific NAT configuration. Use global NAT objects in security policies and VPNs; when you update a device, that device automatically replaces the global NAT object with its device-specific NAT configuration.
NAT passthrough mode	NAT mode in which the router does not check UDP checksums. Used when a NAT device can change the IP address while the UDP header is encrypted, and then the UDP checksum cannot be recalculated. Using this mode for a single remote user does not compromise security, because IPsec protects UDP with an authentication algorithm far stronger than UDP checksums. However, NAT passthrough mode does not support secure access to the router by multiple remote users at locations such as hotels or airports where a NAT device resides between the router and the remote users. Additionally, this mode does not provide secure access for groups of remote users at corporate locations where a NAT device resides between the company's intranet and the public IP network. *See also* NAT-T.
NAT-T	Network Address Translation traversal. IETF standard that allows secure router access for multiple remote hosts behind a NAT device. *See also* NAT passthrough mode.
National Institute of Standards and Technology	NIST. Nonregulatory U.S. federal agency whose mission is to develop and promote measurement, standards, and technology.
NBMA	nonbroadcast multiaccess. Network that connects two or more devices but does not permit broadcast or multicast addressing. *See also* BMA.
NCP	Network Control Protocol. Traffic controller used to establish and configure different network layer protocols for the Point-to-Point Protocol (PPP).
NDP	Neighbor Discovery 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. *See also* ARP.
NEBS	Network Equipment Building System. Set of guidelines originated by Bell Laboratories in the 1970s to assist equipment manufacturers in designing products that were compatible with the telecom environment.
neighbor	Adjacent system reachable by traversing a single subnetwork; an immediately adjacent router. *Also called* a peer. *See also* adjacency.
Neighbor Discovery	Method for determining the link layer addresses of neighbors that reside on attached links and overriding invalid cache entries. Neighbor Discovery is not a true protocol, but routers and hosts (nodes) use Neighbor Discovery messages to determine the link-layer addresses of neighbors that reside on attached links and to overwrite invalid cache entries. Hosts also use it to find neighboring routers that can forward packets on their behalf, and to actively track the ability to reach neighbors.
neighboring routers	Routers that have interfaces to a common network.

nested profile assignment	Profile that references another profile that configures attributes for a dynamic upper-interface encapsulation type.
NET	network entity title. An ISO network address used by CLNS networks; an identifier of a network entity in an end system or intermediate system. A NET consists of an area address (routing domain), system identifier, and selector.
NetBIOS	network basic input/output system. 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.
netmask	32-bit mask that divides an IP address into subnets and specifies the available hosts in a network.
NetScreen Gatekeeper Protocol	NSGP. Juniper Networks proprietary peer-to-peer protocol that enables a security device to act as a server for voice-over-IP (VoIP) traffic.
NetScreen Redundancy Protocol	NRSP. Proprietary protocol that provides configuration, run time object (RTO) redundancy, and a device failover mechanism for security devices in a high availability (HA) cluster.
network access server	NAS. Device that provides connections to a single user, to a network or subnetwork, and to interconnected networks. In reference to TACACS+, the NAS is the E Series router.
Network Address Port Translation	NAPT. 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. *See also* NAT.
Network Address Translation	NAT. *Also called* Network Address Translator. Method of concealing a set of host addresses on a private network behind a pool of public addresses. Using NAT allows conservation of registered IP addresses within private networks, simplifies IP address management through a form of transparent routing, and increases network privacy by hiding internal IP addresses from external networks. It can be used as a security measure to protect the host addresses from direct targeting in network attacks. *See also* bidirectional NAT, traditional NAT, twice NAT.
Network Address Translation traversal	NAT-T. IETF standard that allows secure router access for multiple remote hosts behind a NAT device. *See also* NAT passthrough mode.
Network and Security Manager	NSM. Juniper Networks product for centralized management of security appliances designed to reduce the cost of managing security by minimizing repetitive tasks and delegating administrative responsibilities, among other features.
network basic input/output system	NetBIOS. 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 Control Protocol	NCP. Traffic controller used to establish and configure different network layer protocols for the Point-to-Point Protocol (PPP).
network element	In SNMP, a hardware device, such as a PC or a router. *Also known as* a managed device.
network entity title	NET. An ISO network address used by CLNS networks; an identifier of a network entity in an end system or intermediate system. A NET consists of an area address (routing domain), system identifier, and selector.
Network Equipment Building System	NEBS. Set of guidelines originated by Bell Laboratories in the 1970s to assist equipment manufacturers in designing products that were compatible with the telecom environment.
Network File System	A protocol that allows a user on a client computer to access files over a network similarly to how local storage is accessed by providing transparent remote access to shared files across networks. It is a standard defined in several RFCs, first appearing in RFC 1094, *NFS: Network File System Protocol Specification.*
network interface	Interface, such as an Ethernet or SONET/SDH interface, that primarily provides traffic connectivity. *See also* PIC, services interface.
network layer	Third level in the seven-layer OSI reference model for network protocol design and in the five-layer TCP/IP protocol stack. This layer performs the basic task of routing data across the network (getting packets of data from source to destination).
network layer reachability information	NLRI. Information carried in BGP packets and used by MBGP.
network link advertisement	OSPF link-state advertisement flooded throughout a single area by designated routers to describe all routers attached to the network.
network loopback	Ability to loop data toward the network before the data reaches the frame.
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 management station	NMS, network management system. System that enables a user to configure and monitor network elements.
network management system	NMS, network management station. System that enables a user to configure and monitor network elements.
network mask	*Also known as* subnet mask. Number of bits of the network address used to separate the network information from the host information in a Class A, Class B, or Class C IP address, allowing the creation of subnetworks. In binary notation, a series of 1s followed by a series of contiguous 0s. The 1s represent the network number; the 0s represent the host number. Use of masks can divide networks into subnetworks by extending the network portion of the address into the host portion. Subnetting increases the number of subnetworks and reduces the number of hosts.

network service access point	NSAP. Network connection identified with a hierarchical network address, specifying the point at which network services are made available to a transport layer entity in the OSI reference model. A valid NSAP address is unique and unambiguously identifies a single system. *Also called* ISO address.
network service access point identifier	NSAPI. Unique NSAP identifier that unambiguously identifies a single system.
network summary LSA	OSPF link-state advertisement sent by an ABR to advertise internal OSPF routing knowledge across an area boundary. *See also* ABR.
Network Time Protocol	NTP. Used to synchronize the system clocks of hosts on the Internet to Universal Coordinated Time (UTC). A router can update its clock automatically by configuring it as a Network Time Protocol (NTP) client. Using NTP enables the system to record accurate times of events. You can view the log file of events to monitor the status of the network.
network-to-network interface	NNI. Makes connections possible between users connected to different Frame Relay networks. These separate Frame Relay networks can be considered as subnetworks within a complete network service.
network.conf	Default configuration file for autoinstallation, in which you specify IP addresses and associated hostnames for devices on the network.
NFS	Network File System. A protocol that allows a user on a client computer to access files over a network similarly to how local storage is accessed by providing transparent remote access to shared files across networks. It is a standard defined in several RFCs, first appearing in RFC 1094, *NFS: Network File System Protocol Specification.*
NIC	Network Information Center. Internet authority responsible for assigning Internet-related numbers, such as IP addresses and autonomous system (AS) numbers. *See also* IANA.
NIST	National Institute of Standards and Technology. 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.
NMS	network management system; network management station. System that enables a user to configure and monitor network elements.
NNI	network-to-network interface. Makes connections possible between users connected to different Frame Relay networks. These separate Frame Relay networks can be considered as subnetworks within a complete network service.
non-PPP equal access	Method of allowing remote access in which the router provides IP addresses to subscribers' computers through the Dynamic Host Configuration Protocol (DHCP). This method is particularly convenient for broadband (cable and DSL) environments or environments that use bridged Ethernet over ATM, because network operators can support one central system rather than an individual PPPoE client on each subscriber's computer.

nonbroadcast multiaccess	NBMA. Network that connects two or more devices but does not permit broadcast or multicast addressing. *See also* BMA.
nonbroadcast network	Network that has no broadcast capability but supports more than two routers.
nonce	Random value used to detect and protect against replay attacks (IPsec).
nonclient peer	In a BGP route reflection, a BGP peer that is not a member of a cluster. *See also* client peer.
nonstop forwarding	nonstop forwarding. *Also called* 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. Implementation varies by protocol. *See also* cold restart, warm restart.
nonstop routing	NSR. 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.
nonvolatile storage	NVS. Memory that retains stored information even when power is lost to the device.
not-so-stubby area	NSSA. In OSPF, a type of stub area in which external routes can be flooded.
notification	In SNMP, a message that indicates a status change (equivalent to a trap).
notification cell	Junos OS 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.
NRSP	NetScreen Redundancy Protocol. Proprietary protocol that provides configuration, run time object (RTO) redundancy, and a device failover mechanism for security devices in a high availability (HA) cluster.
NSAP	network service access point. Network connection identified with a hierarchical network address, specifying the point at which network services are made available to a transport layer entity in the OSI reference model. A valid NSAP address is unique and unambiguously identifies a single system. *Also called* ISO address.
NSAPI	network service access point identifier. Unique NSAP identifier that unambiguously identifies a single system.
nsd	Network security process that interprets, executes, and manages the configuration of extended interface attributes, policies, zones, address books, firewall screens, NAT, and other network security treatments.

NSF
nonstop forwarding. *Also called* 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. Implementation varies by protocol. *See also* cold restart, warm restart.

NSGP
NetScreen Gatekeeper Protocol. Juniper Networks proprietary peer-to-peer protocol that enables a security device to act as a server for voice-over-IP (VoIP) traffic.

NSM
Network and Security Manager. Juniper Networks product for centralized management of security appliances designed to reduce the cost of managing security by minimizing repetitive tasks and delegating administrative responsibilities, among other features.

NSR
nonstop routing. 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. Used to synchronize the system clocks of hosts on the Internet to Universal Coordinated Time (UTC). A router can update its clock automatically by configuring it as a Network Time Protocol (NTP) client. Using NTP enables the system to record accurate times of events. You can view the log file of events to monitor the status of the network.

null interface
Method on a router for handling undesired traffic. The null interface is always up, cannot be deleted, and cannot forward or receive traffic. It acts as a data sink; you can avoid the overhead involved with using access lists by directing undesired network traffic to the null interface.

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. *See also* 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.

NVS
nonvolatile storage. Memory that retains stored information even when power is lost to the device.

NVS card
Nonvolatile storage memory card on an SRP module that stores system software, configuration files, and core dumps.

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. *See also* ISAKMP.

OAM	Operation, Administration, and Maintenance. ATM Forum specification for monitoring ATM virtual connections, verifying that the connection is up and that the router is operational. 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). *See also* CFM, LFM.
object	Represents reusable information, such as network addresses, individual users and user groups, and commonly used configuration data. In NSM, objects are shared objects, meaning they are shared between the global domain and all subdomains. Objects are the building blocks of the NSM management system.
Object Manager	Module of the NSM user interface that lets you create and manage the objects used in your NSM system.
objects table (mteObjectsTable)	SNMP term for a table that defines objects to add to event messages. You can create a list of user-specified objects and bind them to a trigger event. This can provide a snapshot of other values on a router when the trigger occurs. You can bind objects to a specific trigger, a type of test (for example, existence or Boolean tests), or a type of event (for example, rising or falling events). One of the three parts of the Event MIB. *See also* event table (mteEventTable), trigger table (mteTriggerTable).
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.
ODBC	Open Database Connectivity. Standard or open application programming interface (API) for accessing a database.
OIF	outgoing interface. Used by multicast functions within a router to determine which egress ports to use for forwarding multicast groups.
OIR	online insertion and removal. Ability to install or remove certain modules (SRE, NIC, and so on) on the SRX mid-range services gateway without having to power off the device. Each OIR-capable model will have an OFFLINE button that is pressed to take the module offline for removal.
one-rate rate-limit profile	Profile in which, when the committed rate is exceeded, the rate limiter drops a single packet and then resumes transmission up to a configurable burst window. *See also* rate-limit profile, two-rate rate-limit profile.

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 Junos XML protocol remote procedure calls (RPCs).
opaque LSAs	LSAs that provide a generalized way of extending OSPF. The router generates opaque LSAs to carry traffic engineering information, accepts them from other routers, and floods them accordingly. OSPF uses the traffic engineering information to build a database from which paths can be computed for MPLS label-switched paths.
Open Database Connectivity	ODBC. Standard or open application programming interface (API) for accessing a database.
Open message	BGP message that allows two neighbors to negotiate the parameters of the peering session.
Open Shortest Path First	OSPF. Dynamic routing protocol intended to operate within a single Autonomous System. It advertises the states of local network links within the AS and makes routing decisions based on the shortest-path-first (SPF) algorithm (also referred to as the Dijkstra algorithm). OSPF is a link-state routing protocol, similar to the Intermediate System-to-Intermediate System (IS-IS) routing protocol. OSPF was designed expressly for the TCP/IP Internet environment, including explicit support for classless interdomain routing (CIDR) and the tagging of externally derived routing information. *See also* AS.
Open Systems Interconnection	OSI. Standard reference model for how messages are transmitted between two points on a network.
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	op script. Extensible Stylesheet Language for Transformations (XSLT) script written to automate network troubleshooting and network management. Op scripts can perform any function available through Junos XML protocol remote procedure calls (RPCs).
Operation, Administration, and Maintenance	OAM. ATM Forum specification for monitoring ATM virtual connections, verifying that the connection is up and that the router is operational. 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). *See also* CFM, LFM.
operational mode	Junos OS mode that allows a user to view statistics and information about the router's current operating status.
operational virtual router	For a secure IP tunnel, the VR in which a secure IP tunnel exists. *See also* transport virtual router.
optical carrier	*See* OC.optical carrier. In SONET, the OC level indicates the transmission rate of digital signals on optical fiber.

ordered control MPLS label distribution method whereby an LSR does not advertise a label for a FEC unless it is the egress LSR for the FEC, or until it has received a label for the FEC from its downstream peer. In this manner, the entire LSP is established before MPLS begins to map data onto the LSP, preventing inappropriate (early) data mapping from occurring on the first LSR in the path. JunosE Software does not support ordered control when LDP or BGP is the signaling protocol. *See also* downstream-on-demand, independent control.

ORF outbound route filter, outbound route filtering. BGP capability that enables a BGP speaker to send its inbound route filter to a peer, which then installs that filter to apply after its own outbound route filter. The BGP peer then sends to the BGP speaker only routes desired by that speaker, thus minimizing the number of unwanted routing updates sent.

origin In BGP, attribute that describes the source of the route.

orlonger Junos OS 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. Dynamic routing protocol intended to operate within a single Autonomous System. It advertises the states of local network links within the AS and makes routing decisions based on the shortest-path-first (SPF) algorithm (also referred to as the Dijkstra algorithm). OSPF is a link-state routing protocol, similar to the Intermediate System-to-Intermediate System (IS-IS) routing protocol. OSPF was designed expressly for the TCP/IP Internet environment, including explicit support for classless interdomain routing (CIDR) and the tagging of externally derived routing information. *See also* AS.

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.

OTASP Over-the-Air Service Provisioning. Activation method used by cellular network providers such as Verizon for CDMA EV-DO 3G wireless modem cards. *See also* IOTA, Internet-based Over-the-Air.

outbound route filter (filtering) ORF. BGP capability that enables a BGP speaker to send its inbound route filter to a peer, which then installs that filter to apply after its own outbound route filter. The BGP peer then sends to the BGP speaker only routes desired by that speaker, thus minimizing the number of unwanted routing updates sent.

outbound traffic (IPsec) In the context of a secure interface, the clear traffic forwarded to the interface (either by policy or by routing) that is typically secured according to security parameters set for that interface.

outgoing interface OIF. Used by multicast functions within a router to determine which egress ports to use for forwarding multicast groups.

output policy	Policy that is applied to packets before they leave an interface. *See also* input policy, policy, secondary input policy.
outside global address	In a NAT context, a configured, publicly routable IP address assigned to a host on the outside network.
outside local address	In a NAT context, a translated IP address of an outside host as it appears to the inside network.
outside network	In a NAT context, the public portion of a network that uses legitimate, publicly routable IP addresses to which you want private hosts to connect.
outside source information	Information used in NAT configuration only when addresses of external hosts might create a conflict on a private network. When an outside host sends a packet inbound to the inside network, the NAT router translates the source information and, in the outbound direction, restores the original information. For inbound traffic, the NAT router translates the outside global address into the outside local address.
Over-the-Air Service Provisioning	OTASP. Activation method used by cellular network providers such as Verizon for CDMA EV-DO 3G wireless modem cards. *See also* IOTA, Internet-based Over-the-Air.
overlapping VPN	When a site is a member of more than one VPN; often used to provide centralized services. The central site might contain DNS servers or WWW servers or management stations that need to be reachable from multiple VPNs. Overlapping IPv4 and IPv6 VPNs are supported by the same route-target mechanism. *See also* full-mesh VPN, hub-and-spoke VPN.
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. *See also* bandwidth oversubscription.

P

P router	provider core router. Router within a service provider core that connects directly to PE routers or other P routers and does not connect directly to a customer edge (CE) device. *See also* PE router.
P2MP LSP	point-to-multipoint LSP. RSVP-signaled LSP with a single source and multiple destinations.
package	Collection of files that make up a Junos OS component.
packet	Fundamental unit of information (message or fragment of a message) carried in a packet-switched network, for example, the Internet. *See also* 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
- 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. *See also* traffic sampling.

- 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 packets in the J-Web interface as they are captured, or save them to a file and analyze them offline with packet analyzers such as Ethereal. J-Web packet capture does not capture transient traffic.

- A logging option in the IDP Series. You can enable packet capture for traffic that matches your security policy rule.

packet classification
Also called classification. Process of taking in a single data stream and sorting it into multiple output substreams. 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. *See also* BA classifier, multifield classifier.

packet data protocol
PDP. Network protocol, such as IP, used by packet data networks connected to a GPRS network.

packet detection
For GRE tunnel interfaces, event when the router receives a packet with a source IP address that is not in the demultiplexer table, which triggers dynamic creation of subscriber interfaces. In this case, the primary IP interface must be in autoconfiguration mode. Packet detection is the only method of dynamically creating subscriber interfaces on GRE tunnel interfaces; you cannot use a DHCP local server or DHCP external server.

packet filtering
A router/firewall process that uses access control lists (ACL) to restrict flow of information based on characteristics such as source/destination IP address, protocol, or port used. Generally, packet-filtering routers do not track sessions except when doing NAT (which tracks the session for NAT purposes).

