



JUNOS® Software

Hierarchy and RFC Reference

Release 9.4

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

Part Number: 530-028717-01, Revision 1

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

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

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

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

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

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

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

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

JUNOS® Software Hierarchy and RFC Reference,
Release 9.4

Copyright © 2009, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Writing: Tony Mauro
Editing: Joanne McClintock
Cover Design: Edmonds Design

Revision History
15 January 2009—Revision 1

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Abbreviated Table of Contents

	About This Guide	xv
Part 1	JUNOS Software Specification	
Chapter 1	Product Description	3
Chapter 2	Product Components and Supported Software Standards	5
Chapter 3	JUNOS Configuration Specification	45
Part 2	Configuration Commands and Statements	
Chapter 4	Configuration Mode Commands	49
Chapter 5	Complete JUNOS Configuration Statement Hierarchy	51
Part 3	Indexes	
	Index	261
	Index of Supported Software Standards	263

Table of Contents

	About This Guide	xv
	Objectives	xv
	Audience	xv
	Supported Platforms	xvi
	Using the Indexes	xvi
	Using the Examples in This Manual	xvi
	Merging a Full Example	xvii
	Merging a Snippet	xvii
	Documentation Conventions	xviii
	List of Technical Publications	xx
	Documentation Feedback	xxvi
	Requesting Technical Support	xxvii
Part 1	JUNOS Software Specification	
Chapter 1	Product Description	3
Chapter 2	Product Components and Supported Software Standards	5
	User Interfaces	6
	Command-Line Interface	6
	JUNOS XML, JUNOScript, and NETCONF APIs	8
	J-Web User Interface	8
	Supported Network Management Features and Standards	8
	Supported System Access and Access Management Standards	15
	Supported Time Synchronization Standard	16
	Supported BOOTP and DHCP Standards	16
	Supported DTCP Standard	17
	Supported Adaptive Services Standards	17
	Supported DLSw Standards	20
	Supported Interface Standards	20
	Supported Standards for ATM Interfaces	20
	Supported Standards for Frame Relay Interfaces	20
	Supported Standards for GRE and IP-IP Interfaces	21
	Supported Standards for PPP Interfaces	21
	Supported Standards for Serial Interfaces	22
	Supported Standard for T3 Interfaces	22
	Supported Chassis Configuration Features	22

Supported CoS Standards and Features	22
Supported Routing Table Features	25
Supported IP Routing Protocols	27
Supported TCP/IPv4 Standards	27
Supported IPv6 Standards	28
Supported IS-IS and ES-IS Standards and Features	30
Supported OSPF Standards and Features	31
Supported RIP and RIPng Standards	32
Supported ICMP and Neighbor Discovery Standards	33
Supported BGP Standards	33
Supported IP Multicast Standards	34
Supported Standards for MPLS Applications	35
Supported LDP Standards	36
Supported GMPLS Standards	36
Supported MPLS Standards	37
Supported RSVP Standards	38
Supported Routing Policy Features	39
Supported Packet Filtering Standards and Features	40
Supported Policing Standard and Features	41
Supported VPN, VPLS, and Layer 2 Circuit Standards	42
Supported Standards for SDH and SONET Interfaces	43
Supported Standards for Ethernet Interfaces	44
Supported Miscellaneous Routing Features	44

Chapter 3 JUNOS Configuration Specification 45

Configuration Operations	45
Configuration Versions	46
Configuration Groups	46

Part 2 Configuration Commands and Statements

Chapter 4 Configuration Mode Commands 49

Chapter 5 Complete JUNOS Configuration Statement Hierarchy 51

[edit access] Hierarchy Level	53
[edit accounting-options] Hierarchy Level	59
[edit applications] Hierarchy Level	60
[edit bridge-domains] Hierarchy Level	61
[edit chassis] Hierarchy Level	63
[edit class-of-service] Hierarchy Level	68
[edit dynamic-profiles] Hierarchy Level	72
[edit ethernet-switching-options] Hierarchy Level	73
[edit event-options] Hierarchy Level	75

[edit firewall] Hierarchy Level	77
Common Firewall Actions	77
Common IP Firewall Actions	77
Common IPv4 Firewall Actions	78
Common IP Firewall Match Conditions	78
Common IPv4 Firewall Match Conditions	79
Common Layer 2 Firewall Match Conditions	79
Complete [edit firewall] Hierarchy	80
[edit forwarding-options] Hierarchy Level	87
[edit groups] Hierarchy Level	94
[edit interfaces] Hierarchy Level	95
[edit logical-systems] Hierarchy Level	110
[edit multicast-snooping-options] Hierarchy Level	111
[edit poe] Hierarchy Level	112
[edit policy-options] Hierarchy Level	113
Common Policy Terms	113
Common Policy Match Conditions	114
Common Ingress Policy Match Conditions	115
Complete [edit policy-options] Hierarchy	116
[edit protocols] Hierarchy Level	117
[edit protocols ancp] Hierarchy Level	118
[edit protocols bfd] Hierarchy Level	118
[edit protocols bgp] Hierarchy Level	119
[edit protocols connections] Hierarchy Level	127
[edit protocols dlsu] Hierarchy Level	128
[edit protocols dot1x] Hierarchy Level	129
[edit protocols dvmrp] Hierarchy Level	130
[edit protocols esis] Hierarchy Level	131
[edit protocols gvrp] Hierarchy Level	132
[edit protocols igmp] Hierarchy Level	133
[edit protocols igmp-snooping] Hierarchy Level	134
[edit protocols ilmi] Hierarchy Level	135
[edit protocols isis] Hierarchy Level	136
[edit protocols l2circuit] Hierarchy Level	139
[edit protocols l2iw] Hierarchy Level	140
[edit protocols l2-learning] Hierarchy Level	141
[edit protocols lacp] Hierarchy Level	142
[edit protocols layer2-control] Hierarchy Level	143
[edit protocols ldp] Hierarchy Level	144
[edit protocols link-management] Hierarchy Level	147
[edit protocols lldp] Hierarchy Level	148
[edit protocols lldp-med] Hierarchy Level	149
[edit protocols mld] Hierarchy Level	150
[edit protocols mpls] Hierarchy Level	151
Common MPLS Options	151
Complete [edit protocols mpls] Hierarchy	152
[edit protocols msdp] Hierarchy Level	156
[edit protocols mstp] Hierarchy Level	158
[edit protocols neighbor-discovery] Hierarchy Level	159
[edit protocols oam] Hierarchy Level	160
[edit protocols ospf] Hierarchy Level	162

[edit protocols ospf3] Hierarchy Level	166
[edit protocols pgm] Hierarchy Level	168
[edit protocols pim] Hierarchy Level	169
[edit protocols ppp] Hierarchy Level	172
[edit protocols protection-group] Hierarchy Level	173
[edit protocols rip] Hierarchy Level	174
[edit protocols ripng] Hierarchy Level	176
[edit protocols router-advertisement] Hierarchy Level	177
[edit protocols router-discovery] Hierarchy Level	178
[edit protocols rstp] Hierarchy Level	179
[edit protocols rsvp] Hierarchy Level	180
[edit protocols sap] Hierarchy Level	182
[edit protocols sflow] Hierarchy Level	183
[edit protocols vrrp] Hierarchy Level	184
[edit protocols vstp] Hierarchy Level	185
[edit routing-instances] Hierarchy Level	186
[edit routing-options] Hierarchy Level	194
Common Routing Options	194
Complete [edit routing-options] Hierarchy	194
[edit schedulers] Hierarchy Level	201
[edit security] Hierarchy Level	202
[edit services] Hierarchy Level	222
[edit snmp] Hierarchy Level	239
[edit switch-options] Hierarchy Level	243
[edit system] Hierarchy Level	244
[edit virtual-chassis] Hierarchy Level	256
[edit vlans] Hierarchy Level	257

Part 3

Indexes

Index	261
Index of Supported Software Standards	263

List of Tables

Table 1: Notice Icons	xviii
Table 2: Text and Syntax Conventions	xviii
Table 3: Technical Documentation for Supported Routing Platforms	xx
Table 4: JUNOS Software Network Operations Guides	xxiv
Table 5: JUNOS Software for J-series Services Routers and SRX-series Services Gateways Documentation	xxv
Table 6: Additional Books Available Through http://www.juniper.net/books	xxvi
Table 7: Routing Table Route Properties	26

About This Guide

This preface provides the following guidelines for using the *JUNOS® Software Hierarchy and RFC Reference*:

- Objectives on page xv
- Audience on page xv
- Supported Platforms on page xvi
- Using the Indexes on page xvi
- Using the Examples in This Manual on page xvi
- Documentation Conventions on page xviii
- List of Technical Publications on page xx
- Documentation Feedback on page xxvi
- Requesting Technical Support on page xxvii

Objectives

This reference discusses the JUNOS configuration mode commands and includes the complete hierarchy of JUNOS configuration statements.



NOTE: This guide documents Release 9.4 of the JUNOS software. For additional information about the JUNOS software—either corrections to or information that might have been omitted from this guide—see the software release notes at <http://www.juniper.net/>.

Audience

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

To use this guide, you need a broad understanding of networks in general, the Internet in particular, networking principles, and network configuration. You must also be familiar with one or more of the following Internet routing protocols:

- Border Gateway Protocol (BGP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Intermediate System-to-Intermediate System (IS-IS)

- Internet Control Message Protocol (ICMP) router discovery
- Internet Group Management Protocol (IGMP)
- Multiprotocol Label Switching (MPLS)
- Open Shortest Path First (OSPF)
- Protocol-Independent Multicast (PIM)
- Resource Reservation Protocol (RSVP)
- Routing Information Protocol (RIP)
- Simple Network Management Protocol (SNMP)

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

Supported Platforms

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

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

Using the Indexes

This reference contains two indexes: a standard index with topic entries, and an index of supported software standards.