Packet Forwarding Engine
Portion of the router that processes packets by forwarding them between input and output interfaces.

packet loss priority
PLP. 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.

packet loss priority bit
PLP 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.

packet mirroring
JunosE Software feature that enables sending a copy of a packet to an external host for analysis. Packet mirroring has many uses, including traffic debugging and troubleshooting user networking problems. With it you can mirror traffic traversing a specific interface or traffic that is to or from a particular user. Packet mirroring is always transparent to users and does not affect the delivery of the original traffic. In some cases, the means and authority for conducting packet mirroring can depend on the regulations of specific countries. *See also* CLI-based packet mirroring, RADIUS-based packet mirroring.

packet or cell switching	Transmission of packets from many sources over a switched network.
packet over SONET	POS. Communications protocol for transmitting packets over SDH or SONET, which are both circuit switched protocols.
packet over SONET/SDH	Serial transmission of data over SONET frames through the use of a protocol such as PPP.
Packet Transfer Mode	PTM. Method of transporting packet-based services based on the EFM IEEE 802.3ah standard.
packet-switched network, packet-switching network	PSN. Uses the addressing information in packets to switch packets from one physical network to another, moving each packet toward its final destination.
PADI	PPPoE Active Discovery Initiation packet. Point-to-Point Protocol over Ethernet (PPPoE) initiation packet that is broadcast by the client to start the discovery process.
PADM	PPPoE Active Discovery Message. Control message that servers send to clients.
PADN	PPPoE Active Discovery Network. Message that a PPPoE server sends to a client. The information sent associates the PPPoE sessions with a set of routes. The client can use this set of routes to determine which session to use based on the destination IP address.
PADO	PPPoE Active Discovery Offer packet. 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. 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. Point-to-Point Protocol over Ethernet (PPPoE) packet sent by the selected access concentrator to confirm the session.
PADT	PPPoE Active Discovery Termination packet. Point-to-Point Protocol over Ethernet (PPPoE) packet sent by either the client or the access concentrator to terminate a session.
PAP	Password Authentication Protocol. Security protocol that uses password protection to authenticate a user to a network or host. *See also* CHAP, Challenge Handshake Authentication Protocol.
partial sequence number PDU (protocol data unit)	PSNP. Packet that contains only a partial list of the LSPs in the IS-IS link-state database; a PDU sent by designated router to acknowledge and request link-state information..
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.
passive interface	Interface that only advertises its IP address in its LSPs. It does not send or receive IS-IS packets.

passive peers	BGP peers from which a BGP speaker accepts inbound BGP connections but never initiates an outbound BGP connection to the peers. This passive status conserves CPU and TCP connection resources when the neighbor does not exist.
Password Authentication Protocol	PAP. Security protocol that uses password protection to authenticate a user to a network or host. *See also* CHAP, Challenge Handshake Authentication Protocol.
PAT	Port Address Translation. Translation of the original source port number in a packet to a different, randomly designated port number.
path attribute	Information about a BGP route, such as the route origin, AS path, and next-hop router.
path layer	For a channelized OCx/STMx interface, the layer that maps the user payload into a SONET/SDH format suitable for the line layer. This layer transports the actual network services (such as T3s) between SONET/SDH multiplexing devices and provides end-to-end transmission. *See also* line layer, section layer.
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, PBBN, provider backbone bridge network. 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, 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.
PBX	private branch exchange. Telephone system that enables telephone extensions within the system to connect with each other as well as with the public telephone system.
PC Card	*Previously known as* a PCMCIA Card. Removable storage media that ships with each router and contains a copy of the Junos OS. The PC Card is based on standards published by the Personal Computer Memory Card International Association (PCMCIA).
pcap	Software library for packet capturing. *See also* 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 devices, 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.

PCR — peak cell rate. Maximum allowable rate, measured in cells per second, at which cells can be transported along a connection in an ATM network.

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).

PDL — progressive download. An HTTP media delivery mode in which the media file is played while it is being downloaded, unlike the full download method whereby the media file is downloaded completely before playback can begin.

PDP —
- packet data protocol. Network protocol, such as IP, used by packet data networks connected to a GPRS network.
- policy decision point. The COPS server, which makes policy decisions for itself and for clients that request decisions. The SRC (formerly called SDX) application is the PDP.

PDP context — In the mobile wireless network, indicates a logical association between an MS (Mobile Station) and PDN (Public Data Network) running across a GPRS network; a user session on a GPRS network. The context defines aspects such as Routing, QoS (Quality of Service), Security, Billing, and so on.

PDU — protocol data unit. OSI term equivalent to packet, containing protocol control information and, possibly, user data. Also refers to a specific layer of the OSI seven-layer model and a specific protocol.

PE — PE router. Router in the service provider's network that is connected to a customer edge (CE) device and participates in a virtual private network (VPN). *See also* P router.

PE router — provider edge router. Router in the service provider's network that is connected to a customer edge (CE) device and participates in a virtual private network (VPN). *See also* P router.

peak cell rate — PCR. Maximum allowable rate, measured in cells per second, at which cells can be transported along a connection in an ATM network.

peak information rate — PIR. 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. *See also* CIR, trTCM.

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. *See* BGP peer, neighbor.
peering	Practice of exchanging Internet traffic with directly connected peers according to commercial and contractual agreements.
PEM	• Privacy Enhanced Mail. 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.
pending state	State of an SRP module to which the system transitions when an unsupported application is configured. When a transition to the pending state occurs, the system generates SNMP traps and log messages. How the router behaves depends on which high availability state the application is in when it shifts to a pending state.
penultimate hop popping	PHP. 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. *See also* UHP.
penultimate router	Last transit router before the egress router in an MPLS label-switched path.
PEP	policy enforcement point. COPS client that enforces policy decisions. The JunosE Software COPS interface is a PEP.
per-hop behavior	PHB. Traffic conditioning applied to traffic at each node in a differentiated services domain. The PHB provides the scheduling behavior and drop probability required by the traffic.
Perfect Forward Secrecy	PFS. 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. PFS provides added security, but requires extra processing for a new key exchange on every key refresh.
Peripheral Component Interconnect	PCI. Standard, high-speed bus for connecting computer peripherals. Used on the Routing Engine.
Peripheral Component Interconnect Express	PCI 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 devices, PCI Express slots are backward compatible with PCI and can accept Physical Interface Modules (PIMs) intended for either PCI Express or PCI slots.

permanent interface	Interface that is always present in the routing platform. *See also* management Ethernet interface, transient interface.
permanent virtual channel (or circuit or connection)	PVC. *Also called* permanent virtual connection when referring to ATM. Software-defined logical connection in a network; a virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and teardown in situations where certain virtual circuits must exist all the time. *See also* SVC, switched virtual connection (or circuit).
persistent change	Configuration change generated by a commit script and copied to the candidate configuration, often a result of using a template. Persistent changes remain in the candidate configuration unless you explicitly delete them. *See also* transient change.
persistent tunnel	Tunnel that is configured to remain available. Persistent tunnels have only local significance; that is, they apply only to the end of the tunnel where they are set. If the other end of the tunnel chooses to terminate the tunnel, the tunnel is removed.
Personal Computer Memory Card International Association	PCMCIA. Industry group that promotes standards for credit card-size memory and I/O devices.
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, *The Point-to-Point Protocol (PPP)*. PFC allows you to conserve bandwidth by transmitting less data. *See also* ACFC.
PFS	Perfect Forward Secrecy. 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. PFS provides added security, but requires extra processing for a new key exchange on every key refresh.
PGM	Pragmatic General Multicast. 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. Strong cryptographic technique invented by Philip Zimmerman in 1991.
PHB	per-hop behavior. Traffic conditioning applied to traffic at each node in a differentiated services domain. The PHB provides the scheduling behavior and drop probability required by the traffic.
PHP	penultimate hop popping. 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. *See also* UHP.

PHY	PHY can be either of the following:
	• 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. *See also* LAN PHY and WAN PHY.
	• Open Systems Interconnection (OSI) physical layer. Layer 1 of the OSI model that defines the physical link between devices.
physical interface	A port on a Physical Interface Card (PIC) or Physical Interface Module (PIM).
Physical Interface Card	PIC. Network interface–specific card that can be installed on an FPC in the router.
Physical Interface Module	PIM. Network interface card installed in a device 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.
physical layer	First and lowest level in the seven-layer OSI reference model for network protocol design and in the five-layer TCP/IP protocol stack. This layer defines all the electrical and physical specifications for devices and provides the transmission of bits over the network medium. It includes the physical media: cables, microwaves, and networking equipment such as hubs and repeaters.
Physical Layer Convergence Procedure	PLCP. A protocol defined by IEEE 802.6 that is used for DS3 transmission of ATM. ATM cells are encapsulated in a frame defined by the PLCP, which is defined by the DS3 M-frame.
physical server	The server machine itself, which can run multiple server applications. *See also* real server.
PIB	Policy Information Base. Collection of sets of attributes that represent configuration information for a device.
PIC	Physical Interface Card. 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	PIM can be either of the following:

- Protocol Independent Multicast. 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).

- Physical Interface Module. Network interface card installed in a device 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.

PIM dense mode	Protocol Independent Multicast dense mode. Uses a reverse-path multicast, flood-and-prune mechanism. *See also* dense mode.
PIM sparse mode	Protocol Independent Multicast sparse mode. A sparse mode multicast protocol, which uses shared trees. In a shared tree, sources forward multicast datagrams to a directly connected router, the designated router. The designated router encapsulates the datagram and unicasts it to an assigned rendezvous point router, which then forwards the datagram to members of multicast groups. *See also* sparse mode.
PIM sparse mode remote neighbors	Neighbors that are used to run multicast services over BGP/MPLS virtual private networks.
PIM sparse-dense mode	Protocol Independent Multicast sparse-dense mode. Used to send data when a rendezvous point (RP) is not known for a group. However, if the router discovers an RP or you configure an RP statically, PIM sparse mode takes over.
PIM SSM	Protocol Independent Multicast source-specific multicast. Extension of the PIM protocol where a client can receive multicast traffic directly from the source. PIM SSM uses PIM sparse mode functionality to create a shortest-path tree (SPT) between the client and the source, but builds the SPT without using a rendezvous point.
ping of death	Intentionally oversized or irregular ICMP packet that can trigger a denial-of-service condition, freezing, or other adverse system reactions.
pipe (and short-pipe) model	Tunneling model whereby any traffic conditioning (in a pure JunosE environment, a change in traffic class/color combination) that is applied when traffic goes through the tunnel has no effect on the EXP bits coding in the inner header. That is, when traffic exits an LSP (when a label is popped) or when traffic enters an LSP, the inner header's EXP bits coding is not changed. The pipe and short-pipe models differ in the header that the tunnel egress uses when it determines the PHB of an incoming packet. With the short-pipe model, the tunnel egress uses an inner header used for forwarding. With the pipe model, the outermost label is always used. Because of this, you cannot use PHP with the pipe model. *See also* uniform model.

PIR	peak information rate. The PIR must be equal to or greater than the CIR (committed information rate), and both must be configured to be greater than 0. Packets that exceed the PIR are marked red, which corresponds to high loss priority. *See also* CIR, trTCM.
PKCS	Public-Key Cryptography Standards. Series of standards established by RSA Laboratories.
PKCS10	PKCS #10. Digital format of messages sent to request certification of a public key.
PKI	public key infrastructure. 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.
plaintext	Unencrypted form of encrypted text. *Also known as* cleartext.
platform label space	Large, single, unconfigurable pool of labels that can be shared by the platform—all MPLS interfaces on a given virtual router. *See also* interface label space.
player	Any media player software used for playing back digital video data from files of appropriate formats such as MPEG, AVI, RealVideo, Flash, QuickTime, and so on. In addition to VCR-like functions such as playing, pausing, stopping, rewinding, and forwarding, some common functions include zooming/full screen, audio channel selection, subtitle selection, and frame capturing.
PLCP	Physical Layer Convergence Procedure. A protocol defined by IEEE 802.6 that is used for DS3 transmission of ATM. ATM cells are encapsulated in a frame defined by the PLCP, which is defined by the DS3 M-frame.
Plesiochronous Digital Hierarchy	PDH. 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).
PLMN	Public Land Mobile Network. 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. Ingress router of a backup tunnel or a detour LSP.
PoE	Power over Ethernet. PoE supports the implementation of the IEEE 802.3af and IEEE 802.3at standards; this implementation allows both data and electrical power to pass over a copper Ethernet LAN cable.

point of local repair	PLR.. Ingress router of a backup tunnel or a detour LSP.
point of presence	POP. Physical access point to the Internet. The location of the servers, routers, and ATM switches used to provide access to the Internet. The demarcation point between two networks (for example, between a LAN and a WAN).
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. *See also* point-to-point connection.
point-to-multipoint LSP	P2MP LSP. RSVP-signaled LSP with a single source and multiple destinations. .
point-to-multipoint network	Nonbroadcast network where OSPF treats connections between routers as point-to-point links. There is no election of a designated router and no LSA generated for the network. A router in a point-to-multipoint network sends Hello packets to all neighbors with which it can directly communicate.
point-to-point circuits	In IS-IS, circuits that have less overhead than broadcast circuits, because they do not use designated routers, the link-state database has no representation of the pseudonode or network LSA, and they do not require periodic database synchronization. However, if more than two routers are connected on the LAN media, routing information in the network is reduced. *See also* broadcast circuits.
point-to-point connection	Unidirectional or bidirectional connection between two end systems. Point-to-point is one of two fundamental connection types. *See also* point-to-multipoint connection.
point-to-point network	Joins two routers over a Wide Area Network (WAN), for example, two security devices connected by an IPsec VPN tunnel. On point-to-point networks, the OSPF router dynamically detects neighbor routers by sending Hello packets to the multicast address 224.0.0.5.
Point-to-Point Protocol	PPP. 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, *The Point-to-Point Protocol (PPP)*.
Point-to-Point Protocol over Ethernet	Allows multiple users at a site to share the same digital subscriber line, cable modem, or wireless connection to the Internet. You can configure PPPoE client instances, including the username and password, on any or all interfaces on some security devices. *See also* PPPoE.
Point-to-Point Protocol process	pppd. Point-to-Point Protocol process (daemon) that processes packets that use PPP.
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	PEC. In traffic policing, a set of packets that are treated the same way by the packet classifier.
policy	Condition and action attached to an interface that cause the router to handle packets passing through the interface in a certain way. *See also* input policy, output policy, secondary input policy.
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.
policy decision point	PDP, policy decision point. The COPS server, which makes policy decisions for itself and for clients that request decisions. The SRC (formerly called SDX) application is the PDP.
policy enforcement point	PEP. A COPS client that enforces policy decisions. The JunosE Software COPS interface is a PEP.
Policy Information Base	PIB. Collection of sets of attributes that represent configuration information for a device.
policy list	In policy management, a set of rules, each of which specifies a policy action.
policy management	Feature that allows network service providers to implement packet forwarding and routing specifically tailored to their customer's requirements. Using policy management, customers can implement policies that selectively cause packets to take different paths.
policy routing	Routing method that redefines a classified packet flow to a destination port or IP address.
policy rule	Policy action optionally combined with a classification. A set of policy rules defines what specialized treatment to apply to classified traffic flows.
pop	Removal of the last label, by a router, from a packet as it exits an MPLS domain.
POP	point of presence. Physical access point to the Internet. The location of the servers, routers, and ATM switches used to provide access to the Internet. The demarcation point between two networks (for example, between a LAN and a WAN).
Port Address Translation	PAT. Translation of the original source port number in a packet to a different, randomly designated port number.
port mapping	Translation of the original destination port number in a packet to a different, predetermined port number.
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.
port mode	Feature on some security devices that allows you to select one of several different sets of port, interface, and zone bindings on the device. Changing the port mode removes any existing configurations on the device and requires a system reset.

port scan	Attack in which a single source address attempts to connect to every port on a single machine, in an attempt to provide attackers with information about your network configuration.
port shaping	Method for shaping the aggregate traffic through a port or channel to a rate that is less than the line or port rate.
POS	packet over SONET. Communications protocol for transmitting packets over SDH or SONET, which are both circuit switched protocols.
Power Entry Module	Distributes DC power within the router chassis. Supported on M40e, M160, M320, and T Series routing platforms.
Power over Ethernet	PoE. PoE supports the implementation of the IEEE 802.3af and IEEE 802.3at standards; this implementation allows both data and electrical power to pass over a copper Ethernet LAN cable.
PPP	Point-to-Point Protocol. 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	PADI. Point-to-Point Protocol over Ethernet (PPPoE) initiation packet that is broadcast by the client to start the discovery process.
PPPoE Active Discovery Message	PADM. Control message that servers send to clients.
PPPoE Active Discovery Network	PADN. Message that a PPPoE server sends to a client. The information sent associates the PPPoE sessions with a set of routes. The client can use this set of routes to determine which session to use based on the destination IP address.
PPPoE Active Discovery Offer packet	PADO. 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.
PPPoE Active Discovery Request packet	PADR. Point-to-Point Protocol over Ethernet (PPPoE) packet sent by the client to one selected access concentrator to request a session.
PPPoE Active Discovery Session Confirmation packet	PADS. Point-to-Point Protocol over Ethernet (PPPoE) packet sent by the selected access concentrator to confirm the session.

PPPoE Active Discovery Termination packet	PADT. Point-to-Point Protocol over Ethernet (PPPoE) packet sent by either the client or the access concentrator to terminate a session.
PPPoE over ATM	*Also called* PPPoA. Network protocol that encapsulates Point-to-Point Protocol over Ethernet (PPPoE) frames in Asynchronous Transfer Mode (ATM) for digital subscriber line (DSL) transmission, and connects multiple hosts over a simple bridging access device to a remote access concentrator.
PPPoE service name table	Collection of service name tags, as defined in RFC 2516, *A Method for Transmitting PPP Over Ethernet (PPPoE)*, for an access concentrator (AC) such as an E Series router. PPPoE clients use service name tags to request that an AC support certain services. Configuring PPPoE service name tables enables the AC to support multiple service name tags in addition to the empty service name tag. *See also* service name tag.
Pragmatic General Multicast	PGM. 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.
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.
precedence level	Order in which the effectiveness of CLI privilege levels of E Series routers is implemented. The CLI uses the following order of precedence:

1. Privilege level set for all commands within a mode, including modes that are accessed from another mode; for example, Global Configuration mode. *See also* switch.

2. Privilege level set for all commands that begin with the same keyword; for example, **snmp** commands.

3. Privilege level set for individual commands; for example, **snmp-server** community.

preference	Value associated with a route that the virtual router uses to select the active route when there are multiple routes to the same destination network. The preference value is determined by the protocol or origin of the route. The lower the preference value of a route, the more likely the route is to be selected as the active route.
preferred address	On an interface, the default local address used for packets sourced by the local router to destinations on the subnet.
preferred roaming list	PRL. File that contains information for accessing a device's home network, as well as the service provider's roaming partners.
prefix	First part of a BGP route, which describes a set of IP addresses that can be reached using the route. Prefixes are made possible by classless interdomain routing (CIDR).

prefix list	Sequential collection of permit and deny conditions that apply to IP or IPv6 addresses. Like an access list, the router tests addresses one by one against the conditions in a prefix list. Unlike an access list, the prefix list specifies a base IP or IPv6 address and a length. The tested address is matched against the prefix.
prefix tree	Nonsequential collection of permit and deny conditions that apply to IP addresses. Like a prefix list, the prefix tree specifies a base IP address and a length (the number of bits applied to the base) to determine the network prefix. The tested address is matched against the prefix. The prefix tree also enables route summarization. However, the prefix tree does not match addresses one by one in sequence against the listed conditions. The router performs a binary search against the tree structure of the entries. The prefix tree provides a faster search methodology and matches the test address more closely than either the access list or the prefix list.
prefix-length-range	Junos OS 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.
prepended header	Header created by the policy-mirroring action during packet mirroring, and used for demultiplexing at the analyzer to sort through the multiple mirrored streams that arrive from different sources. During a packet mirroring session, the router prepends a special UDP/IP header to each mirrored packet that is sent to the analyzer port.
presentation layer	Sixth level in the seven-layer OSI reference model for network protocol design. This layer transforms data to provide a standard interface for the application layer.
prestage	Data placed on a Media Flow Controller or origin server before an HTTP request comes in for it.
Pretty Good Privacy	PGP. Strong cryptographic technique invented by Philip Zimmerman in 1991.
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 OS 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.
primary IP address	IP address configured as primary from the set of real interface addresses. VRRP advertisements are always sent (by the master router) using the primary IP address as the source of the IP packet.
primary IP interface	Normal IP interface on a supported layer 2 interface, such as Ethernet. You create a primary interface by assigning an IP address to the Ethernet interface.

priority	Combination of the facility and severity level of a system log message. By default, priority information is not included in system log messages, but you can configure Junos OS to include it.
Privacy Enhanced Mail	PEM. Technique for securely exchanging electronic mail over a public medium.
private branch exchange	PBX. Telephone system that enables telephone extensions within the system to connect with each other as well as with the public telephone system.
private community	Convenient way to categorize groups of routes to facilitate the use of routing policies. *Also called* local-use community or general community.
private line aggregation	Consolidation of multiple high-speed access lines into one access point.
Privileged Exec mode	User Exec mode that provides privileged-level access. Privileged Exec commands allow you to perform such functions as displaying system information, setting operating parameters, and gaining access to Global Configuration mode. *See also* User Exec mode.
privileged level	Access level in the CLI of E Series routers that enables you to view router configuration, change a configuration, and run debugging commands. You need a password to access this level. This level gives you full CLI privileges. The CLI has the ability to map any command to one of 16 levels of command privilege (in the range 0–15). When you access Privileged Exec mode, you have access to those commands that map to your access level or below.
PRL	preferred roaming list. File that contains information for accessing a device's home network, as well as the service provider's roaming partners.
probe	An action taken or an object used to learn something about the state of the network. Real-time performance monitoring (RPM) uses several types of requests to probe a network.
probe interval	Time, in seconds, between probe packets.
process ID	Unique identifier for a process, displayed in a system log message along with the name of the process that generated the event.
process status	Display on a security device that shows information about processes on that device.
profile	Set of characteristics that act as a pattern. Defined through CLI commands to configure dynamic interfaces.
programmable read-only memory	PROM. Form of digital memory in which each bit is locked by using a fuse or antifuse action to store information permanently.

progress indicator	Animated representation of how much progress has been made on a CLI operation that does not finish within the expected completion time. This type of status indicator is supported for the file system synchronization application and the file copy application. The progress indicator displays a series of dots that represents the time required to complete the operation. The dots are followed by the actual percentage of the total that has been completed and by an oscillating asterisk that indicates ongoing activity. As the application progresses, the dots are replaced with asterisks, starting at the left, to represent how much of the operation is finished.
progressive download	PDL. An HTTP media delivery mode in which the media file is played while it is being downloaded, unlike the full download method whereby the media file is downloaded completely before playback can begin.
PROM	programmable read-only memory. Form of digital memory in which each bit is locked by using a fuse or antifuse action to store information permanently.
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.
promiscuous peer group	BGP peer group that accepts incoming BGP connections from any remote address that matches an access list. Promiscuous peers are useful when the remote address of the peer is not known ahead of time. An example is in B-RAS applications, in which interfaces for subscribers are created dynamically and the remote address of the subscriber is assigned dynamically from a local pool or by using RADIUS or some other method.
protect interface	Provides the redundant connection on modules that have APS/MSP or that otherwise enable port redundancy.
Protected System Domain	PSD. 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	Rules determining the format and transmission of data between end points in a telecommunication connection.
protocol address	Logical Layer 3 address assigned to an interface within the Junos OS.
protocol anomaly	Deviation from the RFC specifications that dictate how communications between two entities should be implemented. Most legitimate traffic does not deviate from the protocols; when anomalies are detected they are often a sign of malicious traffic and seen as a threat to the system.
protocol data unit	PDU. OSI term equivalent to packet, containing protocol control information and, possibly, user data. Also refers to a specific layer of the OSI seven-layer model and a specific protocol.
protocol families	Grouping of logical properties within an interface configuration, for example, the inet, inet4, and mpls protocol families.

Protocol Field Compression	PFC. 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, *The Point-to-Point Protocol (PPP)*. PFC allows you to conserve bandwidth by transmitting less data. *See also* ACFC.
Protocol Independent Multicast	PIM. A set of multicast routing protocols for one-to-many and many-to-many data distribution over networks or the Internet. PIM is protocol-independent, using the routing information from other routing protocols such as BGP. 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).
Protocol Independent Multicast dense mode	PIM dense mode. Uses a reverse-path multicast, flood-and-prune mechanism. *See also* dense mode.
Protocol Independent Multicast source-specific multicast	PIM SSM. Extension of the PIM protocol where a client can receive multicast traffic directly from the source. PIM SSM uses PIM sparse mode functionality to create a shortest-path tree (SPT) between the client and the source, but builds the SPT without using a rendezvous point.
Protocol Independent Multicast sparse mode	PIM sparse mode. A sparse mode multicast protocol, which uses shared trees. In a shared tree, sources forward multicast datagrams to a directly connected router, the designated router. The designated router encapsulates the datagram and unicasts it to an assigned rendezvous point router, which then forwards the datagram to members of multicast groups. *See also* sparse mode.
Protocol Independent Multicast sparse-dense mode	PIM sparse-dense mode. Used to send data when a rendezvous point (RP) is not known for a group. However, if the router discovers an RP or you configure an RP statically, PIM sparse mode takes over.
protocol normalization	Method of reducing false positives in network intrusion detection systems, by "normalizing" traffic into a common format for accurate analysis, so that access to hosts takes place in a manner that is unambiguous.
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	PBB, PBBN, provider backbone bridge network. Defined in IEEE 802.1ah, PBBs offer a scalable solution for building large bridged networks by improving MAC address scalability and service instance scalability.
provider backbone bridge network	PBBN, 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.
provider core router	P router. Router within a service provider core that connects directly to PE routers or other P routers and does not connect directly to a customer edge (CE) device. *See also* PE router.

provider edge router	PE router. Router in the service provider's network that is connected to a customer edge (CE) device and participates in a virtual private network (VPN). *See also* P router.
provider router	Router in the service provider's network that is not connected to a customer edge (CE) device.
proxy	Proxy or proxy server is a technique used to cache information on a Web server and acts as an intermediary between a Web client and that Web server. It breaks the connection between sender and receiver and acts as a relay between client and server.
proxy ARP	proxy Address Resolution Protocol. Enables an E Series router to respond to ARP requests on behalf of an Ethernet end node.
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	Protected System Domain. 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.
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. Packet that contains only a partial list of the LSPs in the IS-IS link-state database; a PDU sent by a designated router to acknowledge and request link-state information.
PSTN	public switched telephone network. The public worldwide voice telephone network.
PTM	Packet Transfer Mode. Method of transporting packet-based services based on the EFM IEEE802.3ah standard.
public key infrastructure	PKI. 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.
Public Land Mobile Network	PLMN. Telecommunications network for mobile stations.
public switched telephone network	PSTN. The public worldwide voice telephone network.
Public-Key Cryptography Standards	PKCS. Series of standards established by RSA Laboratories.
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 or channel. Also called permanent virtual connection (when referring to ATM. Software-defined logical connection in a network; a virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and teardown in situations where certain virtual circuits must exist all the time. *See also* SVC, switched virtual connection (or circuit).

Q

Q-in-Q	The IEEE802.1ad specification for encapsulation and bridging of Ethernet frames. *Also known as* IEEE 802.1QinQ, provider bridging, or stacked VLANs, Q-in-Q allows multiple VLAN headers to be inserted into a single frame, an essential capability for implementing Metro Ethernet network topologies.
QoS	quality of service. Performance, such as transmission rates and error rates, of a communications channel or system. A suite of features that configure queuing and scheduling on the forwarding path of an E Series router. QoS provides a level of predictability and control beyond the best-effort delivery that the router provides by default. (Best-effort service provides packet transmission with no assurance of reliability, delay, jitter, or throughput.) *See also* CoS.
QoS administrator	Person responsible for implementing a QoS queuing architecture by defining the scheduler profiles and referencing them from QoS profiles. A QoS administrator also configures parameter definitions that control the parameters, interfaces, and ranges of values that QoS clients, using QoS parameters, can assign.
QoS client	Person responsible for configuring services for individual subscribers by creating parameter instances. The parameter instances that a QoS client creates depend on the settings that the QoS administrator defined in parameter definitions. QoS clients can use the CLI, Service Deployment System (SDX), IP multicast bandwidth adjustment, RADIUS, or Service Manager to manage these services.
QoS parameters	Special parameters that enable you to configure a queuing architecture without specifying numeric subscriber rates and weights in scheduler profiles. You then use the same QoS and scheduler profiles across all subscribers who use the same services but at different bandwidths, reducing the total number of QoS profiles and scheduler profiles required.
QoS port-type profile	QoS profile that is automatically attached to ports of the corresponding type if you do not explicitly attach a QoS profile.
QoS profile	Collection of QoS commands that specify queue profiles, drop profiles, scheduler profiles, and statistics profiles in combination with interface types.
QoS profile attachment	Reference that applies the rules in the QoS profile to a specific interface.
quad-wide	Type of PIC that combines the PIC and FPC within a single FPC slot.
quadruple play	Addition of mobile phone service to triple play. *See also* triple play.
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	QoS. Performance, such as transmission rates and error rates, of a communications channel or system. A suite of features that configure queuing and scheduling on the forwarding path of an E Series router. QoS provides a level of predictability and control beyond the best-effort delivery that the router provides by default. (Best-effort service provides packet transmission with no assurance of reliability, delay, jitter, or throughput.) *See also* CoS, class of service.
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, the 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. *See also* 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.
queue profile	Template that specifies the buffering and tail-dropping behavior of an egress queue.
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. Trusted third-party organization that acts on behalf of a certificate authority (CA) to verify the identity of a digital certificate user.
rack unit	RU. The standard single unit height of a rack-mounted device.
radio frequency interference	RFI. Interference from high-frequency electromagnetic waves emanating from electronic devices.
radio network controller	RNC. Manages the radio part of the network in UMTS.
RADIUS	Remote Authentication Dial-In User Service. Distributed client/server AAA service method that protects networks against unauthorized access. RADIUS clients running on an E Series router send authentication requests to a central RADIUS server. The central RADIUS server stores all the required user authentication and network access information. RADIUS informs the router of the privilege levels for which RADIUS-authenticated users have enable access. The router permits or denies enable access accordingly.

RADIUS-based packet mirroring	RADIUS administrator uses RADIUS attributes to configure packet mirroring of a particular user's traffic without regard to how often the user logs in or out or which E Series router or interface the user uses. It is particularly appropriate for large networks and for debugging network problems related to mobile users, who do not always log in to a particular router.
random early detection	RED. 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.
Rapid Spanning Tree Protocol	RSTP. Used to prevent loops in bridge configurations. RSTP is not aware of VLANs and blocks ports at the physical level. *See also* MSTP, Multiple Spanning Tree Protocol.
RAS	remote access service. Any combination of hardware and software to enable users to remotely access services protected by your network security devices . Typically, you use a virtual private network (VPN) to enable RAS, then add RAS users to the VPN.
rate limiting	• Method of applying rate limits on bandwidth and burst size for traffic on a particular interface. *See also* one-rate rate-limit profile, two-rate rate-limit profile, policing. • In IDP Series, an application policy enforcement (APE) rule-based action. When the bandwidth rate for matching traffic is below the rate limit, the IDP series appliance does nothing. When the bandwidth rate exceeds the limit, the IDP appliance behaves as if no bandwidth is available and drops the packets.
rate shaping	Mechanism that throttles the rate at which an interface can transmit packets.
rate-limit hierarchy	Enables lower-priority traffic to access unused bandwidth allocated for real-time traffic during times when no real-time traffic is flowing. *See also* color-aware rate limit, color-blind rate limit.
rate-limit profile	Set of bandwidth attributes and associated actions that provides a variety of services, including tiered bandwidth service where traffic conforming to configured bandwidth levels is treated differently than traffic that exceeds the configured values, and a hard-limit service where a fixed bandwidth limit is applied to a traffic flow. Also provides a TCP-friendly rate-limiting service that works in conjunction with TCP's native flow-control functionality. *See also* one-rate rate-limit profile, two-rate rate-limit profile.
RBOC	Regional Bell Operating Company, pronounced "are-bock". Regional telephone companies formed as a result of the divestiture of the Bell System in 1984. *Also known as* Baby Bell.
RC2, RC4, RC5	RSA codes. 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. Presents data in a tabular form with a means of manipulating the tabular data with relational operators.
RDI cell	remote defect indication cell. Cell received from the remote endpoint of the virtual path (VP) or virtual connection (VC) that indicates an interruption in the cell transfer capability of the VP/VC.

RDM	Russian Dolls model. A bandwidth constraints model that makes efficient use of bandwidth by allowing the class types to share bandwidth, as defined in RFC 4127, *Russian Dolls Bandwidth Constraints Model for DiffServ-aware MPLS Traffic Engineering*. "Russian Dolls" refers to a traditional type of nested doll-within-a-doll set.
real server	The logical representation of a service or server application residing on a physical server. A real server is defined by an IP address and an optional port corresponding to the service. *See also* physical server.
Real-Time Messaging Protocol	RTMP. A multimedia streaming and remote procedure call (RPC) protocol primarily used in Adobe Flash. RTMP has three variations: The "plain" protocol that works on top of TCP and uses port 1935; RTMPT which is encapsulated within HTTP requests to traverse firewalls; and RTMPS which works just like RTMPT but over a secure HTTPS connection.
real-time performance monitoring	RPM. Tool for creating active probes to track and monitor traffic.
Real-Time Streaming Protocol	RTSP. Application-level protocol for control over the delivery of data with real-time properties, it provides an extensible framework to enable controlled, on-demand delivery of real-time data such as audio and video. Sources of data can include both live data feeds and stored clips. This protocol is intended to control multiple data delivery sessions, provide a means for choosing delivery channels such as UDP, multicast UDP and TCP, and provide a means for choosing delivery mechanisms based upon RTP.
Real-Time Transport Protocol	RTP. 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.
real-time variable bit rate	RTVBR. 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.
Realtime Monitor	Module of NSM user interface that displays views of the Device Monitor, the VPN Monitor, and the NSRP Monitor. It provides continuous monitoring of the status of your security devices.
receive	Next hop for a static route that allows all matching packets to be sent to the Routing Engine for processing.
receive collision	Result of two devices on the same Ethernet network attempting to receive data at exactly the same time. Collisions on the line are detected by the Carrier Sense Multiple Access Collision Detection (CSMA/CD) protocol.
receive window size	RWS. Number of packets that an L2TP peer can transmit without receiving an acknowledgment from the router. L2TP uses the RWS to implement a sliding window mechanism for the transmission of control messages. If the RWS is not configured for the L2TP tunnel, the router determines the RWS and uses this value for all new tunnels on both the L2TP access concentrator (LAC) and the L2TP network server (LNS).
Recommended Standard 232	RS-232. Serial line protocol recommended standard. *Also known as* EIA-232. Standard connector used commonly in computer serial ports.

Recommended Standard 449	RS-449. Serial line protocol recommended standard that defines the functional and mechanical characteristics of the interface between DTE and DCE. *Also known as* EIA-449.
record route object	RRO. An RSVP message object that notes the IP address of each router along the path of an LSP.
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.
redirected authentication	Service that helps offload AAA activity on the router, by providing the domain-mapping-like feature remotely on the RADIUS server.
redistribution	*Also known as* route redistribution. Method of placing learned routes from one protocol into another protocol operating on the same router. The Junos OS accomplishes this with a routing policy.
redistribution list	List imported by current routing domain from another routing domain using a different protocol. *See also* route redistribution.
redundancy	*Also called* line module redundancy. Configuration in which an extra line module in a group of identical line modules provides redundancy if one of the modules fails. The process by which the router switches to the spare line module is called switchover. The requirements for line module redundancy depend on the router type. *See also* HA, switchover.
redundancy midplane	Hardware component that provides additional connectivity so the spare line module can take control of the I/O module associated with any failed line module in the redundancy group. *See also* midplane.
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	RBOC, pronounced "are-bock". Regional telephone companies formed as a result of the divestiture of the Bell System in 1984. *Also known as* Baby Bell.
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	RA. Trusted third-party organization that acts on behalf of a certificate authority (CA) to verify the identity of a digital certificate user.