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file `ex-script.conf`. Copy the `ex-script.conf` file to the `/var/tmp` directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xsl;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the `load merge` configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file `ex-script-snippet.conf`. Copy the `ex-script-snippet.conf` file to the `/var/tmp` directory on your routing platform.

```
commit {
  file ex-script-snippet.xsl; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

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

3. Merge the contents of the file into your routing platform configuration by issuing the `load merge relative` configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the `load` command, see the *JUNOS CLI User Guide*.

Documentation Conventions

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

Table 1: Notice Icons





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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the <code>configure</code> command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active

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

Convention	Description	Examples
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces important new terms. Identifies book names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>JUNOS System Basics Configuration Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Plain text like this	Represents names of configuration statements, commands, files, and directories; IP addresses; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	stub <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select Protocols > Ospf .

List of Technical Publications

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

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

Table 3: Technical Documentation for Supported Routing Platforms

Book	Description
JUNOS Software for Supported Routing Platforms	
<i>Access Privilege</i>	Explains how to configure access privileges in user classes by using permission flags and regular expressions. Lists the permission flags along with their associated command-line interface (CLI) operational mode commands and configuration statements.
<i>Broadband Subscriber Management Solutions</i>	Describes residential subscriber management and how you can deploy solutions that include multisubscriber IP address assignment, service provisioning, authentication, authorization, accounting, and dynamic request services in your network.
<i>Class of Service</i>	Provides an overview of the class-of-service (CoS) functions of the JUNOS software and describes how to configure CoS features, including configuring multiple forwarding classes for transmitting packets, defining which packets are placed into each output queue, scheduling the transmission service level for each queue, and managing congestion through the random early detection (RED) algorithm.
<i>CLI User Guide</i>	Describes how to use the JUNOS command-line interface (CLI) to configure, monitor, and manage Juniper Networks routing platforms. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>Feature Guide</i>	Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS software.
<i>High Availability</i>	Provides an overview of hardware and software resources that ensure a high level of continuous routing platform operation and describes how to configure high availability (HA) features such as nonstop active routing (NSR) and graceful Routing Engine switchover (GRES).
<i>MPLS Applications</i>	Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols.
<i>Multicast Protocols</i>	Provides an overview of multicast concepts and describes how to configure multicast routing protocols.

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

Book	Description
<i>Multiplay Solutions</i>	Describes how you can deploy IPTV and voice over IP (VoIP) services in your network.
<i>MX-series Layer 2 Configuration Guide</i>	Provides an overview of the Layer 2 functions of the MX-series routers, including configuring bridging domains, MAC address and VLAN learning and forwarding, and spanning-tree protocols. It also details the routing instance types used by Layer 2 applications. All of this material was formerly covered in the <i>JUNOS Routing Protocols Configuration Guide</i> .
<i>MX-series Layer 2 Solutions Guide</i>	Describes common configuration scenarios for the Layer 2 features supported on the MX-series routers, including basic bridged VLANs with normalized VLAN tags, aggregated Ethernet links, bridge domains, Multiple Spanning Tree Protocol (MSTP), and integrated routing and bridging (IRB).
<i>Network Interfaces</i>	Provides an overview of the network interface functions of the JUNOS software and describes how to configure the network interfaces on the routing platform.
<i>Network Management</i>	Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP and accounting options.
<i>Policy Framework</i>	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, and forwarding options.
<i>Protected System Domain</i>	Provides an overview of the JCS 1200 platform and the concept of Protected System Domains (PSDs). The JCS 1200 platform, which contains up to six redundant pairs of Routing Engines running JUNOS software, is connected to a T320 router or to a T640 or T1600 routing node. To configure a PSD, you assign any number of Flexible PIC concentrators (FPCs) in the T-series routing platform to a pair of Routing Engines on the JCS 1200 platform. Each PSD has the same capabilities and functionality as a physical router, with its own control plane, forwarding plane, and administration.
<i>Routing Protocols</i>	Provides an overview of routing concepts and describes how to configure routing instances, and unicast routing protocols.
<i>Secure Configuration Guide for Common Criteria and JUNOS-FIPS</i>	Provides an overview of secure Common Criteria and JUNOS-FIPS protocols for the JUNOS software and describes how to install and configure secure Common Criteria and JUNOS-FIPS on a routing platform.
<i>Services Interfaces</i>	Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the router.
<i>Software Installation and Upgrade Guide</i>	Describes the JUNOS software components and packaging and explains how to initially configure, reinstall, and upgrade the JUNOS system software. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .

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

Book	Description
<i>Subscriber Access</i>	Provides an overview of the subscriber access features of the JUNOS software and describes how to configure subscriber access support on the router, including dynamic profiles, class of service, AAA, and access methods.
<i>System Basics</i>	Describes Juniper Networks routing platforms and explains how to configure basic system parameters, supported protocols and software processes, authentication, and a variety of utilities for managing your router on the network.
<i>VPNs</i>	Provides an overview and describes how to configure Layer 2 and Layer 3 virtual private networks (VPNs), virtual private LAN service (VPLS), and Layer 2 circuits. Provides configuration examples.
JUNOS References	
<i>Hierarchy and RFC Reference</i>	Describes the JUNOS configuration mode commands. Provides a hierarchy reference that displays each level of a configuration hierarchy, and includes all possible configuration statements that can be used at that level. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>Interfaces Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot interfaces.
<i>Routing Protocols and Policies Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot routing policies and protocols, including firewall filters.
<i>System Basics and Services Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot system basics, including commands for real-time monitoring and route (or path) tracing, system software management, and chassis management. Also describes commands for monitoring and troubleshooting services such as class of service (CoS), IP Security (IPsec), stateful firewalls, flow collection, and flow monitoring.
<i>System Log Messages Reference</i>	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
J-Web User Guide	
<i>J-Web Interface User Guide</i>	Describes how to use the J-Web graphical user interface (GUI) to configure, monitor, and manage Juniper Networks routing platforms.
JUNOS API and Scripting Documentation	
<i>JUNOScript API Guide</i>	Describes how to use the JUNOScript application programming interface (API) to monitor and configure Juniper Networks routing platforms.
<i>JUNOS XML API Configuration Reference</i>	Provides reference pages for the configuration tag elements in the JUNOS XML API.

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

Book	Description
<i>JUNOS XML API Operational Reference</i>	Provides reference pages for the operational tag elements in the JUNOS XML API.
<i>NETCONF API Guide</i>	Describes how to use the NETCONF API to monitor and configure Juniper Networks routing platforms.
<i>JUNOS Configuration and Diagnostic Automation Guide</i>	Describes how to use the commit script and self-diagnosis features of the JUNOS software. This guide explains how to enforce custom configuration rules defined in scripts, how to use commit script macros to provide simplified aliases for frequently used configuration statements, and how to configure diagnostic event policies.
Hardware Documentation	
<i>Hardware Guide</i>	Describes how to install, maintain, and troubleshoot routing platforms and components. Each platform has its own hardware guide.
<i>PIC Guide</i>	Describes the routing platform's Physical Interface Cards (PICs). Each platform has its own PIC guide.
<i>DPC Guide</i>	Describes the Dense Port Concentrators (DPCs) for all MX-series routers.
JUNOScope Documentation	
<i>JUNOScope Software User Guide</i>	Describes the JUNOScope software graphical user interface (GUI), how to install and administer the software, and how to use the software to manage routing platform configuration files and monitor routing platform operations.
Advanced Insight Solutions (AIS) Documentation	
<i>Advanced Insight Solutions Guide</i>	Describes the Advanced Insight Manager (AIM) application, which provides a gateway between JUNOS devices and Juniper Support Systems (JSS) for case management and intelligence updates. Explains how to run AI-Scripts on Juniper Networks devices.
Release Notes	
<i>JUNOS Release Notes</i>	Summarize new features and known problems for a particular software release, provide corrections and updates to published JUNOS, JUNOScript, and NETCONF manuals, provide information that might have been omitted from the manuals, and describe upgrade and downgrade procedures.
<i>Hardware Release Notes</i>	Describe the available documentation for the routing platform and summarize known problems with the hardware and accompanying software. Each platform has its own release notes.
<i>JUNOScope Release Notes</i>	Contain corrections and updates to the published JUNOScope manual, provide information that might have been omitted from the manual, and describe upgrade and downgrade procedures.

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

Book	Description
<i>AIS Release Notes</i>	Summarize AIS new features and guidelines, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide initial setup, upgrade, and downgrade procedures.
<i>AIS AI-Scripts Release Notes</i>	Summarize AI-Scripts new features, identify known and resolved problems, provide information that might have been omitted from the manuals, and provide instructions for automatic and manual installation, including deleting and rolling back.

Table 4: JUNOS Software Network Operations Guides

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

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

Table 5: JUNOS Software for J-series Services Routers and SRX-series Services Gateways Documentation

Book	Description
J-series and SRX-series Platforms	
<i>JUNOS Software Interfaces and Routing Configuration Guide</i>	Explains how to configure SRX-series and J-series interfaces for basic IP routing with standard routing protocols, ISDN service, firewall filters (access control lists), and class-of-service (CoS) traffic classification.
<i>JUNOS Software Security Configuration Guide</i>	Explains how to configure and manage SRX-series and J-series security services such as stateful firewall policies, IPsec VPNs, firewall screens, Network Address Translation (NAT), Public Key Cryptography, chassis clusters, Application Layer Gateways (ALGs), and Intrusion Detection and Prevention (IDP).
<i>JUNOS Software Administration Guide</i>	Shows how to monitor SRX-series and J-series devices and routing operations, firewall and security services, system alarms and events, and network performance. This guide also shows how to administer user authentication and access, upgrade software, and diagnose common problems.
<i>JUNOS Software CLI Reference</i>	Provides the complete configuration hierarchy available on SRX-series and J-series devices. This guide also describes the configuration statements and operational mode commands unique to these devices.
<i>JUNOS Release Notes</i>	Summarize new features and known problems for a particular release of JUNOS software, including JUNOS software for J-series and SRX-series devices. The release notes also contain corrections and updates to the manuals and software upgrade and downgrade instructions for JUNOS software.
J-series Only	
<i>JUNOS Software Design and Implementation Guide</i>	Provides guidelines and examples for designing and implementing IPsec VPNs, firewalls, and routing on J-series Services Routers running JUNOS software.
<i>J-series Services Routers Quick Start</i>	Explains how to quickly set up a J-series Services Router. This document contains router declarations of conformity.
<i>J-series Services Routers Hardware Guide</i>	Provides an overview, basic instructions, and specifications for J-series Services Routers. This guide explains how to prepare a site, unpack and install the router, replace router hardware, and establish basic router connectivity. This guide contains hardware descriptions and specifications.
<i>JUNOS Software Migration Guide</i>	Provides instructions for migrating an SSG device running ScreenOS software to JUNOS software or upgrading a J-series device to a later version of the JUNOS software.
<i>WXC Integrated Services Module Installation and Configuration Guide</i>	Explains how to install and initially configure a WXC Integrated Services Module in a J-series Services Router for application acceleration.

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

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

Documentation Feedback

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

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

Part 1

JUNOS Software Specification

- Product Description on page 3
- Product Components and Supported Software Standards on page 5
- JUNOS Configuration Specification on page 45

Chapter 1

Product Description

The JUNOS software includes IP routing protocol software, as well as software for interface, network, and chassis management. The same software runs on all Juniper Networks J-series, M-series, MX-series, and T-series routing platforms. Juniper Networks routing platforms use two types of processing engine:

- Routing Engine—Maintains routing tables and controls routing protocols.
- Packet Forwarding Engine—Forwards network traffic, which is processed by application-specific integrated circuits (ASICs) and other components.

Juniper Networks offers three versions of the JUNOS software:

- Canada and United States version, which incorporates cryptographic functionality and is therefore subject to export controls. When used in combination with an ES Physical Interface Card (PIC), the strong cryptographic functionality in the Canada and U.S. version of the JUNOS software substantially supports IP Security (IPsec). The software also supports secure remote network management sessions (using SSH and Secure Sockets Layer [SSL]), and secure transmission of control traffic between Routing Engines (using SSH).
- Worldwide version, which omits most cryptographic functionality, including support for IPsec with the ES PIC.
- JUNOS-FIPS version, which meets the requirements of Federal Information Processing Standard (FIPS) PUB 140-2.

Chapter 2

Product Components and Supported Software Standards

This chapter describes the following product components and supported software standards for the JUNOS software:

- User Interfaces on page 6
- Supported Network Management Features and Standards on page 8
- Supported System Access and Access Management Standards on page 15
- Supported Time Synchronization Standard on page 16
- Supported BOOTP and DHCP Standards on page 16
- Supported DTCP Standard on page 17
- Supported Adaptive Services Standards on page 17
- Supported DLSw Standards on page 20
- Supported Interface Standards on page 20
- Supported Chassis Configuration Features on page 22
- Supported CoS Standards and Features on page 22
- Supported Routing Table Features on page 25
- Supported IP Routing Protocols on page 27
- Supported Standards for MPLS Applications on page 35
- Supported Routing Policy Features on page 39
- Supported Packet Filtering Standards and Features on page 40
- Supported Policing Standard and Features on page 41
- Supported VPN, VPLS, and Layer 2 Circuit Standards on page 42
- Supported Standards for SDH and SONET Interfaces on page 43
- Supported Standards for Ethernet Interfaces on page 44
- Supported Miscellaneous Routing Features on page 44

User Interfaces

The JUNOS software provides several user interfaces, including a command-line interface (CLI), the JUNOScript application programming interface (API), the NETCONF API, and the J-Web graphical user interface. They are described in the following sections:

- Command-Line Interface on page 6
- JUNOS XML, JUNOScript, and NETCONF APIs on page 8
- J-Web User Interface on page 8

For more information about the user interfaces, see the *JUNOS CLI User Guide*.

Command-Line Interface

The JUNOS *command-line interface (CLI)* is the user interface available when a user logs in to a routing platform through the console or auxiliary port, or logs in remotely. The CLI has two modes: operational mode, which provides commands for monitoring the JUNOS software, routing protocols, network interfaces and connectivity, and routing platform hardware; and configuration mode, which provides commands for configuring the JUNOS software. For more information about configuration mode, see “JUNOS Configuration Specification” on page 45.

The JUNOS CLI provides the following functionality:

- Context-sensitive name completion for commands, configuration statements, and other text strings, such as filenames and usernames. When you type only the initial part of a name and press the Tab key or the Spacebar, the CLI automatically adds the remainder of the name if there is only one possible completion. If multiple completions are possible, the CLI lists them and displays a short description of each.

Similarly, if you type a question mark (?) after the starting portion of a term (word) in a command or configuration statement, or after a complete term and a following space, the CLI displays the terms that can be specified at that position in the command or statement, along with a short description of each.

- Keyword search for commands and configuration statements (similar to the UNIX **apropos** command). The **help apropos topic** command displays all commands or configuration statements that include the specified topic word in their names or short description. In configuration mode, this feature is context-sensitive—the CLI displays only the matching terms that are valid at or below the current level in the configuration hierarchy.
- Automatic display of one screen at a time when command output or the list of possible completions is longer than the screen length (similar to the effect of the UNIX **more** utility). You can scroll backward and forward through the screen output and search for text strings in it.
- Keyboard sequences for editing the command line and moving the cursor on it, and for scrolling through a list of recently executed commands. The keyboard

sequences are the same as those used in the UNIX editor Emacs. For example, when you type Ctrl + b, the cursor moves backward one character.

- Tracking of commands issued during the current CLI session. To display then, issue the **show cli history** command.

You can customize your CLI environment in the following ways:

- Define the terminal type as ANSI, VT100, or regular or small xterm.
- Disable command completion.
- Display helpful hints about how to use the CLI.
- Enable an automatic prompt for the user to restart the routing platform after a software upgrade. Restarting is required for the new software to take effect.
- Set the CLI prompt.
- Set the duration that a login session can be idle before it is terminated.
- Set the screen length, width, or both.

You can apply filters to command output to change the CLI's standard display behavior in the following ways:

- Count the number of lines in the output instead of displaying the actual output.
- Display only text that matches or does not match a pattern. The JUNOS software supports the use of extended (modern) regular expressions as defined in POSIX 1003.2.
- Display all output at once (override the default behavior of displaying one screen of output at a time).
- Display only the final lines of output.
- Suppress redisplay of the CLI prompt at the end of command output.
- Save (redirect) the screen output to a file.

When displaying the current configuration, you can filter the output in the following ways in addition to those in the preceding list:

- Compare the current configuration with a previously saved configuration.
- Display additional information about the configuration, including the version of the JUNOS software under which the configuration was created.

You can also apply multiple filters in sequence, and write scripts that customize the output in ways not provided by the CLI. For information about scripting, see the *JUNOS Configuration and Diagnostic Automation Guide*.

For detailed information about the CLI features described in this section, see the *JUNOS CLI User Guide*.

JUNOS XML, JUNOScript, and NETCONF APIs

The *JUNOS Extensible Markup Language (XML) application programming interface (API)* defines XML tag elements that correspond to all JUNOS configuration statements and many operational commands. XML is a language for defining a set of markers (tag elements) that are applied to a data set or document to describe the function of individual elements and codify the hierarchical relationships between them.

The *JUNOScript API* enables client applications to exchange information with Juniper Networks routing platforms. The JUNOScript API defines XML tag elements that retrieve and change JUNOS configuration objects, which are represented by the XML tag elements in the JUNOS XML API.

The *NETCONF API* is similar in function to the JUNOScript API and is defined in RFC 4741, *NETCONF Configuration Protocol*. The NETCONF server and client applications use the SSH protocol for communication in accordance with RFC 4742, *Using the NETCONF Configuration Protocol over Secure SHell (SSH)*.

J-Web User Interface

The *J-Web* user interface is a graphical user interface that enables you to configure and monitor Juniper Networks routing platforms through an Internet browser. The J-Web interface includes the following features:

- Quick Configuration pages for performing basic configuration operations
- Monitoring tools that display system status, routes, and statistics
- Diagnostic tools
- A View Events page that displays system log messages
- File utilities for managing configuration files, licenses, and temporary files

Supported Network Management Features and Standards

The JUNOS software supports the use of scripts and event-triggered policies that you write to automate network management. The functions you can perform with these utilities include the following:

- Automatically detect, diagnose, and fix network problems. When it detects a problem, the script can issue a command that includes options appropriate to the current situation, and then interpret the command output to determine the next appropriate command or action.
- Periodically check for alarms or other indicators of network or chassis problems, and perform specific actions if they exist.
- Respond automatically to the occurrence of events and conditions that also trigger system log messages or SNMP traps.
- Verify that the routing platform's configuration includes only statements you deem appropriate for your network, and automatically add or remove statements as necessary.

- Automatically change the routing platform's configuration in response to network problems or conditions you specify.
- Generate custom error, warning, or system log messages.

For more information about scripts and event policies, see the *JUNOS Configuration and Diagnostic Automation Guide*.

The JUNOS software substantially supports SNMP version 1, version 2c, and version 3. The JUNOS SNMP agent software accepts both IP version 4 (IPv4) and IP version 6 (IPv6) addresses.

The JUNOS software supports the majority of network management features defined in the following standards documents. All RFCs and Internet drafts are published by the Internet Engineering Task Force (IETF).

- Extended Security Options (ESO) Consortium, *ESO Consortium MIB*
- Institute of Electrical and Electronics Engineers (IEEE) standard 802.3ad, *Aggregation of Multiple Link Segments* (only the following objects:
dot3adAggPortDebugActorChangeCount,
dot3adAggPortDebugActorSyncTransitionCount,
dot3adAggPortDebugPartnerChangeCount,
dot3adAggPortDebugPartnerSyncTransitionCount, dot3adAggPortDebugMuxState,
dot3adAggPortDebugRxState, dot3adAggPortTable, dot3adAggPortListTable,
dot3adAggPortStatsTable, dot3adAggTable, and dot3adTablesLastChanged)

Gigabit Ethernet interfaces on J-series Services Routers do not support the 802.3ad MIB.

- Internet Assigned Numbers Authority (IANA), *IANAiftype Textual Convention MIB* (referenced by RFC 2863, *The Interfaces Group MIB*)
- RFC 1155, *Structure and Identification of Management Information for TCP/IP-based Internets*
- RFC 1156, *Management Information Base for Network Management of TCP/IP-based internets*
- RFC 1157, *A Simple Network Management Protocol (SNMP)*
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments* (only the following objects: isisAreaAddr, isisCirc, isisCircLevel, isisISAdj, isisISAdjAreaAddr, isisAdjIPAddr, isisISAdjProtSupp, isisIPRA, isisMANAreaAddr, isisPacketCount, isisRa, isisSysProtSupp, isisSummAddr, and isisSystem)
- RFC 1212, *Concise MIB Definitions*

- RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*. The JUNOS software supports the following features:
 - MIB II and its SNMP version 2 derivatives, including the following:
 - Statistics counters
 - IP (except for the `ipRouteTable` object, which has been replaced by `ipCidrRouteTable` [RFC 2096, *IP Forwarding Table MIB*])
 - SNMP management
 - Interface management
 - SNMP version 1 `Get` and `GetNext` requests and version 2 `GetBulk` requests
 - JUNOS-specific secured access list
 - Master configuration keywords
 - Reconfigurations upon receipt of the SIGHUP signal
- RFC 1215, *A Convention for Defining Traps for use with the SNMP* (only MIB II SNMP version 1 traps and version 2 notifications)
- RFC 1406, *Definitions of Managed Objects for the DS1 and E1 Interface Types* (T1 MIB is supported) (obsoleted by RFC 2495)
- RFC 1407, *Definitions of Managed Objects for the DS3/E3 Interface Type* (T3 MIB is supported) (obsoleted by RFC 2496)
- RFC 1472, *The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol*
- RFC 1473, *The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol*
- RFC 1657, *Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2* (except for the `bgpBackwardTransition` and `bgpEstablished` notifications)
- RFC 1695, *Definitions of Managed Objects for ATM Management Version 8.0 Using SMIv2* (obsoleted by RFC 2515)
- RFC 1724, *RIP Version 2 MIB Extension*
- RFC 1850, *OSPF Version 2 Management Information Base* (except for the `ospfOriginateNewLsas` and `ospfRxNewLsas` objects, the Host Table, and the `ospfLsdbApproachingOverflow`, `ospfLsdbOverflow`, and `ospfOriginateLSA` traps)
- RFC 1901, *Introduction to Community-based SNMPv2*
- RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)* (obsoleted by RFC 3416)
- RFC 1907, *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)* (obsoleted by RFC 3418)
- RFC 2011, *SNMPv2 Management Information Base for the Internet Protocol using SMIv2*

- RFC 2012, *SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2*
- RFC 2013, *SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2*
- RFC 2024, *Definitions of Managed Objects for Data Link Switching using SMIv2* (read-only access) (except for the `dlswInterface` and `dlswSdlc` object groups; the `dlswDirLocateMacTable`, `dlswDirLocateNBTable`, and `dlswDirNBTable` tables; the `dlswCircuitDiscReasonLocal` and `dlswCircuitDiscReasonRemote` tabular objects; and the `dlswCircuitS1Dlc`, `dlswDirMacCacheNextIndex`, and `dlswDirNBCacheNextIndex` scalar objects)
- RFC 2096, *IP Forwarding Table MIB* (The `ipCidrRouteTable` object is extended to include the tunnel name when the next hop is through an RSVP-signaled label-switched path [LSP].)
- RFC 2115, *Management Information Base for Frame Relay DTEs Using SMIv2* (only the `frDlcmiTable` object)
- RFC 2233, *The Interfaces Group MIB using SMIv2* (obsoleted by RFC 2863)
- RFC 2287, *Definitions of System-Level Managed Objects for Applications* (only the following objects: `sysApplElmtRunTable`, `sysApplInstallElmtTable`, `sysApplInstallPkgTable`, and `sysApplMapTable`)
- RFC 2465, *Management Information Base for IP Version 6: Textual Conventions and General Group* (except for IPv6 and Internet Control Message Protocol version 6 [ICMPv6] statistics)
- RFC 2466, *Management Information Base for IP Version 6: ICMPv6 Group*
- RFC 2495, *Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types* (except for the following objects: `dsx1FarEndConfigTable`, `dsx1FarEndCurrentTable`, `dsx1FarEndIntervalTable`, `dsx1FarEndTotalTable`, and `dsx1FracTable`)
- RFC 2496, *Definitions of Managed Objects for the DS3/E3 Interface Type* (except for the following objects: `dsx3FarEndConfigTable`, `dsx3FarEndCurrentTable`, `dsx3FarEndIntervalTable`, `dsx3FarEndTotalTable`, and `dsx3FracTable`)
- RFC 2515, *Definitions of Managed Objects for ATM Management* (except for the `aal5VccTable`, `atmVcCrossConnectTable`, and `atmVpCrossConnectTable` objects)
- RFC 2558, *Definitions of Managed Objects for the SONET/SDH Interface Type* (obsoleted by RFC 3592)
- RFC 2570, *Introduction to Version 3 of the Internet-standard Network Management Framework*
- RFC 2571, *An Architecture for Describing SNMP Management Frameworks* (read-only access)
- RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* (read-only access) (obsoleted by RFC 3412)
- RFC 2576, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*
- RFC 2578, *Structure of Management Information Version 2 (SMIv2)*
- RFC 2579, *Textual Conventions for SMIv2*

- RFC 2580, *Conformance Statements for SMIv2*
- RFC 2662, *Definitions of Managed Objects for the ADSL Lines* (J-Series Services Routers; all MIB tables, objects, and traps applicable to the asymmetric digital subscriber line [ADSL] transceiver unit-remote [ATU-R] agent)
- RFC 2665, *Definitions of Managed Objects for the Ethernet-like Interface Types*
- RFC 2667, *IP Tunnel MIB*
- RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol* (except for row creation, the **Set** operation, and the **vrpStatsPacketLengthErrors** object)
- RFC 2790, *Host Resources MIB*. The following objects are supported:
 - Only the **hrStorageTable** object. The file systems **/**, **/config**, **/var**, and **/tmp** always return the same index number. When SNMP restarts, the index numbers for the remaining file systems might change.
 - Only the objects in the **hrSystem** and **hrSWInstalled** groups.
- RFC 2819, *Remote Network Monitoring Management Information Base* (only the **alarmTable**, **eventTable**, and **logTable** objects and the **etherStatsTable** object for Ethernet interfaces)
- RFC 2863, *The Interfaces Group MIB*
- RFC 2864, *The Inverted Stack Table Extension to the Interfaces Group MIB*
- RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations* (only the following objects: **pingCtlTable**, **pingMaxConcurrentRequests**, **pingProbeHistoryTable**, **pingResultsTable**, **traceRouteCtlTable**, **traceRouteHopsTable**, **traceRouteProbeHistoryTable**, and **traceRouteResultsTable**)