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	RDBMS. Presents data in a tabular form with a means of manipulating the tabular data with relational operators.
relative strict-priority scheduling	Process that provides strict-priority scheduling within a shaped aggregate rate. It differs from true strict priority in that it can implement an aggregate shaping rate for both strict and nonstrict traffic. With true strict priority, you can shape the nonstrict or the strict traffic separately, but you cannot shape the aggregate to a single rate.
relative URL	Points to the location of a file from a point of reference, usually the directory beneath. Preceded by two dots (../directory_path/file.txt) for the directory above; one dot (./directory_path/file.txt) for the current directory. *Contrast with* absolute URL.
relay proxy	*Also called* DHCP relay proxy, an enhancement to the E-series router's DHCP relay component that manages host routes for DHCP clients, including selecting the single most appropriate offer from multiple DHCP servers.
remote access service	RAS. Any combination of hardware and software that enables users to remotely access services protected by network security devices . Typically, you use a virtual private network (VPN) to enable RAS, then add RAS users to the VPN.
Remote Authentication Dial-In User Service	RADIUS.Distributed client/server AAA service method that protects networks against unauthorized access. RADIUS clients running on an E Series router send authentication requests to a central RADIUS server. The central RADIUS server stores all the required user authentication and network access information. RADIUS informs the router of the privilege levels for which RADIUS-authenticated users have enable access. The router permits or denies enable access accordingly.
remote defect indication cell	RDI cell. Cell received from the remote endpoint of the virtual path (VP) or virtual connection (VC) that indicates an interruption in the cell transfer capability of the VP/VC.
remote loopback	Ability to request that remote devices enter into loopback; the ability to be placed in loopback by remote devices.
remote monitoring	RMON. 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.
remote neighbors	RIP neighbors that enable the router to establish neighbor adjacencies through unidirectional interfaces, such as MPLS tunnels, rather than the standard practice of using the same interface for receipt and transmission of RIP packets. The remote neighbor can be more than one hop away through intermediate routes that are not running RIP. RIP uses the interface associated with the best route to the remote neighbor to reach the neighbor. A best route to the neighbor must exist in the IP routing table.

remote procedure call	RPC. 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.
remote settings object	Object that defines the DNS and WINS servers that are assigned to L2TP RAS users after they have connected to the L2TP tunnel.
rename	Junos OS 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	RP. For PIM sparse mode, a core router acting as the root of the distribution tree in a shared tree.
Report Manager	Module of the NSM user interface for generating and viewing reports of log entries and alarms. The reports are used to track and analyze log incidents, network traffic, and potential attacks.
Request for Comments	RFC. Internet standard specifications published by the Internet Engineering Task Force (IETF).
request message	RIP message used by a router to ask for all or part of the routing table from a neighbor.
requesting authority	Group that is authorized to request or conduct packet mirroring (E Series routers).
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	RSVP. Establishes a session between two routers to transport a specific traffic flow. *See also* RSVP-TE.
Resource Reservation Protocol—Traffic Engineering	RSVP-TE. RSVP with traffic engineering extensions, as defined by RFC 3209, that allow RSVP to establish label-switched paths (LSPs) in MPLS networks. *See also* MPLS, RSVP.
resource threshold monitor	RTM. CLI mode that enables you to set the rising and falling thresholds and trap hold-down times for certain interfaces. You can also view the resource threshold information.
response message	RIP message used to advertise routing information into a network.
Response Time Reporter	RTR. Feature that enables you to monitor network performance and resources by measuring response times and the availability of your network devices. The primary objective of RTR is to collect statistics and information about network performance.
result cell	Junos OS 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	RPF. 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.
reverse path multicasting	RPM. Routing algorithm used by Distance Vector Multicast Routing Protocol (DVMRP) to forward multicast traffic.
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 interference. Interference from high-frequency electromagnetic waves emanating from electronic devices.
RIB	routing information base. Logical data structure used by BGP to store routing information, including routes BGP learned from peers, local routes resulting from the application of BGP policies to the learned routes, and the routes that BGP advertises to its peers. *See also* routing table.
RID	router identification. 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. Interior gateway protocol (IGP) typically used in small, homogeneous IPv4 networks, it uses distance-vector routing to route information based on hop count. *See also* distance-vector routing.
RIP messages	Messages sent from the RIP port that contain routing information. RIP exchanges routing information by means of User Datagram Protocol (UDP) data packets. Each RIP router sends and receives datagrams on UDP port number 520, the RIP version 1/RIP version 2 port. All communications intended for another router's RIP process area are sent from the RIP port.
RIP metric	Compares the value of different routes, based on hop count. The hop count is the number of routers that data packets must traverse between RIP networks. Metrics range from 0 for a directly connected network to 16 for an unreachable network. This small range prevents RIP from being useful for large networks. *Also known as* cost.

RIPng	Routing Information Protocol next generation. Used in IPv6 networks, a distance-vector interior gateway protocol that makes routing decisions based on hop count.
Rivest-Shamir-Adleman (encryption algorithm)	RSA. Algorithm for public key encryption.
RJ-45 connector	Connector commonly used for 10Base and 100Base Ethernet connections.
RMON	remote monitoring. 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.
role-based administration	Method of creating a security environment by defining strategic roles for administrators and creating domains of network devices where access is granted by assigned role.
root certificate	Self-signed public key certificate for a root CA; root certificates are used to verify other certificates.
Root System Domain	RSD. Pair of redundant Routing Engines on 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).
round-robin server access	Method of access for RADIUS servers. The first configured server is treated as a primary for the first request, the second server configured as primary for the second request, and so on. When the router reaches the end of the list of servers, it starts again at the top of the list until it comes full cycle through the list. *See also* direct server access.
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 OS syntax used in a routing policy to match an individual route or a group of routes.
route flap damping, route flap dampening	Method for minimizing instability caused by route flapping. The router stores a penalty value with each route. Each time the route flaps, the router increases the penalty by 1000. If the penalty for a route reaches a configured suppress value, the router suppresses the route. That is, the router does not include the route as a forwarding entry and does not advertise the route to BGP peers. *See also* route flapping.
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 leakage
Process of allowing routes from one protocol or area to be learned by another protocol or area. Routes can be leaked into OSPF or from OSPF as follows:

- Route leakage into OSPF—When another routing protocol adds a new route to the routing table, or when a static route is added to the routing table, OSPF can be informed through the redistribute commands. When OSPF learns the new route, it floods the information into the routing domain by using external LSAs.

- Route leakage from OSPF—OSPF adds routing information to the routing table, which is used in forwarding IP packets.

route maps
- Modify the characteristics of a route (generally to set its metric or to specify additional attributes) as it is transmitted or accepted by a router. Route maps control and modify routing information and define conditions for redistributing routes between routing domains. Route maps can use access lists to identify the set of routes to modify.

- In BGP, route maps consist of match clauses and set clauses. Match clauses specify the attribute values that determine whether a route matches a route map. Set clauses modify the specified attributes of routes that pass all match clauses in the route map.

route redistribution
Method of placing learned routes from one protocol into another protocol operating on the same router. The Junos OS 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. An alternative to confederations as a strategy to reduce IBGP meshing. BGP specifies that a BGP speaker cannot advertise routes to an IBGP neighbor if the speaker learned the route from a different IBGP neighbor. In route reflection, a BGP speaker (the route reflector) advertises routes learned from each of its IBGP neighbors to its other IBGP neighbors. Routes are reflected among IBGP routers that are not meshed. *See also* cluster, confederation, route reflector, route reflector client.

route reflector
BGP speaker that advertises routes learned from each of its IBGP neighbors to its other IBGP neighbors; routes are reflected among IBGP routers that are not meshed. The route reflector's neighbors are called route reflector clients. The clients are neighbors only to the route reflector, not to each other. Each route reflector client depends on the route reflector to advertise its routes within the AS; each client also depends on the route reflector to pass routes to the client.

A route reflector and its clients are collectively referred to as a cluster. Clients peer only with a route reflector and do not peer outside their cluster. Route reflectors peer with clients and other route reflectors within a cluster; outside a cluster they peer with other reflectors and other routers that are neither clients nor reflectors. Route reflectors and nonclient routers must be fully meshed. *See also* route reflector client.

route reflector client
A neighbor of a route reflector. The clients are neighbors only to the route reflector, not to each other. Each route reflector client depends on the route reflector to advertise its routes within the AS. Each client also depends on the route reflector to pass routes to the client. *See also* cluster, route reflector.

route tag	• Field in an RIP message that allows boundary routers in an autonomous system (AS) to exchange information about external routes. Route tags provide a method of separating internal RIP routes (routes within the RIP routing domain) from external RIP routes, which may have been imported from an EGP (Exterior Gateway Protocol) or another IGP (Interior Gateway Protocol).
	• In IS-IS, a numeric value assigned to the IP addresses on an IS-IS route before the route is propagated to other routers in an IS-IS domain. You can use this tag to control IS-IS route redistribution, route leaking, or route summarization by referencing it in a route map.
route target	BGP extended community used to define VPN membership. The route target appears in a field in the update messages associated with VPN-IPv4. You create route-target import lists and route-target export lists for each VRF. The route targets that you place in a route-target export list are attached to every route advertised to other PE routers. When a PE router receives a route from another PE router, it compares the route targets attached to each route against the route-target import list defined for each of its VRFs. If any route target attached to a route matches the import list for a VRF, then the route is imported to that VRF. If no route target matches the import list, then the route is rejected for that VRF.
route-refresh capability	Lower-cost alternative to soft reconfiguration as a means to change policies without major disruptions. The router advertises the route-refresh capability when it establishes a BGP session with a peer to indicate that it is capable of exchanging BGP route-refresh messages. *See also* cooperative route filtering, soft reconfiguration.
router ID	RID. 32-bit number that uniquely identifies a router within an autonomous system, for example, 10.10.1.5.
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 OPSF or IS-IS interface that is used as the first criterion in electing the designated router or designated intermediate system, respectively.
router solicitation address	IP address to which a DHCP client can transmit router solicitation requests.
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.
router.conf	Default router configuration file for autoinstallation, with a minimum configuration sufficient for you to telnet to the device and configure it manually.
routing domain	Collection of contiguous networks that provide full connectivity to all end systems located within them. A routing domain is partitioned into areas. *See also* AS.
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	Firewall, Network Address Translation (NAT) router, or other routing device used as a customer premises equipment (CPE) terminator in the home, office, or local point of presence (POP).
routing information base	RIB. Logical data structure used by BGP to store routing information, including routes BGP learned from peers, local routes resulting from the application of BGP policies to the learned routes, and the routes that BGP advertises to its peers. *See also* routing table.
Routing Information Protocol	RIP. Interior gateway protocol (IGP) typically used in small, homogeneous IPv4 networks, it uses distance-vector routing to route information based on hop count. *See also* distance-vector routing.
Routing Information Protocol next generation	RIPng. Used in IPv6 networks, a distance-vector interior gateway protocol that makes routing decisions based on hop count.
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 policy	Method to control flow of routes into and out of the router. Determines how the system handles the routes it receives from and sends to neighboring routers. In many cases, routing policy consists of filtering routes, accepting certain routes, accepting and modifying other routes, and rejecting some routes.
routing protocol daemon	rpd. Junos OS routing protocol process (daemon). User-level background process responsible for starting, managing, and stopping the routing protocols on a Juniper Networks router.
routing table	Common database of routes learned from one or more routing protocols. Because each protocol typically has multiple routes to a destination, the IP routing table maintains the one best route by protocol. All routes are maintained by the Junos OS 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. 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 OS routing protocol process (daemon). User-level background process responsible for starting, managing, and stopping the routing protocols on a Juniper Networks router.

RPF	reverse path forwarding. 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	• reverse path multicasting. Routing algorithm used by the Distance Vector Multicast Routing Protocol (DVMRP) to forward multicast traffic.
	• real-time performance monitoring. Tool for creating active probes to track and monitor traffic.
RPM target	Remote network endpoint, identified by an IP address or URL, to which the device sends a real-time performance monitoring (RPM) probe.
RPM test	A collection of real-time performance monitoring (RPM) probes sent out at regular intervals.
RRO	record route object. An RSVP message object that notes the IP address of each router along the path of an LSP.
RS-232	Recommended Standard 232. Serial line protocol recommended standard, *also known as* EIA-232. Standard connector commonly used in computer serial ports.
RS-449	Recommended Standard 449. Serial line protocol recommended standard, *also known as* EIA-449. Defines the functional and mechanical characteristics of the interface between DTE and DCE.
RSA	Rivest-Shamir-Adleman (encryption algorithm). Algorithm for public key encryption.
RSA codes	RC2, RC4, RC5. 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.
RSD	Root System Domain. Pair of redundant Routing Engines on 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).
RSTP	Rapid Spanning Tree Protocol. Used to prevent loops in bridge configurations. RSTP is not aware of VLANs, and blocks ports at the physical level. *See also* MSTP.
RSVP	Resource Reservation Protocol. Establishes a session between two routers to transport a specific traffic flow. *See also* RSVP-TE.
RSVP MD5 authentication	Method of authentication that provides hop-by-hop security against message spoofing and replay attacks. When authentication is configured, RSVP embeds an integrity object within secure cleartext RSVP messages sent between peers. The integrity object includes a key ID unique to the sender, a message sequence number, and keyed message digest. These attributes enable verification of both packet content and sender.

RSVP Path 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   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   Resource Reservation Protocol--Traffic Engineering. RSVP with traffic engineering extensions, as defined by RFC 3209, that allow RSVP to establish label-switched paths (LSPs) in MPLS networks. *See also* MPLS, RSVP.

RTM   resource threshold monitor. CLI mode that enables you to set the rising and falling thresholds and trap hold-down times for certain interfaces. You can also view the resource threshold information.

RTMP   Real-Time Messaging Protocol. A multimedia streaming and remote procedure call (RPC) protocol primarily used in Adobe Flash. RTMP has three variations: The "plain" protocol that works on top of TCP and uses port 1935; RTMPT which is encapsulated within HTTP requests to traverse firewalls; and RTMPS which works just like RTMPT but over a secure HTTPS connection.

RTO   run time object. Code object created dynamically in memory during normal operation. Some examples of RTOs are session table entries, ARP cache entries, certificates, DHCP leases, and IPsec Phase 2 security associations (SAs).

RTP   Real-Time Transport Protocol. 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.

RTR   Response Time Reporter. Feature that enables you to monitor network performance and resources by measuring response times and the availability of your network devices. The primary objective of RTR is to collect statistics and information about network performance.

RTSP   Real-Time Streaming Protocol. Application-level protocol for control over the delivery of data with real-time properties, it provides an extensible framework to enable controlled, on-demand delivery of real-time data such as audio and video. Sources of data can include both live data feeds and stored clips. This protocol is intended to control multiple data delivery sessions, provide a means for choosing delivery channels such as UDP, multicast UDP and TCP, and provide a means for choosing delivery mechanisms based upon RTP.

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.

RU   rack unit. The standard single unit height of a rack-mounted device.

rule Statement that defines a specific type of network traffic. When traffic passes through the security device, the device attempts to match that traffic against its list of rules. If a rule is matched, the device performs the action defined in the rule against the matching traffic.

rule base Set of rules that defines what traffic is and is not allowed to pass, using a specific detection mechanism to identify and prevent attacks. A security policy contains one or more rule bases. For example, NSM can contain three types of rule bases: zone, global, and multicast.

run time object RTO. Code object created dynamically in memory during normal operation. Some examples of RTOs are session table entries, ARP cache entries, certificates, DHCP leases, and IPsec Phase 2 security associations (SAs).

RWS receive window size. Number of packets that an L2TP peer can transmit without receiving an acknowledgment from the router. L2TP uses the RWS to implement a sliding window mechanism for the transmission of control messages. If the RWS is not configured for the L2TP tunnel, the router determines the RWS and uses this value for all new tunnels on both the L2TP access concentrator (LAC) and the L2TP network server (LNS).

RX Communications abbreviation for receive; the corresponding abbreviation for transmit is TX.

S

S-TAG Field defined in the IEEE 802.1ad Q-in-Q encapsulation header that carries the S-VLAN identifier information *See also* 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. Similarly, a B-tagged service interface contains a B-TAG field.

S-VLAN stacked VLAN, service VLAN, or switched VLAN. Provides a two-level VLAN tag structure, with a specific service instance VLAN identifier carried inside the S-TAG field. Creating an S-VLAN requires the use of a second encapsulation tag; the router performs decapsulation twice, once to get the S-VLAN tag and once to get the VLAN tag. This double tagging approach enables more than 16 million address possibilities, extending the VLAN ID space to more than 16 million VLANs. This meets and exceeds the scaling requirement for Ethernet B-RAS applications. Defined by IEEE 802.1ad, an S-VLAN often corresponds to a network aggregation device such as a DSLAM. Scheduling and shaping is often established for an S-VLAN to provide CoS for downstream devices with little buffering and simple schedulers. *See also* B-VID, C-VLAN.

S-VLAN oversubscription Ability to configure up to the maximum number of S-VLANs supported on an I/O module or IOA, knowing that no more than the maximum number of supported PPP sessions can be connected to the router at any one time.

S-VLAN tunnel Special type of stacked VLAN that uses a single interface to tunnel traffic from multiple VLANs across an MPLS network. The S-VLAN tunnel enables multiple VLANs, each configured with a unique VLAN ID tag, to share a common S-VLAN ID tag when they traverse an MPLS network.

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. Set of security parameters that dictates how IPsec processes a packet. The SA defines what rules to use for authentication and encryption algorithms, key exchange mechanisms, and secure communications between two parties. A single secure tunnel uses multiple SAs. *See also* SA parameters.

SA parameters | Actual session parameters used to secure a specific data flow associated with a specific secure IP interface. How SA parameters are set depends on how the IP interfaces are secured:

- For manual secure IP interfaces, the system administrator sets SA parameters manually, which allows provisioning IP security (using IKE) to destinations that do not support SA negotiation.

- For signaled secure IP interfaces, the two security gateway peers negotiate SA parameters; the system administrator cannot set any of the parameters. For some of these parameters, such as session keys, the system administrator does not have even read access.

SAFI | subsequent address family identifier. Number that further identifies an address family identified by an AFI. In an MP-BGP update message, SAFI is used with AFI to identify the network layer protocol associated with the network address of the next hop and the semantics of the NLRI that follows. *See also* AFI.

salt encryption | Random string of data used to modify a password hash.

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 | • Session Announcement Protocol. Used with multicast protocols to handle session conference announcements.

- 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.

SAR scheduler | One part of the integrated scheduler used to extend ATM QoS functionality. The commercial SAR scheduler enables you to configure traditional ATM cell-based QoS. *See also* HRR scheduler.

SAS | serial-attached SCSI. Data transfer technology used to move data to and from computer storage devices such as hard drives and tape drives.

SATA | Serial Advanced Technology Attachment. A computer bus technology primarily for transfer of data to and from a hard disk.

SC | system controller. Subsystem located on the SRP modules on the E320 router that controls the overall operations on the router.

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 OS command-line interface (CLI) to refer to the TX Matrix platform in a routing matrix.

SCEP   Simple Certificate Enrollment Protocol. 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.

schedule object   Object that defines the time interval that a firewall rule is in effect. Use a schedule object in a firewall rule to determine when a device enforces that rule.

scheduler hierarchy   Hierarchical, tree-like arrangement of scheduler nodes and queues. The router supports up to three levels of scheduler nodes stacked above a port (level 0), with a final level of queues stacked above the nodes. A traffic-class group uses a scheduler level at level 1.

scheduler maps   In class of service, schedule maps associate schedulers with specific forwarding classes. *See also* schedulers, forwarding classes.

scheduler node   Element within the hierarchical scheduler that implements bandwidth controls for a group of queues. Queues are stacked above scheduler nodes in a hierarchy. The root node is associated with a channel or physical port.

scheduler profile   Collection of commands that configures the bandwidth at which queues drain as a function of relative weight, assured rate, and shaping rate.

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. *See also* 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). *See also* FIFO.

scope   Value used in some unicast and multicast IPv6 addresses that identifies the application suitable for the address. *See also* address scope.

SCP   secure copy. A protocol, program, or command based on SSH (Secure Shell Protocol) that securely transfers computer files, usually between a local and a remote host or between two remote hosts.

SCR   sustained cell rate. Upper bound on the conforming average rate of an ATM connection over a sustained time interval that is longer than the time interval for which the PCR is defined.

SCSI	small computer system interface. A standard interface and command set for transferring data between devices over a computer bus.
SCU	source class usage. 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. International standard defined by the International Telecommunication Union for transmitting bits over fiber-optic cable. 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. 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. A type of RAM that is stored on dual in-line memory modules (DIMMs) and synchronized with the system clock.
SDSL	symmetric digital subscriber line. Version of digital subscriber line (DSL) where the upload speeds and download speeds are the same, typically in the range 144 Kbps–1.5 Mbps. SDSL uses one cable pair and does not share lines with analog phones.
SDX software	Service Deployment System software. Deprecated term. *See* SRX software.
secondary input policy	Evaluates conditions after a route lookup. *See also* input policy, output policy, policy.
section layer	For channelized OCx/STMx interfaces, the layer that manages the transport of STS/STM frames across the physical path. This layer is responsible for frame alignment, scrambling, error detection, error monitoring, signal reception, and signal regeneration. *See also* line layer, path layer.
Secure Access Device	Juniper Networks SSL VPN appliance.
secure copy	SCP. A protocol, program, or command based on SSH (Secure Shell Protocol) that securely transfers computer files, usually between a local and a remote host or between two remote hosts.
Secure Hash Algorithm	SHA. One of the cryptographic hashing functions used by FIPS, it is a standard published by NIST. *See also* hashing, SHA-1.
secure IP interfaces	Virtual IP interfaces that you can configure to provide confidentiality and authentication services for the data flowing through such interfaces. The software provides these services using mechanisms created by the suite of IPsec standards established by the IETF.
secure policy	Policy that is created with a mirror action and that contains information about where to forward mirrored traffic during packet mirroring. *See also* packet mirroring.

Secure Server Protocol	SSP. Modified version of TCP that is more reliable than ordinary TCP, requires less CPU and memory resources from servers, and reduces the number of acknowledgement packets on the network. SSP uses AES encryption and SH1 authentication for all connections. NSM uses SSP for communication between the UI, the GUI Server, and the Device Server.
Secure Shell	SSH. 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**.
Secure Sockets Layer	SSL. 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.
secure tunnel	Virtual connection between two security gateways used to exchange data packets in a secure way. A secure tunnel is made up of a local SA and a remote SA, where both are negotiated in the context of an ISAKMP SA.
security association	SA. Set of security parameters that dictates how IPsec processes a packet. The SA defines what rules to use for authentication and encryption algorithms, key exchange mechanisms, and secure communications between two parties. A single secure tunnel uses multiple SAs. *See also* SA parameters.
security device	Hardware device that enables secure access to your network components and protects your network against malicious traffic.
security level	Measure of how seriously a triggering event affects device functions.
Security Parameter Index	SPI. 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.
security policy	• Set of rules defining access to your network, including permitted services, users, and time periods. Use security policies to control the shape of your network traffic as it passes through the firewall, or to log specific network events. • In IDP Series, a set of one or more rule bases that determine which traffic to inspect, what to look for, and what action to take if a rule matches.
security policy database	SPD. Ordered list of policy entries that specifies what services are to be offered to IP datagrams and in what fashion. The SPD must discriminate between traffic that has IPsec protection and traffic that is allowed to bypass IPsec. This applies to the IPsec protection to be applied by a sender and that must be present at the receiver. The SPD requires distinct entries for inbound and outbound traffic. For any outbound or inbound datagram, three processing choices are possible: discard, bypass IPsec, or apply IPsec.
security zone	Collection of one or more network segments requiring the regulation of inbound and outbound traffic through the use of access policies.

segmentation and reassembly	SAR. Buffering used with ATM.
Serial Advanced Technology Attachment	SATA. A computer bus technology primarily for transfer of data to and from a hard disk.
serial interface	DTE/DCE interface for WAN links. *See also* DTE and DCE.
Serial Line Address Resolution Protocol	SLARP. Simple control protocol provided by the Cisco High-Level Data Link Control implementation that maintains serial link keepalives. *See also* Cisco HDLC.
serial-attached SCSI	SAS. Data transfer technology used to move data to and from computer storage devices such as hard drives and tape drives.
Server Manager	Module of the NSM user interface used to manage and monitor the individual server processes that comprise your NSM system.
service access point	SAP. Device that identifies routing protocols and provides the connection between the network interface card and the rest of the network.
Service Deployment System software	SRX software, *formerly known as* Service Deployment System 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.
service level agreement	SLA . Formal agreement between a service provider and its customers (as part of a networking service contract) to provide a certain level of service (usually a level of performance).
service line module	SLM. Tunnel-service line module that does not pair with a corresponding I/O module that provides ingress and egress ports. Receives data from and transmits data to line modules that have ingress and egress ports.
service name tag	Entry in a PPPoE service name table that specifies a particular service that an access concentrator (AC), such as an E Series router, can provide to a PPPoE client. An empty service name tag of zero length indicates that any service is acceptable. *See also* PPPoE service name table.
service object	Service objects represent the IP traffic types for existing protocol standards. Security devices monitor and manage network traffic using these protocols. NSM includes predefined service objects for most standard services. You can also create custom service objects to represent services that are not included in the list of predefined service objects, or to represent a custom service running on your network.
Service Profile Identifier	SPID. 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.

service VLAN	S-VLAN, stacked VLAN, or switched VLAN. Provides a two-level VLAN tag structure, with a specific service instance VLAN identifier carried inside the S-TAG field. Creating an S-VLAN requires the use of a second encapsulation tag; the router performs decapsulation twice, once to get the S-VLAN tag and once to get the VLAN tag. This double tagging approach enables more than 16 million address possibilities, extending the VLAN ID space to more than 16 million VLANs. This meets and exceeds the scaling requirement for Ethernet B-RAS applications. Defined by IEEE 802.1ad, an S-VLAN often corresponds to a network aggregation device such as a DSLAM. Scheduling and shaping is often established for an S-VLAN to provide CoS for downstream devices with little buffering and simple schedulers. *See also* B-VID, C-VLAN.
Services and Routing Engine	SRE. SRX mid-range services gateway module that provides processing power for security services, routing protocol processes, and other software processes that control the services gateway interfaces, some of the chassis components, system management, and user access to the device.
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. *See also* network interface.
Serving GPRS Support Node	SGSN. Device in the mobile network that requests PDP contexts with a GGSN.
Session and Resource Control software	SRX 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.
Session Announcement Protocol	SAP. Used with multicast protocols to handle session conference announcements.
session attribute object	RSVP message object used to control the priority, preemption, affinity class, and local rerouting of the LSP.
Session Description Protocol	SDP. Used with multicast protocols to handle session conference announcements.
Session Initiation Protocol	SIP. 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.
session layer	Fifth level in the seven-layer OSI reference model for network protocol design, it controls the dialogues and connections (sessions) between computers. It establishes, manages, and terminates the connections between the local and remote application. The OSI model made this layer responsible for "graceful close" of sessions, which is a property of TCP, and also for session checkpointing and recovery, which is not usually used in the Internet protocols suite. Session layers are commonly used in application environments that make use of remote procedure calls (RPCs).

set clause	Part of a route map that defines how the attributes are modified for matching routes. The set conditions apply only to routes that pass all the match conditions (or a route map with no match conditions). When a route passes all the match conditions, all set conditions are applied.
set-top box	End host or device used to receive IPTV video streams.
severity	The designated threat level of an attack: critical, high, medium, low, or informational. Attack objects use the severity setting that matches the potential threat level of a detected attack.
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.
	• switch fabric module. A module that works with the SFP module to create a shared memory fabric for the E320 router.
SFP	small form-factor pluggable transceiver. Provides support for optical or copper cables. SFPs are hot-insertable and hot-removable. *See also* XFP.
SGSN	Serving GPRS Support Node. Device in the mobile network that requests PDP contexts with a GGSN.
SHA-1	Secure Hash Algorithm 1. Secure hash algorithm standard defined in FIPS PUB 180-1 (SHA-1). Developed by the National Institute of Standards and Technology (NIST), SHA-1 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. *See also* 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. *See also* traffic shaping.
shared IP interface	Allocation of separate pools of shared resources to subsets of logical interfaces belonging to the same physical port. One of a group of IP interfaces that are created over the same layer 2 logical interface, which enables multiple IP interfaces to share the same logical resources.
shared local address pool	Group of available addresses that enables a local address server to distribute addresses allocated from DHCP local server address pools within the same virtual router. The addresses are configured and managed within DHCP; therefore, thresholds are not configured on the shared pool, but are instead managed by the referenced DHCP local server pool. A shared local address pool references one DHCP address pool, and can then obtain addresses from the referenced DHCP address pool and from any DHCP address pools that are linked to the referenced DHCP address pool.
shared object	Object that can be shared across domains.
shared scheduling and shaping	Allocation of separate pools of shared resources to subsets of logical interfaces belonging to the same physical port.

shared shaper constituent	Multicast forwarding tree established from the rendezvous point (RP) to the last-hop router for a particular group address.
shared shaping	Mechanism that enables dynamic sharing of logical interface bandwidth for traffic that is queued through separate scheduler hierarchies. *Also called* shared rate shaping. *See also* compound shared shaping, simple shared shaping.
shared tunnel-server module	Module that supports dynamic tunnel-server ports. It provides both tunnel services and regular access services.
SHDSL	symmetric high-speed digital subscriber line. 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 ANSI T1E1.4/2001-174 G.SHDSL. *See also* G.SHDSL.
SHDSL transceiver unit—central office	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.
SHDSL transceiver unit—remote	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.
shim header	Location of the MPLS header in a data packet. The Junos OS always places (shims) the header between the existing Layer 2 and Layer 3 headers.
short frame	Contains less than 64 bytes of data.
short message service	SMS. GSM service that enables short text messages to be sent to and from mobile telephones.
short pipe model	*Also called* pipe (and short-pipe) model. Tunneling model whereby any traffic conditioning (in a pure JunosE environment, a change in traffic class/color combination) that is applied when traffic goes through the tunnel has no effect on the EXP bits coding in the inner header. That is, when traffic exits an LSP (when a label is popped) or when traffic enters an LSP, the inner header's EXP bits coding is not changed. The pipe and short-pipe models differ in the header that the tunnel egress uses when it determines the PHB of an incoming packet. With the short-pipe model, the tunnel egress uses an inner header used for forwarding. With the pipe model, the outermost label is always used. Because of this, you cannot use PHP with the pipe model. *See also* uniform model.
shortest path first	SPF. Algorithm used by IS-IS and OSPF to make routing decisions based on the state of network links. *Also called* the Dijkstra algorithm.
shortest-path tree	SPT. Algorithm that builds a network topology that attempts to minimize the path from one router (the root) to other routers in a routing area.

SIB	Switch Interface Board. On a T640 routing node, provides the switching function to the destination Packet Forwarding Engine.
SIBR	Source Interface Based Routing. Method of allowing the security device to forward traffic based on the source interface (the interface on which the data packet arrives on the security device).
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.
signaled secure IP interface	Negotiates an SA on demand with the remote security gateway. The remote security gateway must also support SA negotiation; otherwise, the gateway drops traffic. The router keeps statistics for dropped traffic. *See also* manual secure IP interfaces.
signaling message	Any GTP-PDU except the G-PDU. GTP signalling messages are exchanged between GSN pairs in a path. The signaling messages are used to transfer GSN capability information between GSN pairs and to create, update, and delete GTP tunnels.
Signaling System 7	SS7. Protocol used in telecommunications for delivering calls and services.
SIM	subscriber identity module. Detachable smart card on the GSM HSDPA 3G wireless modem and other mobile devices that stores configuration and subscriber information for the device.
simple authentication	Authentication method in IS-IS that uses a text password (authentication key) that can be entered in encrypted or unencrypted form. The receiving router uses this authentication key to verify the packet.
Simple Certificate Enrollment Protocol	SCEP. 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.
simple explicit shared shaper	One of four types of shared shapers, in which the weight and priority attributes of the shared-shaping-constituent command are ignored, because the simple shared shaper does not allocate bandwidth among constituents. Instead it controls just the best-effort queue or node. *See also* compound explicit shared shaper, compound implicit shared shaper, simple implicit shared shaper.
simple implicit shared shaper	One of four types of shared shapers, in which constituents are best-effort nodes or queues, and all nodes and queues in named traffic-class groups. *See also* compound explicit shared shaper, compound implicit shared shaper, simple explicit shared shaper.
Simple Network Management Protocol	SNMP. Grotocol governs network management and the monitoring of network devices and their functions.
simple shared shaping	Software-assisted mechanism that measures the rate of active constituents, and can shape the best-effort node or queue associated with a logical interface to a shared rate. *See also* compound shared shaping, shared shaping.

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. *See also* MMF.
SIP	Session Initiation Protocol. 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.
SLA	service level agreement. Formal agreement between a service provider and its customers (as part of a networking service contract) to provide a certain level of service, usually a level of performance.
SLARP	Serial Line Address Resolution Protocol. Simple control protocol provided by the Cisco High-Level Data Link Control implementation that maintains serial link keepalives. *See also* Cisco HDLC.
sleep	Feature of SSH that prevents a user who has exceeded the authentication retry limit from connecting from the same host within the specified period.
SLM	service line module. Tunnel-service line module that does not pair with a corresponding I/O module that provides ingress and egress ports. Receives data from and transmits data to line modules that have ingress and egress ports.
slot group	Group of adjacent chassis (module) slots. The number of slots and number of slots per group depend on the system.
SLS	standard local survivability. Configurable software feature that enables a TGM550 to provide limited MGC functionality when no link is available to a registered MGC.
small computer system interface	SCSI. A standard interface and command set for transferring data between devices over a computer bus.
small form-factor pluggable transceiver	SFP. Provides support for optical or copper cables. SFPs are hot-insertable and hot-removable. *See also* XFP.
small outline dual inline memory module	SODIMM. Memory module that is approximately half the size of a standard DIMM.
smart keepalive	*Also known as* high-density keepalive. Mode whereby, when the keepalive timer expires, the interface first verifies whether any frames were received from the peer in the prior keepalive timeout interval. If so, the interface does not send an LCP echo request (keepalive). Keepalive packets are sent only if the peer is silent (if no traffic was received from the peer during the previous keepalive timeout interval). *See also* low-density keepalive mode.

SMDS	Switched Multimegabit Data Service. Connectionless, wide-area networking service designed for LAN interconnection. An SMDS network is composed of a series of SMDS switches inside a service provider's network, a series of channel service units/data service units (CSUs/DSUs) that connect subscribers to the network, and routers and gateways to connect to each CSU/DSU.
SMS	short message service. 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. Protocol governs network management and the monitoring of network devices and their functions.
SNMP agent	Managed device, such as a router, that collects and stores management information. The SNMP agent (SNMPv3) recognizes up to 32 usernames that can have one of the following security levels: no authentication and no privacy, authentication only, authentication and privacy.
SNMP client	Device that executes management applications that monitor and control network elements. Sometimes called a network management station (NMS) or simply a manager. The SNMP client runs on a network host and communicates with one or more SNMP servers on other network devices, such as routers, to configure and monitor the operation of those network devices.
SNMP community	Logical group of SNMP-managed devices and clients in the same administrative domain.
SNMP community name	Name that acts as a password and is used to authenticate messages sent between an SNMP client and a router containing an SNMP server. The community name is sent in every packet between the client and the server.
SNMP event	Condition or state change that might cause the generation of a trap message.
SNMP group	Set of users with the same access privileges to the router. Three predefined groups are available: admin, public, and private. Applies to SNMPv3.
SNMP managed object	Characteristic of something that can be managed, such as a list of currently active TCP circuits in a device.
SNMP MIB	Tree-structured schema that specifies the format of managed data for a device function. The goal of a MIB is to provide a common and consistent management representation for that function across networking devices. E Series routers support both standard and enterprise SNMP MIBs. *See also* enterprise MIB, standard MIB.
SNMP notification	Message that indicates a status change (equivalent to a trap in SNMPv1). Applies to SNMPv3.

SNMP privilege level	MIB access level that allows increasing levels of privilege:

- Read-only—Read-only access to the entire MIB except for SNMP configuration objects.

- Read-write—Read-write access to the entire MIB except for SNMP configuration objects.

- Admin—Read-write access to the entire MIB.

SNMP secure packet mirroring trap	Type of SNMP trap that enables the administrator to capture and report packet mirroring information to an external device. The secure information can then be viewed on the remote device. *See also* packet mirroring.
SNMP server	Managed device, such as a router, that collects and stores management information. The SNMP server operates on a network device, such as a router, a switch, or a workstation. It responds to SNMP requests received from SNMP clients and generates trap messages to alert the clients about notable state changes in the network device. *See also* SNMP client.
SNMP Server Event Manager	Application that works in conjunction with the Event MIB (RFC 2981) to allow many management functions such as fault detection, configuration management, accounting management, and performance management. These functions are traditionally performed by the network management station (NMS). However, by using the SNMP Server Event Manager, you can distribute some of these functions to E Series routers and automate them. *See also* Event MIB.
SNMP trap	Message sent by an SNMP server to a client to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached. Managed devices use traps to asynchronously report certain events to clients. *See also* SNMP server.
SNMP trap severity level	Each SNMP trap message is assigned a severity level. From most severe to least severe, the trap severity levels are: Emergency, Alert, Critical, Warning, and Notice. *See also* SNMP server.
SNMP user	Person who accesses the router. The router can provide authentication and privacy for the user through SNMPv3. Each user is associated with a group. Applies to SNMPv3.
SNMP view	Management information that is available to the user: read, write, or notification. Three predefined views are available for each group:

- Everything—Includes all MIBs associated with the router.