- RFC 2932, *IPv4 Multicast Routing MIB*
- RFC 2933, *Internet Group Management Protocol MIB*
- RFC 2934, *Protocol Independent Multicast MIB for IPv4*
- RFC 2981, *Event MIB*
- RFC 3014, *Notification Log MIB*
- RFC 3019, *IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol*
- RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*
- RFC 3412, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*
- RFC 3413, *Simple Network Management Protocol (SNMP) Applications* (except for the proxy MIB)
- RFC 3414, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*
- RFC 3415, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*

- RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*
- RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)*
- RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*
- RFC 3498, *Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures* (implemented under the Juniper Networks enterprise branch)
- RFC 3592, *Definitions of Managed Objects for the Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) Interface Type*
- RFC 3811, *Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management*
- RFC 3812, *Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)* (read only access)

The following restrictions apply:

- MPLS tunnels as interfaces are not supported.
- The following objects in the `TunnelResource` table are not supported: `mplsTunnelResourceExBurstSize`, `mplsTunnelResourceMaxBurstSize`, `mplsTunnelResourceMeanBurstSize`, `mplsTunnelResourceMeanRate`, and `mplsTunnelResourceWeight`.
- The `mplsTunnelCRLDPResTable` and `mplsTunnelPerfTable` objects are not supported.
- The `mplsTunnelCHopTable` object is supported on ingress routers only.



NOTE: The branch used by the proprietary LDP MIB (`ldpmib.mib`) conflicts with RFC 3812. `ldpmib.mib` has been deprecated and replaced by `jnx-mpls-ldp.mib`.

- RFC 3813, *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)* (except for the following objects: `mplsInSegmentPerfTable`, `mplsInSegmentMapTable`, `mplsInterfacePerfTable`, `mplsOutSegmentPerfTable`, `mplsXCDown`, and `mplsXCUp`; read only)
- RFC 3815, *Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)* (only the `mplsLdpLsrID` and `mplsLdpSesPeerAddrTable` objects)
- RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*
- RFC 4444, *Management Information Base for Intermediate System to Intermediate System (IS-IS)*
- Internet draft `draft-ietf-bfd-mib-02.txt`, *Bidirectional Forwarding Detection Management Information Base*. This MIB provides SNMP trap support for BFD liveness detection. (Support is read-only and includes the `bfdSessDown` and

bfdSessUp traps. Objects in the **bfdSessMapTable** and **bfdSessPerfTable** tables are not supported.) MIB **draft-ietf-bfd-mib-02.txt** is represented by **mib-jnx-bfd-exp.txt** and is implemented under the Juniper Networks Enterprise **jnxExperiment** branch.

- Internet draft **draft-ietf-idr-bgp4-mibv2-04.txt**, *Definitions of Managed Objects for the Fourth Version of Border Gateway Protocol (BGP-4), Second Version* (only the following objects: **jnxBgpM2PrefixInPrefixes**, **jnxBgpM2PrefixInPrefixesAccepted**, and **jnxBgpM2PrefixInPrefixesRejected**)
- Internet draft **draft-ietf-isis-wg-mib-16.txt**, *Management Information Base for IS-IS* (only the following tables: **isisISAdjAreaAddrTable**, **isisISAdjIPAddrTable**, **isisISAdjProtSuppTable**, and **isisISAdjTable**)
- Internet draft **draft-ietf-msdp-mib-08.txt**, *Multicast Source Discovery protocol MIB* (except for the **msdpBackwardTransition**, **msdpEstablished**, and **msdpRequestsTable** objects)
- Internet draft **draft-ietf-ospf-ospfv3-mib-11.txt**, *Management Information Base for OSPFv3* (Represented by **mib-jnx-ospfv3mib.txt** and implemented under the Juniper Networks Enterprise **jnxExperiment** branch. Support for the **ospfv3NbrTable** table only. Read-only. Object names are prefixed by **jnx**, as in **jnxOspfv3NbrAddressType**, **jnxOspfv3NbrPriority**, and **jnxOspfv3NbrTable**.)
- Internet draft **draft-ietf-ppvpn-mpls-vpn-mib-05.txt**, *MPLS/BGP Virtual Private Network Management Information Base Using SMv2* (only the following objects and tables: **mplsVpnScalars**, **mplsVpnVrfPerfTable**, **mplsVpnVrfRouteTargetTable**, and **mplsVpnVrfTable**; expires May 2003)
- Internet draft **draft-reeder-snmv3-usm-3desede-00.txt**, *Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in "Outside" CBC Mode*
- Integrated Local Management Interface (ILMI) MIB (only the **atmfMYIPNmAddress** and **atmfPortMyIfname** objects). For more information about the ILMI MIB, see the *JUNOS Network Management Configuration Guide* and the ATM Forum Web site at <http://www.atmforum.com/>.

The JUNOS software provides numerous enterprise MIBs, including the following:

- Alarm
- Asynchronous Transfer Mode (ATM)
- ATM class of service (CoS)
- BGP4 version 2
- Chassis
- Chassis definitions for routing platform model
- Chassis forwarding
- CoS
- Configuration management
- Destination class usage
- Dynamic flow capture
- Ethernet media access control (MAC)

- Experimental
- Firewall
- Flow collector services
- Host resources
- IP Security (IPsec) monitoring
- IPv4
- IPv6 and ICMPv6
- LDP
- MPLS
- Passive monitoring
- RSVP traffic engineering
- Reverse path forwarding
- Services Physical Interface Card (PIC)
- SONET Automatic Protection Switching (APS)
- SONET/SDH interface management
- Source class usage
- Structure of Management Information (SMI)
- Virtual private network (VPN)

In addition, the JUNOS software provides extensions to the interface, ping, remote monitoring (RMON) events and alarms, and traceroute MIBs.

For some traps, a message is directed to the system log when the trap condition occurs, even if the SNMP agent does not send the trap to a network management system (NMS).

Supported System Access and Access Management Standards

To validate users who attempt to access a routing platform, the JUNOS software supports RADIUS authentication, TACACS+ authentication, and authentication by means of JUNOS user accounts configured on the routing platform. The JUNOS software supports the configuration of Juniper Networks-specific RADIUS and TACACS+ attributes, and the creation of template accounts.

The JUNOS software substantially supports the following RADIUS and TACACS+ standards:

- RFC 1492, *An Access Control Protocol, Sometimes Called TACACS*
- RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*
- RFC 2866, *RADIUS Accounting*

- RFC 2869, *RADIUS Extensions*
- RFC 3576, *Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*

All users who can log in to the routing platform must already be assigned to a JUNOS login class. A *login class* defines its members' access privileges during a login session, the commands they can and cannot issue, the configuration statements they can and cannot view or change, and the idle time before a member's login session is terminated.

The JUNOS software substantially supports the following access protocols and applications: telnet, FTP, rlogin, and finger. In addition, the Canada and U.S. version of the JUNOS software substantially supports SSH as an access protocol.

The JUNOS software substantially supports RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*.

The Canada and U.S. version of the JUNOS software substantially supports the following standards related to Secure Sockets Layer (SSL):

- RFC 1319, *The MD2 Message-Digest Algorithm*
- RFC 1321, *The MD5 Message-Digest Algorithm*
- RFC 2246, *The TLS Protocol Version 1.0*
- RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

Supported Time Synchronization Standard

The JUNOS software substantially supports RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*.

In CLI operational mode, you can set the current date and time on the routing platform manually or from an NTP server.

Supported BOOTP and DHCP Standards

The JUNOS software substantially supports the following bootstrap protocol (BOOTP) and Dynamic Host Control Protocol (DHCP) standards:

- RFC 951, *BOOTSTRAP PROTOCOL (BOOTP)*
- RFC 1001, *PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: CONCEPTS AND METHODS*
- RFC 1002, *PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: DETAILED SPECIFICATIONS*
- RFC 1035, *DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION*
- RFC 1534, *Interoperation Between DHCP and BOOTP*
- RFC 1700, *ASSIGNED NUMBERS*

- RFC 2131, *Dynamic Host Configuration Protocol* (DHCP over virtual LAN [VLAN]-tagged interfaces is not supported.)
- RFC 2132, *DHCP Options and BOOTP Vendor Extensions*
- RFC 3046, *DHCP Relay Agent Information Option*
- RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)* (Address assignment is supported with IPv4 but not IPv6 address assignment.)
- RFC 3397, *Dynamic Host Configuration Protocol (DHCP) Domain Search Option*
- RFC 3925, *Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)*

Supported DTCP Standard

The JUNOS software substantially supports Internet draft draft-cavuto-dtcp-01.txt, *DTCP: Dynamic Tasking Control Protocol*.

Supported Adaptive Services Standards

On Adaptive Services PICs (both standalone and integrated versions) and MultiServices PICs, the JUNOS software supports the following services:

- CoS—Traffic filtering based on class-of-service features.

The JUNOS software substantially supports the following CoS standards:

- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers* (obsoletes RFCs 1349 and 1455)
- RFC 2475, *An Architecture for Differentiated Services*
- Flow monitoring and discard accounting—Tools for sampling traffic, gathering detailed information about traffic flows, and performing discard accounting.

The JUNOS software substantially supports the following standards for Monitoring Services PICs in addition to Adaptive Services and MultiServices PICs:

- Standards for cflowd version 5 and version 8 formats maintained by CAIDA (<http://www.caida.org>)
- RFC 3954, *Cisco Systems NetFlow Services Export Version 9*
- Intrusion detection services (IDS)—Tools for detecting, redirecting, and preventing certain kinds of network attack and intrusion.
- IPsec—Tools for configuring manual or dynamic security associations (SAs) for encryption of data traffic.

The Canada and U.S. version of the JUNOS software substantially supports the IPsec architecture, which provides a security suite for the IPv4 and IPv6 network layers for traffic destined to or originating at the Routing Engine. The Canada and U.S. version of the software also substantially supports Internet Key Exchange (IKE), which defines mechanisms for key generation and exchange, and manages

security associations (SAs). The JUNOS software supports manual and dynamic SAs.

The Canada and U.S. version of the JUNOS software substantially supports the following IPsec standards:

- RFC 2085, *HMAC-MD5 IP Authentication with Replay Prevention*
- RFC 2401, *Security Architecture for the Internet Protocol*
- RFC 2402, *IP Authentication Header* (except for the ES PIC)
- RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH*
- RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*
- RFC 2405, *The ESP DES-CBC Cipher Algorithm With Explicit IV*
- RFC 2406, *IP Encapsulating Security Payload (ESP)*
- RFC 2407, *The Internet IP Security Domain of Interpretation for ISAKMP*
- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 2409, *The Internet Key Exchange (IKE)*
- RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec* [sic]
- RFC 2412, *The OAKLEY Key Determination Protocol*
- RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec* [sic]
- RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*
- Internet draft draft-eastlake-sha2-02.txt, *US Secure Hash Algorithms (SHA and HMAC-SHA)* (expires July 2006)
- Layer 2 Tunneling Protocol (L2TP) client services—Services that enable support for tunneling Point-to-Point Protocol (PPP) traffic across a network.

The JUNOS software substantially supports the following L2TP standards:

- RFC 2661, *Layer Two Tunneling Protocol “L2TP”*
- RFC 2866, *RADIUS Accounting*

- Link services—A system for providing multiple independent links between two systems.

The JUNOS software substantially supports the following link-services standards:

- RFC 1990, *The PPP Multilink Protocol (MP)* (obsoletes RFC 1717)
- RFC 2364, *PPP Over AAL5*
- RFC 2686, *The Multi-Class Extension to Multi-Link PPP*

The following restrictions apply:

- Prefix elision is not supported.
- The JUNOS PPP implementation does not support the negotiation of address field compression and protocol field compression PPP Network Control Protocol (NCP) options. A full 4-byte PPP header is always sent.

- Network Address Translation (NAT)—A security-enhancement procedure that hides the IP addresses of hosts on a private network by substituting publicly visible addresses for them.

The JUNOS software substantially supports the following NAT standards:

- RFC 1631, *The IP Network Address Translator (NAT)*
- RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*
- RFC 3022, *Traditional IP Network Address Translator (Traditional NAT)*

- Real-time performance monitoring (RPM)—Tools for configuring active probes to track and monitor traffic. The JUNOS software provides MIB support with extensions in substantial support of RFC 2925, *Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations*.
- Session Initiation Protocol (SIP) application—The NAT and stateful firewall services support SIP dialogs and UDP IPv4 transport of SIP messages. The JUNOS software substantially supports RFC 3261, *SIP: Session Initiation Protocol*.
- Stateful firewall—A type of firewall filter that considers state information derived from previous communications and other applications when evaluating traffic.
- Tunnel services—A method for transmitting traffic along a secure path in a public network. The JUNOS software substantially supports the tunneling standards listed in “Supported Standards for GRE and IP-IP Interfaces” on page 21.
- Voice services—A utility to transport packetized voice traffic over an IP network infrastructure.

The JUNOS software substantially supports the following voice services standards:

- RFC 2508, *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*
- RFC 2509, *IP Header Compression over PPP*

Supported DLSw Standards

The JUNOS software substantially supports the following data link switching (DLSw) standards:

- RFC 1795, *Data Link Switching: Switch-to-Switch Protocol AIW DLSw RIG: DLSw Closed Pages, DLSw Standard Version 1.0*
- RFC 2166, *APPN Implementer's Workshop Closed Pages Document—DLSw v2.0 Enhancements*

Supported Interface Standards

The JUNOS software substantially supports the standards for the interface types in the following sections:

- Supported Standards for ATM Interfaces on page 20
- Supported Standards for Frame Relay Interfaces on page 20
- Supported Standards for GRE and IP-IP Interfaces on page 21
- Supported Standards for PPP Interfaces on page 21
- Supported Standards for Serial Interfaces on page 22
- Supported Standard for T3 Interfaces on page 22

Supported Standards for ATM Interfaces

The JUNOS software substantially supports the following ATM standards:

- International Telecommunication Union–Telecommunication Standardization (ITU-T) Recommendation I.432.3, *B-ISDN user-network interface - Physical layer specification: 1544 kbit/s and 2048 kbit/s operation*
- RFC 1483, *Multiprotocol Encapsulation over ATM Adaptation Layer 5* (routed protocol data units [PDUs] only)
- RFC 2225, *Classical IP and ARP over ATM* (responses only)
- RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5* (routed PDUs and Ethernet bridged PDUs only)

Supported Standards for Frame Relay Interfaces

The JUNOS software substantially supports the following Frame Relay standards:

- American National Standards Institute (ANSI), *Annex D, Additional Procedures for Permanent Virtual Connections (PVCs) Using Unnumbered Information Frames to T1.617-1991, Integrated Services Digital Network (ISDN)—Signaling Specification for Frame Relay Bearer Service for Digital Subscriber Signaling System Number 1 (DSS1)*
- MFA Forum standard FRF.12, *Frame Relay Fragmentation Implementation Agreement*
- FRF.15, *End-to-End Multilink Frame Relay Implementation Agreement*

- FRF.16.1, *Multilink Frame Relay UNI/NNI Implementation Agreement*
- ITU-T, *Annex A, Additional procedures for Permanent Virtual Connection (PVC) status management (using Unnumbered Information frames)* to Recommendation Q.933, *ISDN Digital Subscriber Signalling System No. 1 (DSS1) - Signalling specifications for frame mode switched and permanent virtual connection control and status monitoring*
- RFC 1973, *PPP in Frame Relay*
- RFC 2427, *Multiprotocol Interconnect over Frame Relay* (obsoletes RFC 1490)
- RFC 2590, *Transmission of IPv6 Packets over Frame Relay Networks Specification*
- Internet draft draft-martini-frame-encap-mpls-01.txt, *Frame Relay Encapsulation over Pseudo-Wires* (except translation of the command/response bit and sequence numbers and padding; expires December 2002)

Supported Standards for GRE and IP-IP Interfaces

The JUNOS software substantially supports the following generic routing encapsulation (GRE) and IP-IP standards:

- RFC 1701, *Generic Routing Encapsulation (GRE)*
- RFC 1702, *Generic Routing Encapsulation over IPv4 networks*
- RFC 2003, *IP Encapsulation within IP*
- RFC 2547, *BGP/MPLS VPNs* (over GRE tunnels)
- RFC 2784, *Generic Routing Encapsulation (GRE)*
- RFC 2890, *Key and Sequence Number Extensions to GRE*. The JUNOS software supports the key field, but not the sequence number field.

Supported Standards for PPP Interfaces

The JUNOS software substantially supports the following Point-to-Point Protocol (PPP) standards:

- RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*
- RFC 1334, *PPP Authentication Protocols*
- RFC 1661, *The Point-to-Point Protocol (PPP)*
- RFC 1662, *PPP in HDLC-like Framing*
- RFC 1717, *The PPP Multilink Protocol (MP)* (see also RFC 1990)
- RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*
- RFC 1989, *PPP Link Quality Monitoring*
- RFC 1990, *The PPP Multilink Protocol (MP)* (see also RFC 1717)
- RFC 2153, *PPP Vendor Extensions*
- RFC 2364, *PPP Over AAL5*

- RFC 2615, *PPP over SONET/SDH*
- RFC 2686, *The Multi-Class Extension to Multi-Link PPP*

The following restrictions apply:

- Prefix elision is not supported.
- The JUNOS implementation of PPP does not support the negotiation of address field compression and protocol field compression PPP NCP options. A full 4-byte PPP header is always sent.

Supported Standards for Serial Interfaces

The JUNOS software substantially supports the following standards for serial interfaces:

- ITU-T Recommendation V.35, *Data transmission at 48 kilobits per second using 60-108 kHz group band circuits*
- ITU-T Recommendation X.21 (1992), *Interface between Data Terminal Equipment and Data Circuit-terminating Equipment for synchronous operation on public data networks*

Supported Standard for T3 Interfaces

The JUNOS software substantially supports ITU-T Recommendation G.703, *Physical/electrical characteristics of hierarchical digital interfaces*.

Supported Chassis Configuration Features

The JUNOS software enables you to configure several properties of the routing platform chassis, including the following:

- Conditions that activate the red and yellow alarm LEDs on the routing platform's craft interface
- SONET/SDH framing and concatenation properties for individual PICs
- Source for clock synchronization
- Synchronization of the system Stratum 3 clock to an external source (M320 and M40e routing platforms only)

Supported CoS Standards and Features

For interfaces that carry IPv4, IPv6, or MPLS traffic, JUNOS CoS features provide multiple classes of service for different applications. You can configure multiple forwarding classes for transmitting packets, defining which packets are placed into each output queue, scheduling the transmission service level for each queue, and managing congestion using a Random Early Detection (RED) algorithm.

JUNOS CoS features are supported on all interface types except the following:

- **cau4**—Channelized STM1 IQ interface (configured on the Channelized STM1 IQ PIC)
- **coc1**—Channelized OC1 IQ interface (configured on the Channelized OC12 IQ PIC)
- **coc12**—Channelized OC12 IQ interface (configured on the Channelized OC12 IQ PIC)
- **cstm-1**—Channelized STM1 IQ interface (configured on the Channelized STM1 IQ PIC)
- **ct1**—Channelized T1 IQ interface (configured on the Channelized DS3 IQ PIC or Channelized OC12 IQ PIC)
- **ct3**—Channelized T3 IQ interface (configured on the Channelized DS3 IQ PIC or Channelized OC12 IQ PIC)
- **ce1**—Channelized E1 IQ interface (configured on the Channelized E1 IQ PIC or Channelized STM1 IQ PIC)
- **dsc**—Discard interface
- **fxp**—Management and internal Ethernet interfaces
- **lo**—Loopback interface, which is internally generated
- **pd**—Interface that de-encapsulates packets on a Platform Independent Multicast (PIM) rendezvous point (RP) routing platform
- **pe**—Interface on a first-hop RP that encapsulates packets destined for the RP routing platform
- **vt**—Virtual loopback tunnel interface

JUNOS CoS applications support the following range of mechanisms:

- **Differentiated Services (DiffServ)**—Implemented as six bits of the type-of-service (ToS) byte in the IP header. The JUNOS software uses DiffServ code points (DSCPs) in the IP ToS field to determine the forwarding class associated with each packet.
- **Two-rate tricolor marking**—For T-series platforms with Enhanced II FPCs, you can configure CoS traffic policing using two-rate tricolor marking (trTCM), which provides three levels of drop precedence (also called packet loss priority [PLP]). Two-rate TCM is a “color-aware” method of traffic policing—high, medium, and low loss priorities are mapped to the colors red, yellow, and green. The color of a packet, which is used or set by the TCM policer, corresponds to the packet’s loss priority. trTCM is defined in RFC 2698, *A Two Rate Three Color Marker*.
- **Layer 2 to Layer 3 CoS mapping**—JUNOS CoS applications substantially support setting a Layer 3 packet’s forwarding class and loss priority value based on information in the Layer 2 packet header. Output involves mapping the forwarding class and loss priority value to a Layer 2-specific marking. You can configure the JUNOS software to mark the Layer 2 and Layer 3 headers simultaneously.

- MPLS EXP—JUNOS CoS applications support mapping of MPLS experimental (EXP) bit settings to forwarding classes and vice versa.
- VPN outer label marking—JUNOS CoS applications support setting of outer label EXP bits based on MPLS EXP mapping.

JUNOS CoS features include the following:

- Classifiers—Assign incoming packets to a forwarding class and loss priority, and direct packets to output queues based on the forwarding class. Two general types of classifiers are supported:
 - Behavior aggregate (BA) or code point traffic classifiers—Determine each packet's forwarding class and loss priority. BA classifiers allow setting of the forwarding class and loss priority of a packet based on DSCP bits, IP precedence bits, MPLS EXP bits, and IEEE 802.1p bits. The default classifier is based on IP precedence bits.
 - Multifield (MF) traffic classifiers—Set a packet's forwarding class and loss priority based on packet filter rules.
- Forwarding classes—Determine the forwarding, scheduling, and marking policies applied to packets as they transit the routing platform. Four forwarding classes are supported: best effort, assured forwarding, expedited forwarding, and network control. Together with loss priority, the forwarding class defines the per-hop behavior.
- Forwarding policy options—Associate forwarding classes with next hops. Also enable creation of classification overrides, which assign forwarding classes to sets of prefixes.
- Loss priorities—Set a packet's priority to be discarded. Typically, packets exceeding some service level are marked with a high loss priority. Loss priority affects the scheduling of a packet. Loss priority is set by configuring a classifier or a policer.
- Oversubscribing interface bandwidth (Gigabit Ethernet IQ and Channelized IQ PICs)—Configures shaping rates so that their sum exceeds the physical Ethernet bandwidth.
- Rewrite markers—Change the code-point value of outgoing packets. Rewriting, or marking, outbound packets is useful when the routing platform is at the border of a network and must alter the code points to meet the policies of the targeted peer.
- Simple filters for metropolitan Ethernet applications (4-port and 8-port Gigabit Ethernet IQ2 PICs only)—Classify IPv4 traffic based on noncomplex filters.

- Transmission scheduling and rate control—Provides a variety of tools to manage traffic flows:
 - Schedulers—Define the priority, bandwidth, delay buffer size, rate control status, and RED drop profiles to be applied to a particular forwarding class for packet transmission.
 - Fabric schedulers (T-series platforms only)—Identify a packet as high or low priority based on its forwarding class.
 - Policers—Limit traffic of a certain class to a specified bandwidth and burst size. Packets exceeding the policer limits can be discarded, or can be assigned to a different forwarding class, to a different loss priority, or to both. Policers are defined with filters that can be associated with either input or output interfaces.
- Virtual channels and virtual channel groups (J-series Services Routers only)—Direct traffic into a virtual channel and apply bandwidth limits to the channel.

The JUNOS software substantially supports the following CoS standards:

- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2475, *An Architecture for Differentiated Services*
- RFC 2597, *Assured Forwarding PHB Group*
- RFC 2598, *An Expedited Forwarding PHB*
- RFC 2697, *A Single Rate Three Color Marker*
- RFC 2698, *A Two Rate Three Color Marker*

Supported Routing Table Features

The JUNOS software maintains two databases for routing information:

- Routing table—Contains all the routing information learned by all routing protocols. (Some vendors refer to this kind of table as a routing information base [RIB].)
- Forwarding table—Contains the routes actually used to forward packets. (Some vendors refer to this kind of table as a forwarding information base [FIB].)

By default, the JUNOS software maintains three routing tables: one for IPv4 unicast routes, a second for multicast routes, and a third for Multiprotocol Label Switching (MPLS). You can configure additional routing tables.

The JUNOS software maintains separate routing tables for IPv4 and IPv6 routes.

The JUNOS software installs all active routes from the routing table into the forwarding table. The active routes are routes that are used to forward packets to their destinations. The JUNOS kernel maintains a master copy of the forwarding table. It copies the forwarding table to the Packet Forwarding Engine, which is the component responsible for forwarding packets.

The JUNOS routing protocol process generally determines the active route by selecting the route with the lowest preference value. The JUNOS software provides support for alternate and tiebreaker preferences, and some of the routing protocols, including BGP and MPLS, use these additional preferences.

You can add static, aggregate, and generated routes to the JUNOS routing tables, configuring the routes with one or more of the properties shown in Table 7 on page 26.

Table 7: Routing Table Route Properties

Description	Static	Aggregate	Generated
Destination address	X	X	X
Default route to the destination	X	X	X
IP address or interface of the next hop to the destination	X	–	–
LSP as next hop	X	–	–
Drop the packets, install a reject route for this destination, and send ICMP unreachable messages	X	X	X
Drop the packets, install a reject route for this destination, but do not send ICMP unreachable messages	X	X	X
Cause packets to be received by the local routing platform	X	–	–
Associate a metric value with the route	X	X	X
Type of route	X	X	X
Preference values	X	X	X
Additional preference values	X	X	X
Independent preference (qualified-next-hop statement)	X	–	–
BGP community information to associate with the route	X	X	X
Autonomous system (AS) path information to associate with the route	X	X	X
OSPF tag strings to associate with the route	X	X	X
Do not install active static routes into the forwarding table	X	–	–
Install the route into the forwarding table	X	–	–
Permanently retain a static route in the forwarding table	X	–	–
Include only the longest common leading sequences from the contributing AS paths	–	X	–
Include all AS numbers for a specific route	–	X	–

Table 7: Routing Table Route Properties (*continued*)

Description	Static	Aggregate	Generated
Retain an inactive route in the routing and forwarding tables	X	X	X
Remove an inactive route from the routing and forwarding tables	X	X	X
Active policy to associate with the route	–	X	X
Specify that a route is ineligible for readvertisement	X	–	–
Specify route to a prefix that is not a directly connected next hop	X	–	–

You can add martian addresses to the JUNOS routing tables.

Supported IP Routing Protocols

The JUNOS software substantially supports the standards for IP routing protocols listed in the following sections:

- Supported TCP/IPv4 Standards on page 27
- Supported IPv6 Standards on page 28
- Supported IS-IS and ES-IS Standards and Features on page 30
- Supported OSPF Standards and Features on page 31
- Supported RIP and RIPng Standards on page 32
- Supported ICMP and Neighbor Discovery Standards on page 33
- Supported BGP Standards on page 33
- Supported IP Multicast Standards on page 34

Supported TCP/IPv4 Standards

The JUNOS software substantially supports the following Transmission Control Protocol/IPv4 (TCP/IPv4) standards:

- RFC 768, *User Datagram Protocol*
- RFC 791, *INTERNET PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 792, *INTERNET CONTROL MESSAGE PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 793, *TRANSMISSION CONTROL PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 826, *Ethernet Address Resolution Protocol—or—Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*

- RFC 854, *TELNET PROTOCOL SPECIFICATION*
- RFC 862, *Echo Protocol*
- RFC 863, *Discard Protocol*
- RFC 896, *Congestion Control in IP/TCP Internetworks*
- RFC 919, *BROADCASTING INTERNET DATAGRAMS*
- RFC 922, *BROADCASTING INTERNET DATAGRAMS IN THE PRESENCE OF SUBNETS*
- RFC 959, *FILE TRANSFER PROTOCOL (FTP)*
- RFC 1027, *Using ARP to Implement Transparent Subnet Gateways*
- RFC 1042, *A Standard for the Transmission of IP Datagrams over IEEE 802 Networks*
- RFC 1157, *A Simple Network Management Protocol (SNMP)*
- RFC 1166, *INTERNET NUMBERS*
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
- RFC 1256, *ICMP Router Discovery Messages*
- RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*
- RFC 1519, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*
- RFC 1812, *Requirements for IP Version 4 Routers*
- RFC 1878, *Variable Length Subnet Table For IPv4*
- RFC 1948, *Defending Against Sequence Number Attacks*
- RFC 2338, *Virtual Router Redundancy Protocol* (obsoleted by RFC 3768 in April 2004)
- RFC 2873, *TCP Processing of the IPv4 Precedence Field*
- RFC 3021, *Using 31-Bit Prefixes on IPv4 Point-to-Point Links*
- RFC 3246, *An Expedited Forwarding PHB (Per-Hop Behavior)*

Supported IPv6 Standards

The JUNOS software substantially supports the following IPv6 standards:

- RFC 1157, *A Simple Network Management Protocol (SNMP)*
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
- RFC 1213, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*. The JUNOS software supports the following features:
 - MIB II and its SNMP version 2 derivatives, including the following:
 - Statistics counters
 - IP (except for the `ipRouteTable` object, which has been replaced by `ipCidrRouteTable` [RFC 2096, *IP Forwarding Table MIB*])

- SNMP management
- Interface management
- SNMP version 1 **Get** and **GetNext** requests and version 2 **GetBulk** requests
- JUNOS-specific secured access list
- Master configuration keywords
- Reconfigurations upon receipt of the SIGHUP signal
- RFC 1215, *A Convention for Defining Traps for use with the SNMP* (only MIB II SNMP version 1 traps and version 2 notifications)
- RFC 1771, *A Border Gateway Protocol 4 (BGP-4)*
- RFC 1772, *Application of the Border Gateway Protocol in the Internet*
- RFC 1901, *Introduction to Community-based SNMPv2*
- RFC 1902, *Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)*
- RFC 1905, *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*
- RFC 1981, *Path MTU Discovery for IP version 6*
- RFC 2080, *RIPng for IPv6*
- RFC 2081, *RIPng Protocol Applicability Statement*
- RFC 2283, *Multiprotocol Extensions for BGP-4*
- RFC 2373, *IP Version 6 Addressing Architecture*
- RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*
- RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*
- RFC 2462, *IPv6 Stateless Address Autoconfiguration*
- RFC 2463, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*
- RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*
- RFC 2472, *IP Version 6 over PPP*
- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2491, *IPv6 Over Non-Broadcast Multiple Access (NBMA) networks*
- RFC 2492, *IPv6 over ATM Networks*
- RFC 2526, *Reserved IPv6 Subnet Anycast Addresses*
- RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*
- RFC 2578, *Structure of Management Information Version 2 (SMIv2)*
- RFC 2675, *IPv6 Jumbograms*
- RFC 2711, *IPv6 Router Alert Option*

- RFC 2740, *OSPF for IPv6*
- RFC 2767, *Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS)*
- RFC 2878, *PPP Bridging Control Protocol (BCP)*
- RFC 2893, *Transition Mechanisms for IPv6 Hosts and Routers*
- RFC 3484, *Default Address Selection for Internet Protocol version 6 (IPv6)*
- RFC 3513, *Internet Protocol Version 6 (IPv6) Addressing Architecture*
- RFC 3515, *The Session Initiation Protocol (SIP) Refer Method*
- RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*
- Internet draft draft-ietf-dhc-dhcpv6-16.txt, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
- Internet draft draft-ietf-idr-flow-spec-00.txt, *Dissemination of flow specification rules*
- Internet draft draft-ietf-isis-ipv6-06.txt, *Routing IPv6 with IS-IS*
- Internet draft draft-ietf-l3vpn-bgp-ipv6-07.txt, *BGP-MPLS IP VPN extension for IPv6 VPN* (expires January 2006)
- Internet draft draft-ietf-ngtrans-bgp-tunnel-04.txt, *Connecting IPv6 Islands across IPv4 Clouds with BGP* (only MP-BGP over IPv4 approach)
- Internet draft draft-kato-bgp-ipv6-link-local-00.txt, *BGP4 + Peering Using IPv6 Link-local Address*
- Internet draft draft-ooms-v6ops-bgp-tunnel-06.txt, *Connecting IPv6 Islands over IPv4 MPLS using IPv6 Provider Edge Routers (6PE)* (expires July 2006, only MP-BGP over IPv4 approach)

Supported IS-IS and ES-IS Standards and Features

The JUNOS software substantially supports the following IS-IS standards:

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 8473, *Information technology — Protocol for providing the connectionless-mode network service*
- ISO/IEC 9542, *Information processing systems — Telecommunications and information exchange between systems — End system to Intermediate system routeing [sic] exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473)*
- ISO/IEC 10589, *Information technology — Telecommunications and information exchange between systems — Intermediate System to Intermediate System intra-domain routeing [sic] information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)*
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
- RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*
- RFC 2763, *Dynamic Hostname Exchange Mechanism for IS-IS*
- RFC 2966, *Domain-wide Prefix Distribution with Two-Level IS-IS*

- RFC 2973, *IS-IS Mesh Groups*
- RFC 3277, *Intermediate System to Intermediate System (IS-IS) Transient Blackhole Avoidance*
- RFC 3358, *Optional Checksums in Intermediate System to Intermediate System (ISIS)*
- RFC 3359, *Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System*
- RFC 3373, *Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies*
- RFC 3567, *Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication*
- RFC 3784, *Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)*
- RFC 3787, *Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS)*
- RFC 3847, *Restart Signaling for Intermediate System to Intermediate System (IS-IS)*
- RFC 4205, *Intermediate System to Intermediate System (IS-IS) Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*
- RFC 5120, *M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)*
- RFC 5130, *A Policy Control Mechanism in IS-IS Using Administrative Tags*
- Internet draft draft-ietf-bfd-base-05.txt, *Bidirectional Forwarding Detection* (except for the transmission of echo packets)
- Internet draft draft-ietf-isis-igp-p2p-over-lan-06.txt, *Point-to-point operation over LAN in link-state routing protocols* (expires October 2006)
- Internet draft draft-ietf-isis-ipv6-06.txt, *Routing IPv6 with IS-IS*
- Internet draft draft-ietf-isis-wg-255adj-02.txt, *Maintaining more than 255 circuits in IS-IS*

JUNOS IS-IS supports authentication for protocol exchanges (HMAC-MD5 or simple authentication), link-state packets, sequence-number packets (CSNP and PSNP), and IS-IS hello packets (IIH).

The JUNOS software supports the advertising of MPLS label-switched paths into IS-IS.

Supported OSPF Standards and Features

The JUNOS software substantially supports the following OSPF standards:

- RFC 1583, *OSPF Version 2*
- RFC 1587, *The OSPF NSSA Option*
- RFC 1793, *Extending OSPF to Support Demand Circuits*
- RFC 2328, *OSPF Version 2*

- RFC 2370, *The OSPF Opaque LSA Option* (support provided by the RSVP `update-threshold` configuration option)
- RFC 2740, *OSPF for IPv6*
- RFC 3101, *The OSPF Not-So-Stubby Area (NSSA) Option*
- RFC 3137, *OSPF Stub Router Advertisement*
- RFC 3509, *Alternative Implementations of OSPF Area Border Routers*
- RFC 3623, *Graceful OSPF Restart*
- RFC 3630, *Traffic Engineering (TE) Extensions to OSPF Version 2*
- RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*
- RFC 4552, *Authentication/Confidentiality for OSPFv3*
- RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4577, *OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4915, *Multi-Topology (MT) Routing in OSPF*
- Internet draft draft-ietf-ccamp-ospf-gmpls-extensions-12.txt, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching* (only interface switching)
- Internet draft draft-ietf-isis-igp-p2p-over-lan-03.txt, *Point-to-point operation over LAN in link-state routing protocols* (expires February 2004)
- Internet draft draft-katz-ward-bfd-02.txt, *Bidirectional Forwarding Detection* (except for the transmission of echo packets)

For a list of supported IPv6 OSPF standards, see “Supported IPv6 Standards” on page 28.

JUNOS OSPF supports the following features:

- Authentication for protocol exchanges (simple authentication)
- Extensions to support MPLS traffic engineering
- Advertisement of MPLS LSPs into OSPF

Supported RIP and RIPng Standards

The JUNOS software substantially supports the following RIP (IPv4) and RIPng (IPv6) standards:

- RFC 1058, *Routing Information Protocol*
- RFC 2080, *RIPng for IPv6*
- RFC 2081, *RIPng Protocol Applicability Statement*

- RFC 2082, *RIP-2 MD5 Authentication* (except for multiple keys using distinct key IDs)
- RFC 2453, *RIP Version 2*

For a list of supported IPv6 RIPng standards, see “Supported IPv6 Standards” on page 28.

JUNOS RIP supports authentication for all protocol exchanges (MD5 or simple authentication).

Supported ICMP and Neighbor Discovery Standards

The JUNOS software substantially supports the following standards for IPv4 ICMP and IPv6 neighbor discovery:

- RFC 1256, *ICMP Router Discovery Messages*
- RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6)*
- RFC 2462, *IPv6 Stateless Address Autoconfiguration*
- RFC 2463, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*

Supported BGP Standards

The JUNOS software substantially supports the following IPv4 BGP standards:

- RFC 1745, *BGP4/IDRP for IP—OSPF Interaction*
- RFC 1772, *Application of the Border Gateway Protocol in the Internet*
- RFC 1965, *Autonomous System Confederations for BGP*
- RFC 1966, *BGP Route Reflection—An alternative to full mesh IBGP*
- RFC 1997, *BGP Communities Attribute*
- RFC 2270, *Using a Dedicated AS for Sites Homed to a Single Provider*
- RFC 2283, *Multiprotocol Extensions for BGP-4*
- RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*
- RFC 2439, *BGP Route Flap Damping*
- RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*
- RFC 2796, *BGP Route Reflection – An Alternative to Full Mesh IBGP*
- RFC 2858, *Multiprotocol Extensions for BGP-4*
- RFC 2918, *Route Refresh Capability for BGP-4*
- RFC 3065, *Autonomous System Confederations for BGP*
- RFC 3107, *Carrying Label Information in BGP-4*
- RFC 3392, *Capabilities Advertisement with BGP-4*
- RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*

- RFC 4360, *BGP Extended Communities Attribute*
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4456, *BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)*
- RFC 4724, *Graceful Restart Mechanism for BGP*
- RFC 4781, *Graceful Restart Mechanism for BGP with MPLS*
- RFC 4893, *BGP Support for Four-octet AS Number Space*
- Internet draft draft-ietf-idr-flow-spec-00.txt, *Dissemination of flow specification rules*
- Internet draft draft-ietf-l3vpn-rfc2547bis-03.txt, *BGP/MPLS IP VPNs*
- Internet draft draft-ietf-l3vpn-bgp-ipv6-07.txt, *BGP/MPLS IP VPN extension for IPv6 VPN* (expires January 2006)
- Internet draft draft-ietf-ngtrans-bgp-tunnel-04.txt, *Connecting IPv6 Islands across IPv4 Clouds with BGP* (expires July 2002)
- Internet draft draft-ietf-ppvpn-rfc2547bis-00.txt, *BGP/MPLS IP VPNs* (expires January 2002)
- Internet draft draft-kato-bgp-ipv6-link-local-00.txt, *BGP4 + Peering Using IPv6 Link-local Address*
- Internet draft draft-ooms-v6ops-bgp-tunnel-06.txt, *Connecting IPv6 Islands over IPv4 MPLS using IPv6 Provider Edge Routers (6PE)* (expires July 2006)

For a list of supported IPv6 BGP standards, see “Supported IPv6 Standards” on page 28.

JUNOS BGP supports authentication for protocol exchanges (MD5 authentication).

Supported IP Multicast Standards

The JUNOS software substantially supports the following IP multicast standards:

- RFC 1112, *Host Extensions for IP Multicasting* (defines IGMP Version 1)
- RFC 2236, *Internet Group Management Protocol, Version 2*
- RFC 2327, *SDP: Session Description Protocol*
- RFC 2362, *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*
- RFC 2365, *Administratively Scoped IP Multicast*
- RFC 2547, *BGP/MPLS VPNs*
- RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*
- RFC 2974, *Session Announcement Protocol*
- RFC 2858, *Multiprotocol Extensions for BGP-4*
- RFC 3031, *Multiprotocol Label Switching Architecture*
- RFC 3208, *PGM Reliable Transport Protocol Specification*

- RFC 3376, *Internet Group Management Protocol, Version 3* (SSM include mode only)
- RFC 3446, *Anycast Rendezvous [sic] Point (RP) Mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*
- RFC 3569, *An Overview of Source-Specific Multicast (SSM)*
- RFC 3590, *Source Address Selection for the Multicast Listener Discovery (MLD) Protocol* (SSM include mode only)
- RFC 3618, *Multicast Source Discovery Protocol (MSDP)*
- RFC 3973, *Protocol Independent Multicast – Dense Mode (PIM-DM): Protocol Specification (Revised)*
- RFC 4601, *Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification (Revised)*
- Internet draft draft-holbrook-idmr-igmpv3-ssm-07.txt, *Using IGMPv3 and MLDv2 for Source-Specific Multicast* (expires December 2004)
- Internet draft draft-ietf-idmr-dvmrp-v3-11.txt, *Distance Vector Multicast Routing Protocol*
- Internet draft draft-ietf-mboned-ssm232-08.txt, *Source-Specific Protocol Independent Multicast in 232/8*
- Internet draft draft-ietf-mmusic-sap-00.txt, *SAP: Session Announcement Protocol*
- Internet draft draft-ietf-pim-sm-bsr-05.txt, *Bootstrap Router (BSR) Mechanism for PIM* (except for the scoping mechanism)
- Internet draft draft-ietf-ssm-arch-06.txt, *Source-Specific Multicast for IP*
- Internet draft draft-raggarwa-l3vpn-2547-mvpn-00.txt, *Base Specification for Multicast in BGP/MPLS VPNs* (expires December 2004)
- Internet draft draft-rosen-vpn-mcast-06.txt, *Multicast in MPLS/BGP VPNs* (expires April 2004)
- Internet draft draft-rosen-vpn-mcast-07.txt, *Multicast in MPLS/BGP VPNs* (Only section 7, “Data MDT: Optimizing flooding,” is supported.)

Supported Standards for MPLS Applications

The JUNOS software substantially supports standards for MPLS applications as listed in the following sections:

- Supported LDP Standards on page 36
- Supported GMPLS Standards on page 36
- Supported MPLS Standards on page 37
- Supported RSVP Standards on page 38

Supported LDP Standards

The JUNOS software substantially supports the following LDP standards:

- RFC 3036, *LDP Specification*
 - For the following features described in the indicated sections of the RFC, the JUNOS software supports one of the possible modes but not the other:
 - Label distribution control (section 2.6.1): Ordered mode is supported, but not Independent mode.
 - Label retention (section 2.6.2): Liberal mode is supported, but not Conservative mode.
 - Label advertisement (section 2.6.3): Downstream Unsolicited mode is supported, but not Downstream on Demand mode.
- RFC 3212, *Constraint-Based LSP Setup using LDP*
- RFC 3215, *LDP State Machine*
- RFC 3478, *Graceful Restart Mechanism for Label Distribution Protocol*

Supported GMPLS Standards

The JUNOS software substantially supports the following Generalized MPLS (GMPLS) standards:

- RFC 3471, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description* (The following features are supported: bidirectional LSPs [upstream label only], control channel separation, generalized label [suggested label only], and generalized label request [bandwidth encoding only].)
- RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation [sic] Protocol-Traffic Engineering (RSVP-TE) Extensions* (Only Section 9, "Fault Handling," is supported.)
- RFC 4206, *Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)*
- Internet draft draft-ietf-ccamp-gmpls-routing-09.txt, *Routing Extensions in Support of Generalized Multi-Protocol Label Switching* (Only interface switching is supported.)
- Internet draft draft-ietf-ccamp-gmpls-rsvp-te-ason-02.txt, *Generalized MPLS (GMPLS) RSVP-TE Signalling in support of Automatically Switched Optical Network (ASON)* (expires January 2005)
- Internet draft draft-ietf-ccamp-gmpls-sonet-sdh-08.txt, *Generalized Multi-Protocol Label Switching Extensions for SONET and SDH Control* (Only S,U,K,L,M-format labels and SONET traffic parameters are supported.)
- Internet draft draft-ietf-ccamp-lmp-09.txt, *Link Management Protocol (LMP)*

- Internet draft draft-ietf-ccamp-ospf-gmpls-extensions-12.txt, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching* (The following sub-TLV types for the Link type, link, value (TLV) are not supported: Link Local/Remote Identifiers [type 11], Link Protection Type [type 14], and Shared Risk Link Group (SRLG) [type 16]; the Interface Switching Capability Descriptor [type 15] sub-TLV type is implemented, but is packet-switch capable only. The features described in Section 2, “Implications on Graceful Restart,” are also not supported.)
- Internet draft draft-ietf-mpls-bundle-04.txt, *Link Bundling in MPLS Traffic Engineering*

Supported MPLS Standards

The JUNOS software substantially supports the following MPLS standards:

- RFC 2547, *BGP/MPLS VPNs*
- RFC 2702, *Requirements for Traffic Engineering Over MPLS*
- RFC 2858, *Multiprotocol Extensions for BGP-4*
- RFC 3031, *Multiprotocol Label Switching Architecture*
- RFC 3032, *MPLS Label Stack Encoding*
- RFC 3063, *MPLS Loop Prevention Mechanism*
- RFC 3140, *Per Hop Behavior Identification Codes*
- RFC 3208, *PGM Reliable Transport Protocol Specification* (only the network element)
- RFC 3270, *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services* (E-LSPs only)
- RFC 3443, *Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks*
- RFC 3469, *Framework for Multi-Protocol Label Switching (MPLS)-based Recovery*
- RFC 3564, *Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering*
- RFC 4124, *Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering*
- RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*
- RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*
- RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*. (The JUNOS software supports the traceroute functionality, but only on transit routers.)
- Internet draft draft-ietf-bfd-mpls-02.txt, *BFD for MPLS LSPs*
- Internet draft draft-ietf-l3vpn-rfc2547bis-04.txt, *BGP/MPLS IP VPNs*
- Internet draft draft-ietf-mpls-icmp-01.txt, *ICMP Extensions for MultiProtocol [sic] Label Switching*

- Internet draft draft-ietf-mpls-label-encaps-07.txt, *MPLS Label Stack Encoding*
- Internet draft draft-ietf-mpls-rsvp-lsp-fastreroute-03.txt, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels* (except for node protection in facility backup)
- Internet draft draft-ietf-mpls-soft-preemption-00.txt, *MPLS Traffic Engineering Soft preemption*
- Internet draft draft-ietf-ppvpn-rfc2547bis-03.txt, *BGP/MPLS VPNs*
- Internet draft draft-martini-l2circuit-encap-mpls-07.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*

The JUNOS software differs from the Internet draft in the following ways:

- A packet with a sequence number of 0 is treated as out of sequence.
- Any packet which does not have the next incremental sequence number is considered out of sequence.
- When out-of-sequence packets arrive, the expected sequence number for the neighbor is set to the sequence number in the Layer 2 circuit control word.
- Internet draft draft-martini-l2circuit-trans-mpls-14.txt, *Transport of Layer 2 Frames Over MPLS*
- Internet draft draft-raggarwa-mpls-p2mp-te-02.txt, *Establishing Point to Multipoint MPLS TE LSPs* (except for no-adjacent signaling for branch LSPs, make-before-break and fast reroute, and LSP hierarchy using point-to-point LSPs)

Supported RSVP Standards

The JUNOS software substantially supports the following RSVP standards:

- RFC 2205, *Resource ReSerVation Protocol (RSVP)—Version 1 Functional Specification*
- RFC 2209, *Resource ReSerVation Protocol (RSVP)—Version 1 Message Processing Rules*
- RFC 2210, *The Use of RSVP with IETF Integrated Services*
- RFC 2211, *Specification of the Controlled-Load Network Element Service*
- RFC 2212, *Specification of Guaranteed Quality of Service*
- RFC 2215, *General Characterization Parameters for Integrated Service Network Elements*
- RFC 2216, *Network Element Service Specification Template*
- RFC 2745, *RSVP Diagnostic Messages*
- RFC 2747, *RSVP Cryptographic Authentication* (updated by RFC 3097)
- RFC 2961, *RSVP Refresh Overhead Reduction Extensions*
- RFC 3097, *RSVP Cryptographic Authentication—Updated Message Type Value* (see also RFC 2747)

- RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels* (the Null Service Object for maximum transmission unit [MTU] signaling in RSVP is not supported)
- RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation [sic] Protocol-Traffic Engineering (RSVP-TE) Extensions* (only Section 9, “Fault Handling,” is supported)
- RFC 3477, *Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)*
- RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels* (except for node protection in facility backup)
- RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*
- RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*
- Internet draft draft-ietf-mpls-rsvp-te-p2mp-01.txt, *Extensions to RSVP-TE for Point to Multipoint TE LSPs* (expires June 2005)

Supported Routing Policy Features

The JUNOS software provides a routing policy language that enables you to control the transfer of routing information between the routing protocols and the routing tables, and between the routing tables and the forwarding table.

You can configure policies that examine characteristics of incoming and outgoing routes, including the following:

- Address family
- Aggregate route contributors
- BGP AS path, AS path group, community, and origin attributes
- Destination prefix
- IP address or list of addresses
- IS-IS level
- Metric
- Multicast source address
- Neighbor (peer)
- Next-hop address
- OSPF area identifier
- OSPF external route and tags
- Preference
- Protocol from which route was learned
- Router interface

- Routing instance
- Routing table

You can configure policies to perform certain actions when routes match specified characteristics, including the following actions:

- Accept the routes
- Add, delete, or set the BGP community
- Add or delete a BGP local preference
- Apply BGP route-damping parameters
- Apply CoS parameters
- Choose a next hop to install into the forwarding table
- Create a forwarding class
- Evaluate the next term in the policy
- Evaluate the next policy in a policy chain
- Extract the last AS number from an AS path
- Maintain packet counts based on source and destination address
- Modify the metric value
- Modify the preference value
- Perform per-packet load balancing
- Prepend an AS path
- Reject the routes
- Set the BGP MED and origin attribute
- Set the external metric type
- Set the next hop
- Specify or modify OSPF tags

Supported Packet Filtering Standards and Features

The JUNOS software provides a packet-filtering language that enables you control the flow of packets being forwarded to a network destination, as well as packets destined for and sent by the routing platform. It substantially supports the following standards:

- RFC 792, *INTERNET CONTROL MESSAGE PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*
- RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*
- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2475, *An Architecture for Differentiated Services*

- RFC 2597, *Assured Forwarding PHB Group*
- RFC 2598, *An Expedited Forwarding PHB*

You can configure filters that examine characteristics of incoming and outgoing packets, including the following:

- Bit fields in the packet header, including IP fragmentation flags, IP options, and TCP flags
- IPv4 numeric range, including destination port, DSCP value, fragment offset, ICMP code, ICMP packet type, interface group, IP precedence, packet length, protocol, and TCP and UDP source and destination port
- IPv6 numeric range, including CoS priority, destination address, destination port, ICMP code, ICMP packet type, interface group, IP address, next header, packet length, source address, source port, and TCP and UDP source and destination port
- Source and destination address and prefix list

You can configure filters to perform certain actions when packets match specified characteristics, including the following actions:

- Accept the packets
- Apply a policer
- Classify the packets based on their source address
- Discard the packets
- Evaluate the next term in the filter
- Increment a packet counter
- Reject the packets
- Sample the packets
- Set the packets' loss priority
- Specify a forwarding class
- Specify an IPsec SA
- Specify the forwarding path that the packets follow within the routing platform
- Write an alert or message to the system log

Supported Policing Standard and Features

The JUNOS software supports policing, or rate limiting, to limit the amount of traffic that passes through an interface. It substantially supports RFC 2698, *A Two Rate Three Color Marker*.

The JUNOS implementation of policing uses a token-bucket algorithm and supports the following features:

- Adaptive shaping for Frame Relay traffic
- Virtual channels

Supported VPN, VPLS, and Layer 2 Circuit Standards

The JUNOS software substantially supports the following Internet draft for Layer 2 VPNs: draft-kompella-ppvpn-l2vpn-03.txt, *Layer 2 VPNs Over Tunnels*.

The JUNOS software substantially supports the following Layer 3 VPN standards:

- RFC 1918, *Address Allocation for Private Internets*
- RFC 2283, *Multiprotocol Extensions for BGP-4*
- RFC 2685, *Virtual Private Networks Identifier*
- RFC 2858, *Multiprotocol Extensions for BGP-4*
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*. (The JUNOS software supports the traceroute functionality, but only on transit routers.)
- RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4577, *OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*
- RFC 4659, *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*
- RFC 4684, *Constrained Route Distribution for Border Gateway Protocol/MultiProtocol [sic] Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*

The JUNOS software supports the following interprovider and carrier-of-carriers VPN standards:

- RFC 3107, *Carrying Label Information in BGP-4*
- RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*
- Internet draft draft-marques-ppvpn-ibgp-00.txt, *RFC2547bis networks using internal BGP as PE-CE protocol*

The JUNOS software substantially supports the following multicast VPN standards:

- Internet draft draft-ietf-l3vpn-2547bis-mcast-bgp-03.txt, *BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs*
- Internet draft draft-ietf-l3vpn-2547bis-mcast-02.txt, *Multicast in MPLS/BGP IP VPNs*

The JUNOS software substantially supports the following virtual private LAN service (VPLS) standards:

- RFC 4761, *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*
- RFC 4762, *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling* (FEC 128, control bit 0, and Ethernet pseudowire type hexadecimal 0x0005)

The JUNOS software substantially supports the following Layer 2 circuit standards:

- Internet draft draft-martini-l2circuit-encap-mpls-07.txt, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*

The JUNOS software differs from the Internet draft in the following ways:

- A packet with a sequence number of 0 is treated as out of sequence.
- Any packet that does not have the next incremental sequence number is considered out of sequence.
- When out-of-sequence packets arrive, the expected sequence number for the neighbor is set to the sequence number in the Layer 2 circuit control word.
- Internet draft draft-martini-l2circuit-trans-mpls-14.txt, *Transport of Layer 2 Frames Over MPLS*

Supported Standards for SDH and SONET Interfaces

The JUNOS software substantially supports the following SDH and SONET standards:

- ANSI T1.105-2001, *Synchronous Optical Network (SONET) – Basic Description including Multiplex Structure, Rates, and Formats*
- ANSI T1.105.02-2001, *Synchronous Optical Network (SONET) – Payload Mappings*
- ANSI T1.105.06-2002, *Synchronous Optical Network (SONET): Physical Layer Specifications*
- GR-253-CORE (Telcordia Generic Requirements standard), *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria* (replaces GR-1377-CORE, *SONET OC-192 Transport System Generic Criteria*)
- GR-499-CORE, *Transport Systems Generic Requirements (TSGR): Common Requirements*
- ITU-T Recommendation G.691, *Optical interfaces for single channel STM-64 and other SDH systems with optical amplifiers*
- ITU-T Recommendation G.707 (1996), *Network node interface for the synchronous digital hierarchy (SDH)*
- ITU-T Recommendation G.783 (1994), *Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks*
- ITU-T Recommendation G.813 (1996), *Timing characteristics of SDH equipment slave clocks (SEC)*

- ITU-T Recommendation G.825 (1993), *The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)*
- ITU-T Recommendation G.826 (1999), *Error performance parameters and objectives for international, constant bit-rate digital paths at or above the primary rate*
- ITU-T Recommendation G.831 (1993), *Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)*
- ITU-T Recommendation G.957 (1995), *Optical interfaces for equipments and systems relating to the synchronous digital hierarchy*
- ITU-T Recommendation G.958 (1994), *Digital line systems based on the synchronous digital hierarchy for use on optical fibre cables*
- ITU-T Recommendation I.432 (1993), *B-ISDN user-network interface – Physical layer specification*
- RFC 1619, *PPP over SONET/SDH*

Supported Standards for Ethernet Interfaces

The JUNOS software substantially supports the following Ethernet standards:

- IEEE 802.1Q, *Virtual LANs*
- IEEE 802.3, *Carrier Sense Multiple Access with Collision Detection (CSMA/CD)*
- IEEE 802.3ad, *Aggregation of Multiple Link Segments*

Supported Miscellaneous Routing Features

The JUNOS software supports unicast reverse-path forwarding.

JUNOS routing protocols and PIM sparse mode support graceful restart, which enables a protocol, before it restarts, to inform its adjacent neighbors and peers of its condition.

The JUNOS software supports graceful Routing Engine switchover for routing platforms in which Adaptive Services (AS) Physical Interface Cards (PICs) are installed. When a Routing Engine switchover occurs, features using adaptive services are interrupted momentarily. Features that do not use adaptive services continue uninterrupted. After switchover, all features are restored and packet forwarding continues. Note, however, that L2TP does not come up after a graceful switchover.

The JUNOS software supports routing instances, which enables you to create multiple instances of BGP, IS-IS, OSPF, PIM, RIP, and static routes.

The JUNOS software supports logical systems, which enables you to create multiple logical routing devices within a single routing platform.

Chapter 3

JUNOS Configuration Specification

This chapter describes the configuration features available on Juniper Networks routing platforms. For more information about displaying and changing routing platform configuration, see the *JUNOS CLI User Guide*.

Configuration Operations

To configure a Juniper Networks routing platform, you define a hierarchy of configuration statements, either by typing them in JUNOS command-line interface (CLI) configuration mode, or by loading a text file that contains the statements in formatted ASCII.

You can also write a JUNOScript or NETCONF application to add, modify, or delete configuration information; for more information, see “JUNOS XML, JUNOScript, and NETCONF APIs” on page 8.

In CLI configuration mode, you issue commands to perform the following operations:

- Activate (commit) a configuration
- Display the current configuration
- Globally search and replace text; you can use regular expressions to locate and replace identifiers and values
- Insert, copy, and delete statements
- Issue operational mode commands
- List the commands that were previously issued during the session
- List the users currently editing the configuration
- Move among the levels of the configuration hierarchy
- Save a configuration to a file
- Verify the syntactic correctness of a configuration before activating it

When you load a text file that contains a configuration, you can commit it immediately to activate the configuration on the routing platform, or you can alter it in CLI configuration mode and commit it later. When loading the file, you can specify that it overwrite the entire configuration or portions of it, or that nonoverlapping portions be merged with the existing configuration.

You can include comments in the configuration to identify or explain particular statement or subhierarchies.

You can copy the contents of currently active file system partitions on the routing platform to standby partitions that are not active.

Configuration Versions

When you change the configuration in CLI configuration mode, your changes are stored in a copy of the currently active configuration. The copy is called the *candidate configuration*. By default, multiple users can edit the candidate configuration at the same time, and all users immediately see the changes made by everyone. Alternatively, you can lock other users out of the candidate configuration as you enter CLI configuration mode, making them unable to change the candidate configuration until you release the lock. For finer-grained control, you can also allow multiple users each to edit nonoverlapping portions of the configuration and to commit only their own changes.

For the candidate configuration to become the *active* configuration running on the routing platform, you must commit it. The candidate file is checked for proper syntax, activated, and saved to a file as the currently active configuration. If the candidate configuration is committed while multiple users are editing it, all changes made by all the users take effect.

In addition to saving the candidate and active configurations, the CLI saves the previous 49 configurations that were committed. You can *roll back* to any of the saved previous versions, making it the candidate configuration and then committing it if desired.

Configuration Groups

JUNOS *configuration groups* are named collections of configuration statements that are defined at the [edit groups] level of the hierarchy and referenced at other locations in the hierarchy. The statements in the configuration group are said to be *inherited* at the referring location and apply at that location as though they were actually typed there. You can apply the same group in multiple locations in the configuration, and apply different sections of one group to different locations.

Part 2

Configuration Commands and Statements

- Configuration Mode Commands on page 49
- Complete JUNOS Configuration Statement Hierarchy on page 51

Chapter 4

Configuration Mode Commands

The complete list of JUNOS command-line interface (CLI) configuration mode commands follows. You can display this list in configuration mode by typing the question mark at any hierarchy level:

```
[edit any-level]
user@host# ?
Possible completions:
<[Enter]>      Execute this command
activate       Remove the inactive tag from a statement
annotate       Annotate the statement with a comment
commit         Commit current set of changes
copy           Copy a statement
deactivate     Add the inactive tag to a statement
delete         Delete a data element
edit           Edit a sub-element
exit           Exit from this level
extension      Extension operations
help           Provide help information
insert         Insert a new ordered data element
load           Load configuration from ASCII file
quit           Quit from this level
rename         Rename a statement
replace        Replace character string in configuration
rollback       Roll back to previous committed configuration
run            Run an operational-mode command
save           Save configuration to ASCII file
set            Set a parameter
show           Show a parameter
status         Show users currently editing configuration
top            Exit to top level of configuration
up             Exit one level of configuration
update         Update private database
wildcard       Wildcard operations
```

For information about operational mode commands, see the *JUNOS CLI User Guide* and the JUNOS command references.

Chapter 5

Complete JUNOS Configuration Statement Hierarchy

This chapter contains the complete hierarchy of JUNOS configuration statements.

When you are working in configuration mode, the banner on the line preceding the `user@host#` prompt indicates the current hierarchy level. In this example, the level is `[edit protocols ospf]`:

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

Use the `set ?` command to display the statements that you can include in the configuration at the current level. The `help apropos` command is also context-sensitive, displaying matching statements only at the current level and below.



NOTE: In this document, statements are listed alphabetically within each hierarchy and subhierarchy. If a subhierarchy is sufficiently long that it might be difficult to determine where it ends and its next peer statement begins, the subhierarchy appears at the end of its parent hierarchy instead of in alphabetical order. In this case, a placeholder appears in its actual alphabetical position.

For example, at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level, the family *family-name* subhierarchy has more than 20 child statements, including several subhierarchies with child statements of their own. The full family *family-name* hierarchy appears at the end of its parent hierarchy (`[edit interfaces interface-name unit logical-unit-number]`), and the following placeholder appears at its actual alphabetical position:

```
family family-name {
    ... family-configuration ...
}
```

Another exception to alphabetical order is that the `disable` statement always appears first in any hierarchy that includes it.

Only one leaf statement is valid at the top `[edit]` level of the hierarchy:

```
[edit]
access-profile profile-name;
```

Every other statement at the `[edit]` level is a container for a subhierarchy. The statements in each subhierarchy are displayed in the following sections:

- `[edit access]` Hierarchy Level on page 53
- `[edit accounting-options]` Hierarchy Level on page 59
- `[edit applications]` Hierarchy Level on page 60
- `[edit bridge-domains]` Hierarchy Level on page 61
- `[edit chassis]` Hierarchy Level on page 63
- `[edit class-of-service]` Hierarchy Level on page 68
- `[edit dynamic-profiles]` Hierarchy Level on page 72
- `[edit ethernet-switching-options]` Hierarchy Level on page 73
- `[edit event-options]` Hierarchy Level on page 75
- `[edit firewall]` Hierarchy Level on page 77
- `[edit forwarding-options]` Hierarchy Level on page 87
- `[edit groups]` Hierarchy Level on page 94
- `[edit interfaces]` Hierarchy Level on page 95
- `[edit logical-systems]` Hierarchy Level on page 110
- `[edit multicast-snooping-options]` Hierarchy Level on page 111
- `[edit poe]` Hierarchy Level on page 112
- `[edit policy-options]` Hierarchy Level on page 113
- `[edit protocols]` Hierarchy Level on page 117
- `[edit routing-instances]` Hierarchy Level on page 186
- `[edit routing-options]` Hierarchy Level on page 194
- `[edit schedulers]` Hierarchy Level on page 201
- `[edit security]` Hierarchy Level on page 202
- `[edit services]` Hierarchy Level on page 222
- `[edit snmp]` Hierarchy Level on page 239
- `[edit switch-options]` Hierarchy Level on page 243
- `[edit system]` Hierarchy Level on page 244
- `[edit virtual-chassis]` Hierarchy Level on page 256
- `[edit vlans]` Hierarchy Level on page 257

[edit access] Hierarchy Level

```

access {
  address-assignment {
    pool pool-name family inet {
      dhcp-attributes {
        boot-file filename;
        boot-server hostname;
        domain-name domain-name;
        grace-period seconds;
        maximum-lease-time (seconds | infinite);
        name-server {
          address;
        }
        netbios-node-type (b-node | h-node | m-node | p-node);
        option option-index (array type-name [ type-values ] | byte 8-bit-value |
          flag (false | off | on | true) | integer signed-32-bit-value | ip-address address |
          short signed-16-bit-value | string text-string | unsigned-integer 32-bit-value |
          unsigned-short 16-bit-value);
        option-match {
          option-82 {
            circuit-id id-number range range-name;
            remote-id id-number range range-name;
          }
        }
        router {
          address;
        }
        tftp-server hostname;
        wins-server {
          address;
        }
      }
      host hostname {
        hardware-address mac-address;
        ip-address ip-address;
      }
      network ip-prefix</prefix-length>;
      range name {
        low lower-limit high upper-limit;
      }
    }
  }
  address-pool name {
    address address-or-prefix value;
    address-range low lower-limit high upper-limit;
    primary-dns primary-dns;
    primary-wins primary-wins;
    secondary-dns secondary-dns;
    secondary-wins secondary-wins;
  }
  firewall-authentication {
    pass-through {
      default-profile profile-name;
      (ftp | http | telnet) {

```

```

        banner {
            fail message-text;
            login message-text;
            success message-text;
        }
    }
}
traceoptions {
    file filename <files number> <match regular-expression>
    <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
web-authentication {
    banner {
        success message-text;
    }
    default-profile profile-name;
}
}
group-profile group-profile-name {
    l2tp {
        interface-id interface-identifier;
        lcp-renegotiation;
        local-chap;
        maximum-sessions-per-tunnel number;
        multilink {
            drop-timeout time;
            fragmentation-threshold bytes;
        }
    }
}
ppp {
    cell-overhead;
    encapsulation-overhead bytes;
    framed-pool pool-identifier;
    idle-timeout seconds;
    interface-id interface-identifier;
    keepalive seconds;
    primary-dns primary-dns;
    primary-wins primary-wins;
    secondary-dns secondary-dns;
    secondary-wins secondary-wins;
}
}
ldap-options {
    assemble {
        common-name name;
    }
    base-distinguished-name name;
    revert-interval seconds;
    search {
        admin-search {
            distinguished-name name;
            password password;
        }
        search-filter filter-name;
    }
}

```

```

    }
  }
  ldap-server server-address {
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
    source-address address;
    timeout seconds;
  }
  profile profile-name {
    ... profile-configuration ...
  }
  radius-disconnect {
    client-address {
      secret password;
    }
  }
  radius-disconnect-port port-number;
  radius-options {
    revert-interval seconds;
  }
  radius-server server-address {
    accounting-port number;
    port number;
    retry number;
    routing-instance routing-instance-name;
    secret password;
    source-address address;
    timeout seconds;
  }
  securid-server {
    server-name configuration-file filename;
  }
  profile profile-name {
    accounting {
      accounting-stop-on-access-deny;
      accounting-stop-on-failure;
      order [ accounting-method ];
      statistics (time | volume-time);
      update-interval minutes;
    }
    accounting-order radius;
    authentication-order (ldap | password | radius | securid);
    client client-name {
      chap-secret chap-secret;
      client-group [ group-names ];
      firewall-user {
        password password;
      }
    }
    group-profile profile-name;
    ike {
      allowed-proxy-pair {
        local local-proxy-address remote remote-proxy-address;
      }
      ike-policy policy-name;
      initiate-dead-peer-detection;
    }
  }

```

```

    interface-id interface-id;
    pre-shared-key (ascii-text key-string | hexadecimal key-string);
  }
  l2tp {
    interface-id interface-identifier;
    lcp-renegotiation;
    local-chap;
    maximum-sessions-per-tunnel number;
    multilink {
      drop-timeout time;
      fragmentation-threshold bytes;
    }
    ppp-authentication (chap | pap);
    ppp-profile profile-name;
    shared-secret shared-secret;
  }
  pap-password pap-password;
  ppp {
    cell-overhead;
    encapsulation-overhead bytes;
    framed-ip-address ip-address;
    framed-pool framed-pool;
    idle-timeout seconds;
    interface-id interface-identifier;
    keepalive seconds;
    primary-dns primary-dns;
    primary-wins primary-wins;
    secondary-dns secondary-dns;
    secondary-wins secondary-wins;
  }
  user-group-profile profile-name;
}
client-name-filter client-name {
  count number;
  domain-name domain-name;
  separator special-character;
}
ldap-options {
  assemble {
    common-name name;
  }
  base-distinguished-name name;
  revert-interval seconds;
  search {
    admin-search {
      distinguished-name name;
      password password;
    }
    search-filter filter-name;
  }
}
ldap-server server-address {
  port port-number;
  retry attempts;
  routing-instance routing-instance-name;
}

```

```

source-address address;
timeout seconds;
}
radius {
  accounting-server [ ip-address ];
  attributes {
    ... attributes-configuration ...
  }
  authentication-server [ ip-address ];
  options {
    accounting-session-id-format (decimal | description);
    ethernet-port-type-virtual;
    interface-description-format (adapter | sub-interface);
    nas-identifier identifier-value;
    nas-port-extended-format {
      adapter-width width;
      port-width width;
      slot-width width;
      stacked-vlan-width width;
      vlan-width width;
    }
    revert-interval interval;
    vlan-nas-port-stacked-format;
  }
  attributes {
    exclude {
      accounting-authentic [ accounting-on | accounting-off ];
      accounting-delay-time [ accounting-on | accounting-off ];
      accounting-session-id [ access-request | accounting-on | accounting-off |
        accounting-stop ];
      accounting-terminate-cause [ accounting-off ];
      called-station-id [ access-request | accounting-start | accounting-stop ];
      calling-station-id [ access-request | accounting-start | accounting-stop ];
      class [ accounting-start | accounting-stop ];
      dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
      dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
      dhcp-options [ access-request | accounting-start | accounting-stop ];
      event-timestamp [ accounting-on | accounting-off | accounting-start |
        accounting-stop ];
      framed-ip-address [ accounting-start | accounting-stop ];
      framed-ip-netmask [ accounting-start | accounting-stop ];
      input-filter [ accounting-start | accounting-stop ];
      input-gigapackets [ accounting-stop ];
      input-gigawords [ accounting-stop ];
      interface-description [ access-request | accounting-start | accounting-stop ];
      nas-identifier [ access-request | accounting-on | accounting-off |
        accounting-start | accounting-stop ];
      nas-port [ access-request | accounting-start | accounting-stop ];
      nas-port-id [ access-request | accounting-start | accounting-stop ];
      nas-port-type [ access-request | accounting-start | accounting-stop ];
      output-filter [ accounting-start | accounting-stop ];
      output-gigapackets [ accounting-stop ];
      output-gigawords [ accounting-stop ];
    }
  }
  ignore {
    framed-ip-netmask;
  }
}

```

```

        input-filter;
        logical-system-routing-instance;
        output-filter;
    }
}
radius-options {
    revert-interval seconds;
}
radius-server server-address {
    accounting-port number;
    port number;
    retry number;
    routing-instance routing-instance-name;
    secret password;
    source-address address;
    timeout seconds;
}
session-options {
    client-group [ group-names ];
    client-idle-timeout minutes;
    client-session-timeout minutes;
}
}

```

[edit accounting-options] Hierarchy Level

```

accounting-options {
  class-usage-profile profile-name {
    destination-classes {
      destination-class-name;
    }
    file filename;
    interval minutes;
    source-classes {
      source-class-name;
    }
  }
  file filename {
    archive-sites {
      site-name;
    }
    files file-number;
    nonpersistent;
    size bytes;
    start-time time;
    transfer-interval minutes;
  }
  filter-profile profile-name {
    counters {
      counter-name;
    }
    file filename;
    interval minutes;
  }
  interface-profile profile-name {
    fields {
      field-name;
    }
    file filename;
    interval minutes;
  }
  mib-profile profile-name {
    file filename;
    interval minutes;
    object-names {
      mib-object-name;
    }
    operation operation-name;
  }
  routing-engine-profile profile-name {
    fields {
      field-name;
    }
    file filename;
    interval minutes;
  }
}

```

[edit applications] Hierarchy Level

```

applications {
  application application-name {
    application-protocol protocol-name;
    destination-port port-number;
    icmp-code value;
    icmp-type value;
    inactivity-timeout value;
    learn-sip-register;
    protocol type;
    rpc-program-number number;
    sip-call-hold-timeout minutes;
    snmp-command command;
    source-port port-number;
    term term-name {
      alg application;
      destination-port port-number;
      icmp-code value;
      icmp-type value;
      inactivity-timeout value;
      protocol type;
      rpc-program-number number;
      source-port port-number;
      uuid hexadecimal-value;
    }
    ttl-threshold value;
    uuid hexadecimal-value;
  }
  application-set application-set-name {
    application application-name;
  }
}

```


[edit bridge-domains] Hierarchy Level

```

bridge-domains {
  bridge-domain-name {
    bridge-options {
      ... bridge-options-configuration ...
    }
    description text-description;
    domain-type bridge;
    forwarding-options {
      dhcp-relay {
        ... same statements as listed in the dhcp-relay subhierarchy in [edit
          forwarding-options] Hierarchy Level ...
      }
      filter {
        input filter-name;
      }
      flood {
        input filter-name;
      }
    }
  }
  interface interface-name;
  multicast-snooping-options {
    ... same statements as listed in [edit multicast-snooping-options] Hierarchy Level
    ...
  }
  no-local-switching;
  protocols {
    ... protocols-configuration ...
  }
  routing-interface irb-interface-name;
  vlan-id (all | none | number);
  vlan-tags outer <tpid.>vlan-id <inner <tpid.>vlan-id>;
  bridge-options {
    interface interface-name {
      interface-mac-limit {
        limit;
        packet-action drop;
      }
      no-mac-learning;
      static-mac mac-address {
        vlan-id number;
      }
    }
    interface-mac-limit {
      limit;
      packet-action drop;
    }
    mac-statistics;
    mac-table-size {
      number-of-addresses;
      packet-action drop;
    }
    no-mac-learning;
  }
}

```

```

protocols {
  igmp-snooping {
    immediate-leave;
    interface interface-name {
      group-limit number;
      host-only-interface;
      immediate-leave;
      multicast-router-interface;
      static {
        group multicast-ip-address {
          source multicast-ip-address;
        }
      }
    }
  }
  proxy {
    source-address ip-address;
  }
  query-interval seconds;
  query-last-member-interval seconds;
  query-response-interval seconds;
  robust-count number;
  traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
      no-world-readable>;
    flag flag <flag-modifier> <disable>;
  }
  vlan vlan-id {
    ... same statements as at the [edit bridge-domains bridge-domain-name
      protocols igmp-snooping] hierarchy level EXCEPT the following ...
    traceoptions {...} # NOT valid at this hierarchy level
    vlan vlan-id {...} # NOT valid at this hierarchy level
  }
}
}
}
}

```

[edit chassis] Hierarchy Level