- User—Includes all MIBs associated with the router, except standard and enterprise MIBs used to configure SNMP operation.

- Nothing—Excludes all MIBs.

SNTP	Simple Network Time Protocol. Adaptation of the Network Time Protocol (NTP) used to synchronize computer clocks in the Internet. SNTP can be used when the ultimate performance of the full NTP implementation described in RFC 1305 is not needed or justified. When operating with current and previous NTP and SNTP versions, SNTP version 4 involves a clarification of certain design features of NTP that allow operation in a simple, stateless remote-procedure call (RPC) mode with accuracy and reliability expectations similar to the UDP/TIME protocol described in RFC 868, *Time Protocol.*

SOC	System On Chip. Integration of all required components of a device into a single integrated chip.
SODIMM	small outline dual inline memory module. Memory module that is approximately half the size of a standard DIMM.
soft reconfiguration	Method used to reapply inbound policies to stored BGP routes without clearing the BGP sessions and therefore disrupting the network.
soft state	In RSVP, control state in hosts and routers that expires if not refreshed within a specified amount of time.
solid-state drive	SSD. Storage device that uses solid-state memory to store persistent data.
SONET	Synchronous Optical Network. 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. *See also* SDH.
SONET Clock Generator	SCG. On a T640 routing node, provides the Stratum 3 clock signal for the SONET/SDH interfaces. Also provides external clock inputs.
source class usage	SCU. 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.
Source Interface Based Routing	SIBR. Method of allowing the security device to forward traffic based on the source interface (the interface on which the data packet arrives on the security device).
source route	An option in the IP header. An attacker can use the source route option to enter a network with a false IP address and have data sent back to the attacker's real address.
source service access point	SSAP. Device that identifies the origin of an LPDU on a DLSw network.
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	SSM. 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.
Spanning Tree Protocol	STP. 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.

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. Routers running sparse mode protocols forward multicast traffic only when explicitly requested to do so. *See also* dense mode.

SPD
security policy database. Ordered list of policy entries that specifies what services are to be offered to IP datagrams and in what fashion. The SPD must discriminate between traffic that has IPsec protection and traffic that is allowed to bypass IPsec. This applies to the IPsec protection to be applied by a sender and that must be present at the receiver. The SPD requires distinct entries for inbound and outbound traffic. For any outbound or inbound datagram, three processing choices are possible: discard, bypass IPsec, or apply IPsec.

SPF
shortest path first. Algorithm used by IS-IS and OSPF to make routing decisions based on the state of network links. *Also called* the Dijkstra algorithm.

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. When enabled, each router does not advertise routes back to the neighbor from which the information originated.

spoof checking
MPLS forwarding table behavior, whereby MPLS determines that an MPLS packet received from an upstream neighbor does not contain an MPLS label that was advertised to that neighbor. The packet is dropped. MPLS supports the following types of spoof checking:

- Router spoof checking—MPLS packets are accepted only if they arrive on an MPLS major interface that is in the same virtual router as the MPLS forwarding table.

- Interface spoof checking—MPLS packets are accepted only if they arrive on the particular MPLS major interface identified in the spoof check field.

SPQ
strict-priority queuing. 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. *See also* APQ.

SPT
shortest-path tree. 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.

SRE   Services and Routing Engine. SRX mid-range services gateway module that provides processing power for security services, routing protocol processes, and other software processes that control the services gateway interfaces, some of the chassis components, system management, and user access to the device.

SRP   switch route processor. ERX router module that performs system management, routing table calculations and maintenance, forwarding table computations, statistics processing, configuration storage, and other control plane functions.

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. 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.

SSD   solid-state drive. Storage device that uses solid-state memory to store persistent data.

SSH   Secure Shell. 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 timeout   Maximum time allowed for a user to be authenticated, starting from the receipt of the first SSH protocol packet.

SSL   Secure Sockets Layer. 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.

SSL certificate   Secure electronic identifier conforming to the X.509 standard, definitively identifying an individual, system, company, or organization. In addition to identification data, the digital certificate contains a serial number, a copy of the certificate holder's public key, the identity and digital signature of the issuing certificate authority (CA), and an expiration date.

SSM   source-specific multicast. 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.
	• Secure Server Protocol. Modified version of TCP that is more reliable than ordinary TCP, requires less CPU and memory resources from servers, and reduces the number of acknowledgement packets on the network. SSP uses AES encryption and SH1 authentication for all connections. NSM uses SSP for communication between the UI, the GUI Server, and the Device Server.
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.
stacked virtual local area network	S-VLAN, stacked VLAN, service VLAN, or switched VLAN. Provides a two-level VLAN tag structure, with a specific service instance VLAN identifier carried inside the S-TAG field. Creating an S-VLAN requires the use of a second encapsulation tag; the router performs decapsulation twice, once to get the S-VLAN tag and once to get the VLAN tag. This double tagging approach enables more than 16 million address possibilities, extending the VLAN ID space to more than 16 million VLANs. This meets and exceeds the scaling requirement for Ethernet B-RAS applications. Defined by IEEE 802.1ad, an S-VLAN often corresponds to a network aggregation device such as a DSLAM. Scheduling and shaping is often established for an S-VLAN to provide CoS for downstream devices with little buffering and simple schedulers. *See also* B-VID, C-VLAN.
stacked VLAN	S-VLAN, service VLAN, or switched VLAN. Provides a two-level VLAN tag structure, with a specific service instance VLAN identifier carried inside the S-TAG field. Creating an S-VLAN requires the use of a second encapsulation tag; the router performs decapsulation twice, once to get the S-VLAN tag and once to get the VLAN tag. This double tagging approach enables more than 16 million address possibilities, extending the VLAN ID space to more than 16 million VLANs. This meets and exceeds the scaling requirement for Ethernet B-RAS applications. Defined by IEEE 802.1ad, an S-VLAN often corresponds to a network aggregation device such as a DSLAM. Scheduling and shaping is often established for an S-VLAN to provide CoS for downstream devices with little buffering and simple schedulers. *See also* B-VID, C-VLAN.
standalone mode	DHCP standalone mode. Mode in which the DHCP local server operates as a basic DHCP server. Clients are not authenticated by default; however, you can optionally configure the DHCP local server to use AAA authentication for the incoming clients.
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. *See also* AAL5 mode, cell-relay mode, Layer 2 circuits, trunk mode.
standard local survivability	SLS. Configurable software feature that enables a TGM550 to provide limited MGC functionality when no link is available to a registered MGC.
standard MIB	MIB defined by a body such as the IETF that fosters consistency of management data representation across many vendors' networking products.

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 access control	Method to address firewall issues; stateful access control guards a network by allowing traffic only in the trusted direction. After a firewall for a protocol is configured, all packets that belong to those applications, that use that protocol, are subject to stateful monitoring.
stateful firewall	Type of firewall created by a 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. *See also* stateful firewall filter, 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. *See also* stateless firewall filter.
stateful firewall recovery	Recovery strategy that preserves parameters concerning the history of connections, sessions, or application status before failure. *See also* stateless firewall recovery.
stateful inspection	Firewall process that checks the TCP header for information about the session's state. The process checks whether it is initializing (SYN), ongoing (SYN/ACK), or terminating (FIN). A stateful inspection firewall tracks each session flowing through it, dropping packets from unknown sessions that appear to be part of ongoing or illegal sessions. All security devices are stateful inspectors.
stateful signature	A signature is any distinctive characteristic that identifies something. A stateful signature knows the pattern it is attempting to find and where to look for that pattern. Stateful signatures produce very few false positives because they understand the context of the attack and can eliminate huge sections of network traffic they know the attack would not be in.
stateful signature detection	Method of attack detection that uses stateful signatures. Stateful signatures are much smarter than regular signatures: they know the protocol or service used to perpetrate the attack, the direction and flow of the attack, and the context in which the attack occurs.
stateful SRP switchover	Ensures rapid SRP module recovery following a switchover. *Also known as* high availability mode. Stateful SRP switchover uses an initial bulk file transfer and subsequent, transaction-based mirroring. In addition to keeping the contents of NVS, stateful SRP switchover keeps state and dynamic configuration data from the SRP memory synchronized between the primary and standby SRP modules.
stateless access control	Method to address firewall issues. You can use the E Series policy manager to provide solutions to access problems, such as address spoofing. E Series routers automatically provide some stateless checks as part of their normal forwarding feature set.

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. *See also* stateful firewall filter.
stateless firewall recovery	Recovery strategy that does not attempt to preserve the history of connections, sessions, or application status before failure. *See also* stateful firewall recovery.
static interface	Created through an existing configuration mechanism such as the command-line interface (CLI) or Simple Network Management Protocol (SNMP). *See also* dynamic interface.
static LSP	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 path.
static oversubscription	Process that enables the router to vary queue thresholds based on the number of queues currently configured, which is relatively static. *See also* bandwidth oversubscription, dynamic oversubscription.
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, requiring packets to use the specified path. 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.
static translation	One of two NAT methods used to assign a translated IP address. Establishes a one-to-one mapping between a local and global address. Entered as a direct configuration setting that remains in the translation table until it is removed. Used when you must initiate connections from both the inside and outside interfaces or when the translation is not subject to change. *See also* dynamic translation.
static tunnel-server port	Virtual port that is always present on dedicated tunnel-server modules. No explicit configuration is required for this type of port.
statistics baseline	Starting point for statistics collection after resetting protocol or application statistics and counters to zero.
statistics profile	Template that specifies rate statistics and event-gathering characteristics. A statistics profile enables you to gather statistics for the rate at which packets are forwarded out of a queue and for the rate at which committed, conformed, or exceeded packets are dropped. Statistics profiles also enable you to use events to monitor the rate statistics.

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.
streaming	Playing a digital media file while it is still being downloaded; letting a user view and hear digitized content as it is being downloaded.
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; a next hop defined by the ingress node that is connected to the previous node in the path. *See also* loose hop.
strict-priority queuing	SPQ. 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. *See also* APQ.
strict-priority scheduling	Process that designates the traffic class (queue) that receives top priority for transmission of its packets through a port. It is implemented with a special strict-priority scheduler node that is stacked directly above the port.
strict-source routing	MPLS routing mechanism that specifies every hop that the packet must traverse. The specified path consists of adjacent hops.
structured query language	SQL. International standard language used to create, modify, and select data from relational databases.
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. *See also* 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	Area that does not get flooded with external link-state advertisements (LSAs) but does carry intra-area and interarea routes and a default route. *See also* NSSA.

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. *See also* P2MP LSP.
subchannel	Group of T1 timeslots. Subchannel numbers are in the range 1–24 but do not necessarily correspond to DS0 timeslots. The subchannel number identifies a fractional T1 channel.
subdomain	Section of a domain that is still a part of the larger whole domain.
subinterface	Mechanism that allows a single physical interface to support multiple logical interfaces or networks. Each subinterface borrows the bandwidth it needs from the physical interface with which it is associated. Configuring multiple virtual interfaces, or subinterfaces, on a single physical interface provides greater flexibility and connectivity on the network.
subnet addressing	Type of addressing used in IP addresses. A subset of a class A, B, or C network. Subnets cannot be used with class D (multicast) addresses. *See also* IP address classes.
subnet mask	Number of bits of the network address used to separate the network information from the host information in a Class A, Class B, or Class C IP address, allowing the creation of subnetworks. In binary notation, a series of 1s followed by a series of contiguous 0s. The 1s represent the network number; the 0s represent the host number. Use of masks can divide networks into subnetworks by extending the network portion of the address into the host portion. Subnetting increases the number of subnetworks and reduces the number of hosts.
subnetwork	Logical division of a LAN created to enhance performance and provide security.
subrate value	Value that reduces the maximum allowable peak rate by limiting the HDLC-encapsulated payload. The subrate value must exactly match that of the remote channel service unit (CSU).
subscriber (client) bridge interface	Type of bridge interface where the traffic flow direction is downstream—from the server (trunk) to the client (subscriber). *See also* trunk (server) bridge interface.
subscriber identity module	SIM. Detachable smart card on the GSM HSDPA 3G wireless modem and other mobile devices that stores configuration and subscriber information for the device.
subscriber interfaces	Extension of a shared IP interface. Subscriber interfaces are bidirectional—they can both receive and transmit traffic, in contrast to shared IP interfaces, which are unidirectional—they can transmit but not receive traffic.
subscriber policy	Set of forwarding and filtering rules that defines how to handle various packet or attribute types.
subsequent address family identifier	SAFI. Number that further identifies an address family identified by an AFI. In an MP-BGP update message, SAFI is used with AFI to identify the network layer protocol associated with the network address of the next hop and the semantics of the NLRI that follows. *See also* AFI.
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.

super administrator	Root user, or manager, of the system. The super administrator role has unrestricted authority to access and modify most of the system, and is the default administrator for all domains.
supplicant	The client in an 802.1X-authenticated network.
sustained cell rate	SCR. Upper bound on the conforming average rate of an ATM connection over a sustained time interval that is longer than the time interval for which the PCR is defined.
SVC	switched virtual connection (or circuit). 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. SVCs are used in situations where data transmission is sporadic. *See also* PVC, permanent virtual connection.
switch	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. *See also* bridge.
switch fabric module	SFM. A module that works with the SFP module to create a shared memory fabric for the E320 router.
Switch Interface Board	SIB. On a T640 routing node, provides the switching function to the destination Packet Forwarding Engine.
switch route processor	SRP. ERX router module that performs system management, routing table calculations and maintenance, forwarding table computations, statistics processing, configuration storage, and other control plane functions.
switch-card chassis	SCC. Term used by the Junos OS command-line interface (CLI) to refer to the TX Matrix platform in a routing matrix.
Switch-to-Switch Protocol	SSP. Protocol implemented between two DLSw routers that establishes connections, locates resources, forwards data, and handles error recovery and flow control.
Switched Multimegabit Data Service	SMDS. Connectionless, wide-area networking service designed for LAN interconnection. An SMDS network is composed of a series of SMDS switches inside a service provider's network, a series of channel service units/data service units (CSUs/DSUs) that connect subscribers to the network, and routers and gateways to connect to each CSU/DSU.
switched virtual circuit, switched virtual connection	SVC. 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. SVCs are used in situations where data transmission is sporadic. *See also* PVC, permanent virtual connection.

switched VLAN S-VLAN, stacked VLAN, or service VLAN. Provides a two-level VLAN tag structure, with a specific service instance VLAN identifier carried inside the S-TAG field. Creating an S-VLAN requires the use of a second encapsulation tag; the router performs decapsulation twice, once to get the S-VLAN tag and once to get the VLAN tag. This double tagging approach enables more than 16 million address possibilities, extending the VLAN ID space to more than 16 million VLANs. This meets and exceeds the scaling requirement for Ethernet B-RAS applications. Defined by IEEE 802.1ad, an S-VLAN often corresponds to a network aggregation device such as a DSLAM. Scheduling and shaping is often established for an S-VLAN to provide CoS for downstream devices with little buffering and simple schedulers. *See also* B-VID, C-VLAN.

Switching and Forwarding Module SFM. On an M160 router, a component of the Packet Forwarding Engine that provides route lookup, filtering, and switching to FPCs.

switchover In a redundant configuration, the process by which the router switches to the spare line module. During switchover, the line, circuit, and IP interfaces on the I/O module or IOAs appear to fail temporarily. The duration of the downtime depends on the number of interfaces and the size of the routing table, because the router must reload the interface configuration and the routing table from the SRP module. *See also* high availability mode.

symmetric digital subscriber line SDSL. Version of digital subscriber line (DSL) where the upload speeds and download speeds are the same, typically in the range 144 Kbps–1.5 Mbps. SDSL uses one cable pair and does not share lines with analog phones.

symmetric high-speed digital subscriber line SHDSL. 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 ANSI T1E1.4/2001-174 G.SHDSL. *See also* G.SHDSL.

SYN TCP flag indicating the use of a synchronization packet when set to 1.

SYN attack Denial-of-service attack in which SYN packets overwhelm a network by initiating so many connection attempts or information requests that the network can no longer process legitimate connection requests.

synchronization	• Process that prevents a redundant NVS card from overwriting saved files on the primary NVS card if the primary SRP module fails and the redundant SRP module takes control. *See also* file system synchronization mode.
	• Mechanism for ensuring that a BGP speaker does not advertise routes to its EBGP peers before all the BGP routes have been redistributed into all routers within its AS that are running an IGP and are not running BGP. When BGP is not synchronized with the IGPs, the IGP routers cannot forward all traffic received from another AS. The BGP speaker cannot propagate a BGP route that it learned from a peer until an IGP route to the prefix has been installed in the BGP speaker's IP routing table.
	• Method that NTP uses to ensure accurate time. There are three stages to synchronization:
	• Preliminary synchronizationThe system evaluates the initial time situation and decides how to proceed with longer-term synchronization.
	• Frequency calibration--Takes place the first time you use NTP or when you reboot the system. During this stage, the system evaluates the frequency error of its clock by measuring change in the offset error. A frequency calibration takes 15 minutes.
	• Progressive synchronizationThe system continues to synchronize to a server after establishing initial NTP parameters.
Synchronous Digital Hierarchy	SDH. International standard defined by the International Telecommunication Union for transmitting bits over fiber-optic cable. A CCITT variation of the SONET standard.
synchronous dynamic random access memory	SDRAM. 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. A type of RAM that is stored on dual in-line memory modules (DIMMs) and synchronized with the system clock.
Synchronous Optical Network	SONET. 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. *See also* SDH.
synchronous static random access memory	SSRAM. 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.
synchronous transport module	STM. CCITT specification for SONET at 155.52 Mbps.
synchronous transport signal	STS. 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. *See also* SONET.
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. Method for sending and storing messages to a log 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 alarm	Predefined alarm triggered by a missing rescue configuration or by a lack of an installed license for a licensed software feature.
System and Switch Board	SSB. On an M20 router, a Packet Forwarding Engine component that performs route lookups and component monitoring and monitors FPC operation.
System Control Board	SCB. On an M40 router, the part of the Packet Forwarding Engine that performs route lookups, monitors system components, and controls FPC resets.
system controller	SC. Subsystem located on the SRP modules on the E320 router that controls the overall operations on the router.
system events	System changes that can be classified into log event categories and that can be used for tracking purposes.
system ID	sysid. Portion of the ISO nonclient peer. The system ID can be any 6 bytes that are unique throughout a domain.
system log	syslog. Method for sending and storing messages to a log 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 Network Architecture	SNA. IBM proprietary networking architecture consisting of a protocol stack that is used primarily in banks and other financial transaction networks.
System On Chip	SOC. Integration of all required components of a device into a single integrated chip.
system reference point/terminal reference point interface	S/T interface. A four-pair connection between the ISDN provider service and the customer terminal equipment.

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.
T-PDU	Transport Protocol Data Unit. Payload that is tunneled in the GTP tunnel.
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.
table map	Mechanism for applying a route map to an IS-IS route as a way to filter and manipulate route attributes before the route is added to the routing table. Issuing the JunosE table-map command (in Router Configuration mode) applies a specified route map as a policy filter on the route before it is installed in the routing table.

TACACS	Terminal Access Controller Access Control System. A security protocol that provides centralized validation of users who are attempting to gain access to a router or NAS.
TACACS+	Terminal Access Controller Access Control System Plus. An authentication method of providing access control for routers, network access servers, and other networked computing devices using one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting services. It is based on TACACS. However, it is an entirely new protocol.
TACACS+ accounting service	Service that enables the creation of an audit trail of User Exec sessions and command-line interface (CLI) commands that have been executed within these sessions. For example, you can track user CLI connects and disconnects, when configuration modes have been entered and exited, and which configuration and operational commands have been executed.
TACACS+ host	Security server on which the TACACS+ process is running. *Also called* a TACACS+ server.
TACACS+ process	Program or software running on a security server that provides AAA services using the TACACS+ protocol. The program processes authentication, authorization, and accounting requests from an NAS. When processing authentication requests, the process might respond to the NAS with a request for additional information, such as a password.
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. *See also* RED.
TCC	translational cross-connect. Switching concept that allows you to establish interconnections between a variety of Data Link Layer (Layer 2) protocols or circuits.
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 OS currently supports two-rate TCM only. *See also* trTCM.
TCP	Transmission Control Protocol. Works in conjunction with the Internet Protocol (IP) to send data over the Internet, creating connections between hosts for the exchange of data. Divides a message into packets and tracks the packets from point of origin to destination. Guarantees that packets are transmitted in their original sequence from sender to receiver.
TCP port 179	Well-known port number used by BGP to establish a peering session with a neighbor.
TCP scan	Attack method that attempts to connect to every TCP port on a single machine, to provide attackers with information about your network configuration.
TCP/IP	Transmission Control Protocol/Internet Protocol. Set of communications protocols that support peer-to-peer connectivity functions for both local and wide area networks. Enables computers with different operating systems to communicate with each other. Controls how data is transferred between computers on the Internet.

tcpdump	• UNIX packet monitoring utility used by the Junos OS to view information about packets sent or received by the Routing Engine. • In IDP Series, a BSD utility used to capture TCP/IP packets.
TDM	time-division multiplexing. A form of multiplexing that divides a transmission channel into successive time slots.
TDMA	Time-Division Multiple Access. 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. *See also* GSM.
TE	traffic engineering. Ability to control the path taken through a network or portion of a network based on a set of traffic parameters (bandwidth, QoS parameters, and so on). Traffic engineering enables performance optimization of operational networks and their resources. *See also* MPLS traffic engineering, RSVP-TE.
tear drop attack	If the first and second parts of a fragmented packet overlap, the server attempting to reassemble the packet can crash. If the security device sees this discrepancy in a fragmented packet, it drops the packet.
TEI	Terminal Endpoint Identifier. 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.
TEID	Tunnel Endpoint Identifier. Uniquely identifies a tunnel endpoint in the receiving GTP-U or GTP-C protocol entity. The receiving end of a GTP tunnel locally assigns the TEID value for the transmitting end.
template	Configuration that is defined once and then can be used for other device configurations. You can specify most device configuration values in a template, and you can specify only those configuration parameters that you want to set. You do not need to specify a complete device configuration.
Terminal Access Controller Access Control System (Plus)	TACACS, TACACS+. An authentication method of providing access control for routers, network access servers, and other networked computing devices using one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting services. It is based on TACACS. However, it is an entirely new protocol.
Terminal Endpoint Identifier	TEI. 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.
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.
test interval	Time, in seconds, between RPM tests.
TFTP	Trivial File Transfer Protocol. An Internet software utility that is simpler to use than the File Transfer Protocol (FTP) but less capable. TFTP does not support any security features, so it is used where user authentication and directory visibility are not required. TFTP uses the User Datagram Protocol (UDP) rather than the Transmission Control Protocol (TCP) to transfer small files on a network.
TGM550	Avaya H.248 Telephony Gateway Module for VoIP, it is installed in a Services Router along with one or more Telephony Interface Modules (TIMs) to connect VoIP and legacy analog telephones and trunks over IP networks. Only the TGM550 has an interface configurable through the J-Web interface or Junos OS CLI. The TIMs are configured and administered from the TGM550 CLI.
Third-Generation Partnership Project	3GPP. Created to expedite the development of open, globally accepted technical specifications for the Universal Mobile Telecommunications System (UMTS).
through	Junos OS routing policy match type representing all routes that fall between the two supplied prefixes in the route filter.
TID	tunnel identifier. Uniquely identifies a particular tunnel or tunnel group.
TIM510	Avaya E1/T1 Telephony Interface Module for VoIP, it is installed in a Services Router to provide an E1 or T1 trunk connection over the Internet to a telephone central office (CO). A TIM510 is configured and administered from a TGM550 installed in the same router.
TIM514	Avaya Analog Telephony Interface Module for VoIP, it is installed in a Services Router to connect individual telephones or trunk lines to the Internet. A TIM514 is configured and administered from a TGM550 installed in the same router.
TIM521	Avaya BRI Telephony Interface Module for VoIP, it is installed in a Services Router to connect ISDN Basic Rate Interface (BRI) trunk lines to a telephone central office (CO) over the Internet for data or voice transmission. A TIM521 is configured and administered from a TGM550 installed in the same router.
time to live	TTL. Value (octet) in the IP header that is (usually) decremented by 1 for each hop the packet passes through. If the field reaches zero, the packet is discarded, and a corresponding error message is sent to the source of the packet.
Time-Division Multiple Access	TDMA. 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. *See also* GSM.

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.
time-division multiplexing	TDM. A form of multiplexing that divides a transmission channel into successive time slots.
timeout timer	Used in a distance-vector protocol to ensure that the current route is still usable for forwarding traffic.
TLS	Transport Layer Security. Protocol that ensures privacy between communicating applications and their users on the Internet by blocking any third party from eavesdropping or message tampering. In NSM, it is used to provide secure communication between the NSM UI and the NSM GUI server.
TLV	type-length-value. An element inside a data communications protocol used to encode optional information. These fields are used as follows:

- Type—A 1-4 byte numeric code that indicates the kind of field that this part of the message represents.

- Length—A 1-4 byte field that denotes the size of the value field, typically in bytes.

- Value—A variable-sized set of bytes that contains the data for this part of the message.

TN power system	Power distribution system that has one point connected directly to earth (ground), usually the star point in a three-phase system. The exposed conductive parts of the installation are connected to that point by protective earth conductors.
TNP	Trivial Network Protocol. Juniper Networks proprietary protocol automatically configured on an internal interface by the Junos OS. 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. 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. However, type 3 LSAs carrying default route information alone are injected into the area. *See also* NSSA, stub area.
traditional NAT	Common method of using network address translation (NAT). Primary use is translating private addresses to legal addresses for use in an external network. There are two types of traditional NAT: basic NAT and NAPT. *See also* basic NAT, NAPT.
traffic class	Chassis-wide collection of buffers, queues, and bandwidth that can be allocated to provide a defined level of service to packets in the traffic class for JunosE QoS.

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** .) *See also* TE, 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. *See also* 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. *See also* shaping rate.
traffic-class group	Separate hierarchy of scheduler nodes and queues over a port. Traffic classes belong to the default group unless they are specifically assigned to a named group. Organizing traffic into multiple traffic-class groups enables you to manage and shape traffic—by service class, for example—when the traffic classes are distributed across different virtual circuits. The router supports up to four traffic-class groups. A traffic class cannot belong to more than one group.
traffic-control profile	Defines the characteristics of a scheduler node, as used at several levels of the CLI, including the physical interface, the interface set, and the logical interface. Scheduling and queuing characteristics are defined for the scheduler node using the shaping-rate, guaranteed-rate, and delay-buffer-rate statements. Queues over these scheduler nodes are defined by referencing a scheduler map. *See also* schedulers and scheduler maps.
transform sets	Sets composed of security parameters that provide a required security level to a particular data flow. Transform sets are used during user SA negotiation to find common agreement between the local and the remote security gateway on how to protect that specific data flow. A transform set includes encapsulation protocols and transforms, for example, encryption/decryption/authentication algorithms.
transient black hole	Condition in which a transit router running both IS-IS and BGP drops traffic because not all of the information required to reach some external destinations is yet available.
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. *See also* 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. *See also* FPC, PIC, 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.
translational cross-connect	TCC. Switching concept that allows you to establish interconnections between a variety of Data Link Layer (Layer 2) protocols or circuits.
Transmission Control Protocol	TCP. Works in conjunction with the Internet Protocol (IP) to send data over the Internet, creating connections between hosts for the exchange of data. Divides a message into packets and tracks the packets from point of origin to destination. Guarantees that packets are transmitted in their original sequence from sender to receiver.
Transmission Control Protocol/Internet Protocol	TCP/IP. Set of communications protocols that support peer-to-peer connectivity functions for both local and wide area networks. Enables computers with different operating systems to communicate with each other. Controls how data is transferred between computers on the Internet.
transparent bridge	Data Link Layer (Layer 2) relay device that connects two or more networks or network systems. Transparent bridging is configured when you create one or more bridge groups on an E Series router. *See also* bridge group, bridge group interface.
transport layer	Fourth level in the seven-layer OSI reference model for network protocol design and in the five-layer TCP/IP protocol stack. This layer provides communication between applications residing in different hosts and reliable transparent data transfer between end users. It is the first layer to address reliability.
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. *See also* tunnel mode.
transport plane	Virtual network path used to distribute data between nodes. *Also known as* data plane, control plane.
Transport Protocol Data Unit	T-PDU. Payload that is tunneled in the GTP tunnel.
transport virtual router	For a secure IP tunnel, the VR in which both of the secure tunnel endpoints,—the source and destination—are routable addresses. Normally, the transport VR is the default ISP routing infrastructure on top of which VPNs are provisioned.

trap
SNMP message that reports significant events occurring on a network device, most often errors or failures. SNMP traps are defined in either standard or enterprise-specific MIBs. *See* SNMP trap.

tricolor marking
TCM. 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 OS currently supports two-rate TCM only. *See also* trTCM.

trigger
RADIUS attribute that identifies a user whose traffic is to be mirrored. Packet mirroring starts when a trigger is detected. *See also* packet mirroring.

trigger table (mteTriggerTable)
SNMP term for a table that lists any currently defined trigger conditions. Triggers fall into three categories—existence, Boolean, and threshold. One of three parts of the Event MIB. *See also* event table (mteEventTable), objects table (mteObjectsTable).

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
3DES. A 168-bit encryption algorithm that encrypts data blocks with three different keys in succession, achieving a higher level of encryption than standard DES. Data is encrypted with the first key, decrypted with the second key, and encrypted again with the third key. 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* Triple DES.

triple play
Provisioning of three services (data, voice, and video) over a single broadband connection. *See also* quadruple play.

Trivial File Transfer Protocol
TFTP. An Internet software utility that is simpler to use than the File Transfer Protocol (FTP) but less capable. TFTP does not support any security features, so it is used where user authentication and directory visibility are not required. TFTP uses the User Datagram Protocol (UDP) rather than the Transmission Control Protocol (TCP) to transfer small files on a network.

Trivial Network Protocol
TNP. Juniper Networks proprietary protocol automatically configured on an internal interface by the Junos OS. 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.

trojan
Program with hidden functionality. Trojans often install a remote administration program (known as a backdoor) that enables attackers to access the target system.

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, *A Two Rate Three Color Marker*. *See also* CIR, PIR.

trunk (server) bridge interface
Bridge interface in which the traffic flow direction is upstream—from the client (subscriber) to the server (trunk). *See also* subscriber (client) bridge interface.

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. *See also* AAL5 mode, cell-relay mode, Layer 2 circuits, standard AAL5 mode.
trunk port	Enables a switch to bundle traffic from several VLANs through a single physical port, sorting the various packets by the VLAN identifier (VID) in their frame headers.
trust zone	One of two predefined zones (trust, untrust) that enables packets to be secured from being seen by devices external to your current domain.
trusted network	Internal network (for instance, an intranet) or your personal computer. *See also* untrusted network.
TSM	Tunnel Service Module. Line module that does not pair with a corresponding I/O module that provides ingress and egress ports. A TSM receives data from and transmits data to line modules that have ingress and egress ports.
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.
TTL	time to live. Value (octet) in the IP header that is (usually) decremented by 1 for each hop the packet passes through. If the field reaches zero, the packet is discarded, and a corresponding error message is sent to the source of the packet.
tunnel	Private, secure path through an otherwise public network. More specifically, it is an LSP that is used by an IGP to reach a destination, or an LSP that uses traffic engineering.
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 Endpoint Identifier	TEID. Uniquely identifies a tunnel endpoint in the receiving GTP-U or GTP-C protocol entity. The receiving end of a GTP tunnel locally assigns the TEID value for the transmitting end.
tunnel interface	Opening, or doorway, through which traffic to or from a VPN tunnel passes. It can be numbered (assigned an IP address) or unnumbered. A numbered tunnel interface can be in either a tunnel zone or security zone. An unnumbered tunnel interface can only be in a security zone that contains at least one security zone interface. The unnumbered tunnel interface borrows the IP address from the security zone interface.
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. *See also* transport mode.

Tunnel Service Module	TSM. Line module that does not pair with a corresponding I/O module that provides ingress and egress ports. A TSM receives data from and transmits data to line modules that have ingress and egress ports.
tunnel services interface	Provides the capability of a Tunnel Services PIC on an AS PIC. *See also* 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.
tunnel zone	Logical segment that hosts one or more tunnel interfaces. A tunnel zone is associated with a security zone that acts as its carrier.
tunneling	Transmission of data intended for use only within a private (usually corporate) network through a public network in such a way that the routing nodes in the public network are unaware that the transmission is part of a private network. Tunneling is generally done by encapsulating the private network data and protocol information within the public network transmission units so that the private network protocol information appears to the public network as data. Tunneling allows the use of the Internet, a public network, to convey data on behalf of a private network. With VPN tunneling, remote users can access the entrance to their corporate VPN network using an Internet service provider and the remote users as well as the organization know that it is a secure connection. *Also known as* port forwarding.
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. It is encapsulated for delivery only; no policies can be applied. Tunneling can also be used to provide various types of VPN functionality such as private addressing.
twice NAT	Both the source and destination addresses are subject to translation as packets traverse the NAT router in either direction. *See also* NAT.
two-rate rate-limit profile	Enables the user to build tiered rate-limit services and to specify different treatments for packets at different rates. *See also* one-rate rate-limit profile, rate-limit profile.
two-rate TCM	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, *A Two Rate Three Color Marker*. *See also* CIR, PIR.
TX	Communications abbreviation for transmit; the corresponding abbreviation for receive is TRX.
TX Matrix platform	Routing platform that provides the centralized switching fabric of the routing matrix.
type of service	ToS. Method of handling traffic using information extracted from the fields in the ToS byte to differentiate packet flows.

type-length-value	TLV. An element inside a data communications protocol used to encode optional information. These fields are used as follows:

- Type—A 1-4 byte numeric code that indicates the kind of field that this part of the message represents.
- Length—A 1-4 byte field that denotes the size of the value field, typically in bytes.
- Value—A variable-sized set of bytes that contains the data for this part of the message.

U

U	Unit. Standard of measurement for rack-mounted equipment (a U equals 1.75 in., or 4.44 cm).
U interface	User reference point interface. A single-pair connection between the local ISDN provider and the customer premises equipment.
U-Boot	Computer software that serves as a bootstrap loader in many embedded systems.
UBR	unspecified bit rate. ATM service category that does not specify traffic-related service guarantees. Specifically, UBR does not define a per-connection negotiated bandwidth.
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.
UDP flood	Denial-of-service attack using multiple UDP packets, sent to slow the target system to the point that it can no longer handle valid connections. You can configure the security device with a threshold to invoke UDP flood attack protection. When UDP packet flow exceeds this threshold, the device records the UDP flood attack as a statistic.
UDP scan	Attack method that attempts to connect to every UDP port on a single machine, to provide attackers with information about your network configuration.
UHP	ultimate hop popping. When the egress router advertises the explicit null label or a non-null label to its upstream neighbor. This advertisement, performed by the signaling protocol (either LDP or RSVP-TE) ensures that all MPLS packets traversing the LSP to the egress router include a label. *See also* PHP.
UI	user interface. Program that controls a display for the user (usually on a computer monitor) and that allows the user to interact with the system. *See also* PHP.
ultimate hop popping	UHP. When the egress router advertises the explicit null label or a non-null label to its upstream neighbor. This advertisement, performed by the signaling protocol (either LDP or RSVP-TE) ensures that all MPLS packets traversing the LSP to the egress router include a label. *See also* PHP.
UME	UNI management entity. 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	UTRAN. WCDMA radio network in UMTS.
UNC	Unified National Coarse. Standard used to specify the thread in screws and bolts.
unchannelized interface	Interface that is not fragmented into channels.
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	UME. 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.
unicast	Operation of sending network traffic from one network node to another individual network node.
unicast address	IPv4 and IPv6 user-to-user addressing protocol used to send a datagram to a single recipient.
Unified National Coarse	UNC. Standard used to specify the thread in screws and bolts.
uniform model	Tunneling method that renders MPLS transparent to the differentiated services operation. From the diff-serv perspective, it is as if MPLS is not used. In the uniform model, if traffic conditioning is applied somewhere along the LSP, the EXP bits of the inner header must be changed at the egress when the inner header becomes the outer header (because of the pop of the outer label). *See also* pipe (and short-pipe) model.
Uniform Resource Identifier	URI. Compact string of characters for identifying an abstract or physical resource. Details can be found in RFC 2396 *Uniform Resource Identifiers (URI): Generic Syntax.*
Uniform Resource Locator	URL. Standard method of specifying the location of an available electronic resource. *Also known as* a location or address, a URL specifies the location of files on servers. A general URL has the syntax **protocol://address**. For example, **http://www.example.com/index.html** specifies that the protocol is **http** and the address is **www.example.com/index.html**. Most commonly used as a compact string representation for a resource available over the Internet, as defined in RFC 1738, *Uniform Resource Locators (URL). See also* Uniform Resource Identifier.
uninterruptible power supply	UPS. 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.
Unit	U. Standard of measurement for rack-mounted equipment (a U equals 1.75 in., or 4.44 cm).
unit	Junos OS syntax that represents the logical properties of an interface.

universal mobile telecommunications system	UMTS. Provides third-generation (3G), packet-based transmission of text, digitized voice, video, and multimedia, at data rates up to 2 Mbps.
Universal Unique Identifier	UUID. 128-bit number assigned to any object within a distributed computing environment (DCE) cell which is guaranteed to be unique.
unnumbered interface	Logical interface that is configured without an IP address.
unspecified bit rate	UBR.. ATM service category that does not specify traffic-related service guarantees. Specifically, UBR does not define a per-connection negotiated bandwidth.
untrust zone	One of two predefined zones (trust, untrust) that enables packets to be seen by devices external to your current domain.
untrusted network	External network, such as the Internet. *See also* trusted network.
UOL	Uniform Object Locator. An intuitive, general-purpose identifier that is hierarchical and readable. Details can be found in Internet Draft draft-boynton-uol-00, *Uniform Object Locator—UOL.*
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. 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 OS 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.
URI	Uniform Resource Identifier. Compact string of characters for identifying an abstract or physical resource. Details can be found in RFC 2396 *Uniform Resource Identifiers (URI): Generic Syntax.*
URL	Uniform Resource Locator. Standard method of specifying the location of an available electronic resource. *Also known as* a location or address, a URL specifies the location of files on servers. A general URL has the syntax **protocol://address**. For example, **http://www.example.com/index.html** specifies that the protocol is **http** and the address is **www.example.com/index.html**. Most commonly used as a compact string representation for a resource available over the Internet, as defined in RFC 1738, *Uniform Resource Locators (URL). See also* Uniform Resource Identifier.
user	Person using the network that your security devices are protecting. NSM supports two types of users: local users and external users.
User Datagram Protocol	UDP. 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.

User Exec mode   CLI mode you are in after you log in to the system. By default, the commands you can execute from User Exec mode provide only user-level access. The User Exec commands allow you to perform such functions as changing terminal settings on a temporary basis, performing ping and trace commands, displaying system information, and accessing Global Configuration mode. *See also* Global Configuration mode, Privileged Exec mode, privileged level.

user interface   UI. Program that controls a display for the user (usually on a computer monitor) and that allows the user to interact with the system. *See also* PHP.

user level   Access level in the CLI of E Series routers that enables you to view router status. This level restricts you to User Exec mode.

user object   User objects represent the users of your managed devices. You can include user objects or groups in security policies or VPNs to permit or deny access to individuals or groups.

user-based security model   USM. Method for providing SNMP message-level security using authentication protocols and privacy protocols..

user-to-network interface   UNI. 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.

USM   user-based security model. Method for providing SNMP message-level security using authentication protocols and privacy protocols.

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. WCDMA radio network in UMTS.

V

V.35 interface   Provides synchronous operation between data communication equipment (DCE) and data terminal equipment (DTE) for data communication over the telephone network.

vapor corrosion inhibitor   VCI. Small cylinder packed with the router that prevents corrosion of the chassis and components during shipment.

variable bit rate   VBR. ATM service category that supports variable bit rate data traffic with average and peak traffic parameters. VBR traffic adds the ability to statistically oversubscribe user traffic. The VBR service category has two subcategories: VBR-NRT and VBR-RT.

VBR   variable bit rate. ATM service category that supports variable bit rate data traffic with average and peak traffic parameters. VBR traffic adds the ability to statistically oversubscribe user traffic. The VBR service category has two subcategories: VBR-NRT and VBR-RT.

VBR-NRT	variable bit rate, non-real time. Subcategory of the VBR service category that is used for bursty or other non-time-sensitive transmissions. VBR-NRT guarantees minimum delay and cell loss.
VBR-RT	variable bit rate, real time. Subcategory of the VBR service category that is used for time-sensitive connections such as video or voice. VBR-NRT guarantees minimum delay and cell loss.
VC	virtual circuit.

- 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. *See also* VPI, VCI, PVC, SVC.

- In IDP Series, corresponds with a physical interface.

VCC	virtual channel connection. Uses all the addressing bits of a cell header to move traffic from one link to another. The VCC is formed by joining a series of virtual channels, which are logical circuits uniquely identified for each link of the network.
VCC cell relay encapsulation	Method for the router to emulate ATM switch behavior by forwarding individual ATM cells over an MPLS pseudowire (also referred to as an MPLS tunnel) created between two ATM VCCs, or as part of a local ATM passthrough connection between two ATM 1483 subinterfaces on the same router.
VCD	virtual circuit descriptor. Unique number that identifies a virtual circuit.
VCI	

- vapor corrosion inhibitor. Small cylinder packed with the router that prevents corrosion of the chassis and components during shipment.

- virtual circuit (channel) identifier. 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. *See also* VPI.

VDSL	very-high-bit-rate digital subscriber line. DSL technology providing faster data transmission over short distances, usually between 1000 and 4500 feet (300 and 1500 meters), of twisted pair copper wire. The shorter the distance, the faster the connection rate.
VDSL2	Enhancement to ITU-T G.993.1 standard VDSL that permits the transmission of asymmetric and symmetric (full duplex) aggregate data at a faster rate.
VE router	VPLS edge device. Router that is analogous to a provider edge (PE) router in a BGP/MPLS VPN configuration, and performs similar functions.
very-high-bit-rate digital subscriber line	VDSL. DSL technology providing faster data transmission over short distances, usually between 1000 and 4500 feet (300 and 1500 meters), of twisted pair copper wire. The shorter the distance, the faster the connection rate.
video on demand	VOD. 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.

video services router	VSR. Router used in a video services network to route 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 OS Release 8.3 or later.
virtual channel	Enables queuing, packet scheduling, and accounting rules to be applied to one or more logical interfaces. *See also* virtual channel group.
virtual channel connection	VCC. Uses all the addressing bits of a cell header to move traffic from one link to another. The VCC is formed by joining a series of virtual channels, which are logical circuits uniquely identified for each link of the network.
virtual channel group	Combines virtual channels into a group and then applies the group to one or more logical interfaces. *See also* virtual channel.
virtual channel identifier, virtual circuit identifier	VCI. 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. *See also* VPI.
virtual chassis	Stacked EX Series devices functioning as one logical EX Series switch.
virtual circuit descriptor	VCD. Unique number that identifies a virtual circuit.
virtual circuit, virtual connection	VC • 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. *See also* VPI, VCI, PVC, SVC. • In IDP Series, corresponds with a physical interface.
virtual host	Capability of some computers to respond to different IP addresses and offer different services, each appearing to be a distinct host on a distinct machine. A single machine can supply several virtual hosts.
virtual IP address	VIP address maps traffic received at one IP address to another address based on the destination port number in the packet header.
virtual link	In OSPF, link created between two routers that are part of the backbone but are not physically contiguous.
virtual local area network	VLAN. 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. VLANs allow network administrators to resegment their networks without physically rearranging the devices or network connections. 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. *See also* bridge domain.

virtual loopback tunnel interface	VT. Virtual 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.
virtual path	VP. Combination of multiple virtual circuits between two devices in an ATM network.
virtual path connection	VPC. A concatenation of VPIs between Virtual Path Terminators (VPTs). VPCs are unidirectional.
virtual path identifier	VPI. 8-bit field in the header of an ATM cell that indicates the virtual path the cell takes. *See also* VCI.
Virtual Player	Server-side player provided by Media Flow Controller to assist in media viewing.
virtual private LAN service	VPLS. 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 *Virtual Private LAN Service*.
virtual private network	VPN. Uses a public TCP/IP network, typically the Internet, while maintaining privacy with a tunneling protocol, encryption, and security procedures. *See also* tunneling protocol.
virtual router	VR. • Multiple distinct logical routers within a single router, which enables service providers to configure multiple, separate, secure routers within a single chassis. Each virtual router has its own separate set of IP interfaces, forwarding table, and instances of routing protocols. Applications for this function include the creation of individual routers dedicated to wholesale customers, corporate virtual private network (VPN) users, or a specific traffic type. • In IDP Series, a pair of virtual circuits, providing a physical path into and out of the appliance.
virtual router identifier	VRID. Number in the range 1—255 that identifies a VRRP instance.
Virtual Router Redundancy Protocol	VRRP. On Fast Ethernet and Gigabit Ethernet interfaces, enables you to configure virtual default routers.
virtual routing and forwarding instance	VRF. *Also known as* a virtual router and forwarding instance. A VRF exists within the context of a VR. VRFs are used to create VPNs. In this case, the VRF forwarding table includes only routes to sites that have at least one VPN in common with the site that is associated with the VRF. The router looks up a packet's destination in the VRF associated with the interface on which the packet is received. In general, any application that can be enabled in a VR can be enabled in a VRF.
virtual security device	VSD. Single logical device comprised of a set of physical security devices.

virtual security interface	VSI. Logical entity at Layer 3 that is linked to multiple Layer 2 physical interfaces in a VSD group. The VSI binds to the physical interface of the device acting as master of the VSD group. The VSI shifts to the physical interface of another device in the VSD group if there is a failover and it becomes the new master.
virtual switch	Routing instance that can contain one or more bridge domains.
VLAN	virtual local area network. 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. VLANs allow network administrators to resegment their networks without physically rearranging the devices or network connections. 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. *See also* bridge domain.
VLAN-tagged frame	Tagged frame whose tag header carries both VLAN identification and priority information.
VOD	video on demand. 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.
Voice over Internet Protocol	VoIP. Enables people to use the Internet as the transmission medium for telephone calls by sending voice data in packets using the Internet Protocol instead of over traditional telephony circuits.
VoIP	Voice over Internet Protocol. Enables people to use the Internet as the transmission medium for telephone calls by sending voice data in packets using the Internet Protocol instead of over traditional telephony circuits.
VP	virtual path. Combination of multiple virtual circuits between two devices in an ATM network.
VP tunneling	Tunneling that enables traffic shaping to be applied to the aggregation of all VCs within a single virtual path. Thus, VP tunnels can be used to ensure that the total traffic transmitted on a VP does not exceed the specified peak cell rate.
VPC	virtual path connection. A concatenation of VPIs between Virtual Path Terminators (VPTs). VPCs are unidirectional.
VPI	virtual path identifier. 8-bit field in the header of an ATM cell that indicates the virtual path the cell takes. *See also* VCI.
VPLS	virtual private LAN service. 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 *Virtual Private LAN Service*.

VPLS domain Set of VPLS edge routers running VPLS instances that participate in that domain. Typically associated with customers who want to use Ethernet-based Layer 2 VPNs to connect geographically dispersed sites in their organization across an MPLS-based service provider core, *also known as* an MPLS backbone. To provide signaling for VPLS, BGP builds a full mesh of label-switched paths (LSPs) among all of the VPLS instances on each of the VPLS edge routers participating in a particular VPLS domain.

VPLS edge device VE router. Router that is analogous to a provider edge (PE) router in a BGP/MPLS VPN configuration, and performs similar functions.

VPLS instance New or existing bridge group that has additional VPLS attributes configured. A single VPLS instance is analogous to a distributed learning bridge (*also known as* a bridge group) used for transparent bridging, and performs similar functions. A bridge group is a collection of bridge interfaces stacked on Ethernet Layer 2 interfaces to form a broadcast domain. Similarly, a VPLS instance is a collection of network interfaces stacked on Ethernet Layer 2 interfaces that transmits packets between the router, or VE device, and the CE device located at the edge of the customer's network. In addition, the VPLS virtual core interface enables a VPLS instance to forward traffic not only between bridge interfaces, like a bridge group, but also between a bridge (network) interface and the service provider core.

VPN virtual private network. Uses a public TCP/IP network, typically the Internet, while maintaining privacy with a tunneling protocol, encryption, and security procedures. *See also* tunneling protocol.

VR virtual router.

- Multiple distinct logical routers within a single router, which enables service providers to configure multiple, separate, secure routers within a single chassis. Each virtual router has its own separate set of IP interfaces, forwarding table, and instances of routing protocols. Applications for this function include the creation of individual routers dedicated to wholesale customers, corporate virtual private network (VPN) users, or a specific traffic type.

- In IDP Series, a pair of virtual circuits, providing a physical path into and out of the appliance.

VRF table Routing instance table that stores VRF routing information. *See also* VRF instance.

VRF, VRF instance VPN routing and forwarding instance. *Also known as* virtual router and forwarding instance. A VRF exists within the context of a VR, and is used to create a VPN, for which the VRF forwarding table includes only routes to sites that have at least one VPN in common with the site that is associated with the VRF. The router looks up a packet's destination in the VRF associated with the interface on which the packet is received. In general, any application that can be enabled in a VR can be enabled in a VRF. 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.

VRID virtual router identifier. Number in the range 1—255 that identifies a VRRP instance.

VRRP	Virtual Router Redundancy Protocol. On Fast Ethernet and Gigabit Ethernet interfaces, enables you to configure virtual default routers.
VRRP router	Router that is running VRRP. It might participate in one or more virtual router IDs (VRIDs).
VSD	virtual security device. Single logical device comprised of a set of physical security devices.
VSI	virtual security interface. Logical entity at Layer 3 that is linked to multiple Layer 2 physical interfaces in a VSD group. The VSI binds to the physical interface of the device acting as master of the VSD group. The VSI shifts to the physical interface of another device in the VSD group if there is a failover and it becomes the new master.
VSR	video services router. 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 OS 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. 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. 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 restart	Result of a redundant, standby SRP module becoming active when high availability (HA) is configured. The line modules remain enabled, forwarding remains active, and the newly active SRP module recovers dynamic state information from mirrored storage. To avoid route flapping during an SRP warm restart,BGP and other routing protocols typically use graceful restart. *See also* cold restart, graceful restart.
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	WDM. Technique for transmitting a mix of voice, data, and video over various wavelengths (colors) of light.
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.

Web filtering	Core part of network security that prevents access to unauthorized Web sites. Protects the network from malware and other related threats.
weight	• In BGP, a preference for a particular route over other routes to a destination. The higher the assigned weight, the more preferred the route. By default, the route weight on E Series routers is 32768 for paths originated by the router, and 0 for other paths. • In QoS, a data unit that specifies the relative weight for queues in the traffic class.
weighted random early detection	WRED. Congestion avoidance technique that signals end-to-end protocols such as TCP that the router is becoming congested along a particular egress path. The intent is to trigger TCP congestion avoidance in a random set of TCP flows before congestion becomes severe and causes tail dropping on a large number of flows.
weighted round-robin	WRR. Scheme used to decide the queue from which the next packet should be transmitted.
WEP	Wired Equivalent Privacy. Protocol for encrypting data exchanged on wireless networks. Defined in the original IEEE 802.11 standard.
Wi-Fi Protected Access	WPA/WPA2. Successor to WEP defined in the IEEE 802.11i standard. *See also* WEP.
Wide Area Network Physical Layer Device	WAN PHY. 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.
Wideband Code Division Multiple Access	WCDMA. Radio interface technology used in most third-generation (3G) systems.
Windows Internet Name Service	WINS. 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.
WINS	Windows Internet Name Service. 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.
Wired Equivalent Privacy (Protocol)	WEP. Encrypts data exchanged on wireless networks. Defined in the original IEEE 802.11 standard.
Wireless Application Protocol	WAP. 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).
wireless local area network	WLAN. Type of LAN in which mobile users can connect to the network through a wireless (radio) connection. The IEEE 802.11 standard specifies the technologies for wireless LANs, including the Wired Equivalent Privacy (WEP) encryption algorithm.

WLAN — wireless local area network. Type of LAN in which mobile users can connect to the network through a wireless (radio) connection. The IEEE 802.11 standard specifies the technologies for wireless LANs, including the Wired Equivalent Privacy (WEP) encryption algorithm.

working interface — Provides the primary connection on modules that have APS/MSP or that otherwise enable redundancy.

WPA/WPA2 — Wi-Fi Protected Access. Successor to WEP defined in the IEEE 802.11i standard. *See also* WEP.

WRED — weighted random early detection. Congestion avoidance technique that signals end-to-end protocols such as TCP that the router is becoming congested along a particular egress path. The intent is to trigger TCP congestion avoidance in a random set of TCP flows before congestion becomes severe and causes tail dropping on a large number of flows.

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

X

X.21 interface — ITU serial line protocol standard, used primarily in the USA and Japan, for differential communications. Provides synchronous operation between data communication equipment and data terminal equipment on public data networks.

XDR — External Data Representation Standard. Standard for the description and encoding of data. XDR can be used to transfer data between computers.

xDSL — Combined term used to refer to ADSL, HDSL, SDSL, and VDSL.

XENPAK Multisource Agreement — Standard that defines a type of pluggable fiber-optic transceiver module that is compatible with the 10-Gigabit Ethernet (10 GbE) standard MSA. *See also* MSA

XENPAK, XENPAK module — A pluggable fiber-optic transceiver module that is compatible with the 10-Gigabit Ethernet (10 GbE) standard MSA. XENPAK modules are hot-insertable and hot-removable. *See also* MSA.

XENPAK-SR 10BASE-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. Provides support for fiber-optic cables. XFPs are hot-insertable and hot-removable. *See also* SFP.

XML — Extensible Markup 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   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** . *Also called* 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. 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** . *Also called* XML Path Language.

XPIM   SRX mid-range services gateway network interface card (NIC) that can only be installed in the 20-gigabit GPIM slots (slots 2 and 6 on the front panel).

- The 24-port GigE XPIM (standard or Power over Ethernet versions) is a double-high, double-wide LAN switch Gigabit-Backplane Physical Interface Module (GPIM) that uses two standard slots vertically and two standard slots horizontally and installs in slots 1, 2, 3, and 4 (connecting in the 20G connector in slot 2) or slots 5, 6, 7, and 8 (connecting in the 20G connector in slot 6).

- The 16-port GigE XPIM (standard or Power over Ethernet versions) is a double-high LAN switch GPIM that uses two standard slots vertically and installs in slots 2 and 4 (connecting in the 20G connector in slot 2) or slots 6 and 8 (connecting in the 20G connector in slot 6).

XSLT   Extensible Stylesheet Language for Transformations. 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.w3.org/TR/xslt** .

Z

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