```

chassis {
  aggregated-devices {
    ethernet {
      device-count number;
    }
    sonet {
      device-count number;
    }
  }
  alarm {
    ds1 {
      ais (ignore | red | yellow);
      ylw (ignore | red | yellow);
    }
    ethernet {
      link-down (ignore | red | yellow);
    }
    integrated-services {
      failure (ignore | red | yellow);
    }
    management-ethernet {
      link-down (ignore | red | yellow);
    }
    serial {
      cts-absent (ignore | red | yellow);
      dcd-absent (ignore | red | yellow);
      dsr-absent (ignore | red | yellow);
      loss-of-rx-clock (ignore | red | yellow);
      loss-of-tx-clock (ignore | red | yellow);
      tm-absent (ignore | red | yellow);
    }
    services {
      hw-down (ignore | red | yellow);
      linkdown (ignore | red | yellow);
      pic-hold-reset (ignore | red | yellow);
      pic-reset (ignore | red | yellow);
      rx-errors (ignore | red | yellow);
      sw-down (ignore | red | yellow);
      tx-errors (ignore | red | yellow);
    }
    sonet {
      (ais-l | ais-p | ber-sd | ber-sf | locd | lol | lop-p | los | pll | plm-p | rfi-l | rfl-p | uneq-p)
      (ignore | red | yellow);
    }
    t3 {
      (ais | exz | ferf | idle | lcv | lof | los | pll | ylw) (ignore | red | yellow);
    }
  }
  cluster {
    control-ports {
      fpc slot-number port port-number;
    }
    heartbeat-interval milliseconds;
  }
}

```

```

    heartbeat-threshold number;
    initial-hold seconds;
    node node-number;
    redundancy-group group-number {
        gratuitous-arp-count number;
        interface-monitor interface-name {
            weight number;
        }
        node node-number {
            priority priority-number;
        }
        preempt;
    }
    reth-count number;
    traceoptions {
        file <filename > <files number> <match regular-expression>
            <size maximum-file-size> <world-readable | no-world-readable>;
        flag flag;
        level severity;
        no-remote-trace;
    }
}
config-button {
    no-clear;
    no-rescue;
}
container-devices {
    device-count number;
}
craft-lockout;
disable-power-management;
feb-fpc-connectivity {
    fpc number feb (slot-number | none);
}
fpc slot-number {
    ... fpc-configuration ...
}
lcc number {
    fpc slot-number {
        pic slot-number {
            atm-cell-relay-accumulation;
            atm-l2-circuit-mode (cell | aal5 | trunk trunk);
            framing (sdh | sonet);
            idle-cell-format {
                itu-t;
                payload-pattern payload-pattern-byte;
            }
            max-queues-per-interface (8 | 4);
            no-concatenate;
        }
    }
    offline;
    online-expected;
}
(packet-scheduling | no-packet-scheduling);
pem {

```

```

    minimum number;
}
redundancy {
    failover {
        on-disk-failure;
        on-loss-of-keepalives;
    }
    feb {
        redundancy-group group-name {
            description description;
            feb slot-number <backup | primary>;
            no-auto-failover;
        }
    }
    graceful-switchover;
    keepalive-time seconds;
    routing-engine slot-number (backup | disabled | master);
    sfm slot-number (always | preferred);
    ssb slot-number (always | preferred);
}
routing-engine {
    on-disk-failure disk-failure-action (halt | reboot);
}
sfm slot-number {
    power off;
}
sib {
    minimum number;
}
(source-route | no-source-route);
synchronization {
    primary (external-a | external-b);
    secondary (external-a | external-b);
    signal-type (e1 | t1);
    switching-mode (non-revertive | revertive);
    transmitter-enable;
    validation-interval seconds;
    y-cable-line-termination;
}
system-domains {
    protected-system-domains psdnumerical-index {
        control-plane-bandwidth-percent percent;
        control-slot-numbers [ slot-numbers ];
        control-system-id control-system-id;
        description description;
        fpcs [ slot-numbers ];
    }
    root-domain-id root-domain-id;
}
vrf-mtu-check;
vtmapping (klm | itu-t);
fpc slot-number {
    offline;
    pic slot-number {
        ... pic-configuration ...
    }
}

```

```

port-mirror-instance port-mirror-instance-name;
power (off | on);
pic slot-number {
  adaptive-services {
    service-package {
      extension-provider {
        control-cores number;
        data-cores number;
        forwarding-db-size megabytes;
        object-cache-size megabytes;
        package package-name;
        policy-db-size megabytes;
        syslog {
          facility severity;
        }
        wired-process-mem-size megabytes;
      }
      layer-2;
      layer-3;
    }
  }
  aggregate-ports;
  atm-cell-relay-accumulation;
  atm-l2circuit-mode (cell | aal5 | trunk trunk);
  ce1 {
    e1 port-number {
      channel-group group-number timeslots slot-number;
    }
  }
  ct3 {
    port port-number {
      t1 link-number {
        channel-group group-number timeslots slot-number;
      }
    }
  }
  ethernet {
    pic-mode (enhanced-switching | routing | switching);
  }
  framing (e1 | sdh | sonet | t1);
  idle-cell-format {
    itu-t;
    payload-pattern payload-pattern-byte;
  }
  max-queues-per-interface (8 | 4);
  mlfr-uni-nni-bundles number;
  no-concatenate;
  port-mirror-instance port-mirror-instance-name;
  q-pic-large-buffer <large-scale | small-scale>;
  red-buffer-occupancy {
    weighted-averaged {
      instant-usage-weight-exponent weight-value;
    }
  }
  shdsl {
    pic-mode (1-port-atm | 2-port-atm);
  }
}

```

```

    }
    sparse-dlcis;
    traffic-manager {
        egress-shaping-overhead number;
        ingress-shaping-overhead number;
        mode (egress-only | ingress-and-egress | session-shaping);
    }
    tunnel-queuing;
    tunnel-services {
        bandwidth (1g | 10g);
    }
    vtmapping (itu-t | klm);
}
}
}

```

[edit class-of-service] Hierarchy Level

```

class-of-service {
  adaptive-shapers {
    adaptive-shaper-name {
      trigger type shaping-rate (bps | percent percentage);
    }
  }
  classifiers {
    type classifier-name {
      forwarding-class class-name {
        loss-priority (high | low | medium-high | medium-low) code-points [ aliases bits ];
      }
      import (classifier-name | default);
    }
  }
  code-point-aliases {
    (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence) {
      alias-name bits;
    }
  }
  drop-profiles {
    profile-name {
      fill-level percentage drop-probability percentage;
      interpolate {
        drop-probability value;
        fill-level value;
      }
    }
  }
  fabric {
    scheduler-map {
      priority (high | low) scheduler scheduler-name;
    }
  }
  forwarding-classes {
    class class-name queue-num queue-number priority (high | low);
    queue queue-number class-name priority (high | low);
  }
  forwarding-policy {
    class class-name {
      classification-override {
        forwarding-class class-name;
      }
    }
    next-hop-map map-name {
      forwarding-class class-name {
        lsp-next-hop [ lsp-regular-expressions ];
        next-hop [ next-hop-names ];
        non-lsp-next-hop;
      }
    }
  }
  fragmentation-maps {
    map-name {

```



```

        forwarding-class class-name {
            drop-timeout milliseconds;
            fragment-threshold bytes;
            multilink-class number;
            no-fragmentation;
        }
    }
}
host-outbound-traffic {
    dscp-code-point value;
    forwarding-class class-name;
    translation-table to-802.1p-from-dscp table-name;
}
interfaces {
    ...interface-configuration ...
}
loss-priority-maps {
    frame-relay-de (map-name | default) {
        loss-priority level code-points [ 0 1 ];
    }
}
restricted-queues {
    forwarding-class class-name queue queue-number;
}
rewrite-rules {
    (dscp | dscp-ipv6 | exp | frame-relay-de | ieee-802.1 | inet-precedence) rewrite-rule
    {
        forwarding-class class-name {
            loss-priority level code-point (alias | bits);
        }
        import (rewrite-rule | default);
    }
}
routing-instances routing-instance-name {
    classifier {
        exp (classifier-name | default);
    }
}
scheduler-maps {
    map-name {
        forwarding-class class-name scheduler scheduler-name;
    }
}
schedulers {
    scheduler-name {
        buffer-size (percent percentage | remainder | temporal microseconds);
        drop-profile-map loss-priority (any | high | low | medium-high | medium-low)
            protocol (any | non-tcp | tcp);
        drop-profile profile-name;
        priority (high | low | medium-high | medium-low | strict-high);
        shaping-rate (bps | percent percentage);
        transmit-rate (bps | percent percentage | remainder) <exact | rate-limit>;
    }
}
traceoptions {

```

```

    file <filename> <files number> <match regular-expression>
      <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
  }
  traffic-control-profiles profile-name {
    delay-buffer-rate (bps | percent percentage);
    guaranteed-rate (bps | percent percentage);
    scheduler-map map-name;
    shaping-rate (bps | percent percentage);
  }
  translation-table {
    to-802.1p-from-dscp table-name {
      to-code-point 3-bit-pattern from-code-points [ 6-bit-patterns ];
    }
    to-dscp-from-dscp table-name {
      to-code-point 6-bit-pattern from-code-points [ 6-bit-patterns ];
    }
    to-dscp-ipv6-from-dscp-ipv6 table-name {
      to-code-point 6-bit-pattern from-code-points [ 6-bit-patterns ];
    }
    to-exp-from-exp table-name {
      to-code-point 3-bit-pattern from-code-points [ 3-bit-patterns ];
    }
    to-inet-precedence-from-inet-precedence table-name {
      to-code-point 3-bit-pattern from-code-points [ 3-bit-patterns ];
    }
  }
  tri-color;
  virtual-channels {
    virtual-channel-name;
  }
  virtual-channel-groups {
    virtual-channel-group-name {
      virtual-channel-name {
        default;
        scheduler-map map-name;
        shaping-rate (bps | percent percentage);
      }
    }
  }
  interfaces {
    interface-name {
      input-scheduler-map map-name;
      input-shaping-rate bps;
      scheduler-map map-name;
      scheduler-map-chassis map-name;
      shaping-rate bps;
      unit logical-unit-number {
        adaptive-shaper adaptive-shaper-name;
        classifiers {
          (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence) (classifier-name |
            default);
        }
        forwarding-class class-name;
        fragmentation-map map-name;
      }
    }
  }

```

```

input-scheduler-map map-name;
input-shaping-rate bps;
input-traffic-control-profile profile-name shared-instance instance-name;
loss-priority-maps {
    (map-name | default);
}
output-traffic-control-profile profile-name <shared-instance instance-name>;
per-session-scheduler;
rewrite-rules {
    dscp (rewrite-name | default) protocols protocol-type;
    dscp-ipv6 (rewrite-name | default);
    exp (rewrite-name | default) protocol protocol-type;
    exp-push-push-push default;
    exp-swap-push-push default;
    frame-relay-de (rewrite-name | default);
    ieee-802.1 (rewrite-name | default) vlan-tag (outer | outer-and-inner);
    ieee-802.1ad (rewrite-name | default) vlan-tag (outer | outer-and-inner);
    inet-precedence (rewrite-name | default) protocols protocol-types;
}
scheduler-map map-name;
shaping-rate bps;
virtual-channel-group group-name;
}
}
}
}

```

[edit dynamic-profiles] Hierarchy Level

```
dynamic-profiles {  
  class-of-service {  
    ... same statements as listed in [edit class-of-service] Hierarchy Level ...  
  }  
  interfaces {  
    ... same statements as listed in [edit interfaces] Hierarchy Level ...  
  }  
  protocols {  
    ... same statements as listed in [edit protocols] Hierarchy Level ...  
  }  
  variables {  
    variable-name {  
      default-value text-string;  
      mandatory;  
      radius {  
        vendor-id id;  
      }  
    }  
  }  
}
```

[edit ethernet-switching-options] Hierarchy Level

```

ethernet-switching-options {
  analyzer {
    ... analyzer-configuration ...
  }
  bpdu-block {
    disable-timeout seconds;
    interface interface-name;
  }
  dot1q-tunneling {
    ether-type (0x8100 | 0x88a8 | 0x9100);
  }
  mac-table-aging-time seconds;
  redundant-trunk-group {
    group rtg-group-name {
      interface interface-name;
    }
  }
  secure-access-port {
    interface interface-name {
      allowed-mac [ mac-addresses ];
      (dhcp-trusted | no-dhcp-trusted);
      mac-limit number action (drop | log | none | shutdown);
      static-ip ip-address vlan vlan-id mac mac-address;
    }
  }
  vlan vlan-id {
    (arp-inspection | no-arp-inspection);
    dhcp-option82 {
      disable;
      circuit-id {
        prefix hostname;
        use-interface-description;
        use-vlan-id;
      }
      remote-id {
        prefix (hostname | mac | none);
        (use-interface-description | use-string text-string);
      }
      vendor-id {
        text-string;
      }
    }
    (examine-dhcp | no-examine-dhcp);
    (ip-source-guard | no-ip-source-guard);
    mac-move-limit number action (drop | log | none | shutdown);
    static-ip ip-address vlan vlan-id mac mac-address;
  }
}
analyzer analyzer-name {
  input {
    egress {
      interface interface-name;
    }
    ingress {

```

```
        interface interface-name;  
        vlan vlan-id;  
    }  
}  
loss-priority (high | low);  
output {  
    interface {  
        interface-name;  
    }  
    vlan {  
        vlan-id;  
    }  
}  
ratio number;  
}
```

[edit event-options] Hierarchy Level

```

event-options {
  destinations {
    destination-name {
      archive-sites {
        url password password;
      }
      transfer-delay seconds;
    }
  }
  event-script {
    file filename;
    traceoptions {
      file <filename> <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag;
      no-remote-trace;
    }
  }
  generate-event event-name {
    time-interval seconds;
    time-of-day hh:mm:ss;
  }
  policy policy-name {
    attributes-match {
      event1.attribute-name equals event2.attribute-name;
      event.attribute-name matches regular-expression;
      event1.attribute-name starts-with event2.attribute-name;
    }
  }
  events [ events ];
  then {
    event-script script-name.xml {
      arguments {
        name value;
      }
      destination destination-name {
        retry-count number retry-interval seconds;
        transfer-delay seconds;
      }
      output-filename filename;
      output-format (text | xml);
      user-name username;
    }
    execute-commands {
      commands {
        "command";
      }
      destination destination-name {
        retry-count number retry-interval seconds;
        transfer-delay seconds;
      }
      output-filename filename;
      output-format (text | xml);
      user-name username;
    }
  }
}

```

```

    }
    ignore;
    raise-trap;
    upload filename committed destination destination-name;
    upload filename filename destination destination-name {
        retry-count number retry-interval seconds;
        transfer-delay seconds;
        user-name username;
    }
}
within seconds {
    events [ events ];
    not events [ events ];
    trigger (after number | on number | until number);
}
}
traceoptions {
    file <filename> <files number> <match regular-expression>
        <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
}

```


[edit firewall] Hierarchy Level

Several statements in the [edit firewall] hierarchy are valid at numerous locations within the hierarchy. To make the complete hierarchy easier to read, the repeated statements are listed in the following sections, which are referenced at the appropriate locations in “Complete [edit firewall] Hierarchy” on page 80.

- Common Firewall Actions on page 77
- Common IP Firewall Actions on page 77
- Common IPv4 Firewall Actions on page 78
- Common IP Firewall Match Conditions on page 78
- Common IPv4 Firewall Match Conditions on page 79
- Common Layer 2 Firewall Match Conditions on page 79
- Complete [edit firewall] Hierarchy on page 80

Common Firewall Actions

This section lists statements that are valid at each of the following hierarchy levels, and is referenced at those levels in “Complete [edit firewall] Hierarchy” on page 80 instead of the statements being repeated.

- [edit firewall family (any | bridge | ccc | inet | inet6 | mpls | vpls) filter *filter-name* term *term-name* then]
- [edit firewall filter *filter-name* term *term-name* then]

The common firewall actions are as follows:

```
count counter-name;
forwarding-class class-name;
loss-priority (high | low | medium-high | medium-low);
next term;
policer policer-name;
three-color-policer policer-name {
    (single-rate single-rate-policer-name | two-rate two-rate-policer-name);
}
```

Common IP Firewall Actions

This section lists statements that are valid at each of the following hierarchy levels, and is referenced at those levels in “Complete [edit firewall] Hierarchy” on page 80 instead of the statements being repeated.

- [edit firewall family inet filter *filter-name* term *term-name* then]
- [edit firewall family inet6 filter *filter-name* term *term-name* then]
- [edit firewall filter *filter-name* term *term-name* then]

The common IP firewall actions are as follows:

```
log;
```

```

logical-system logical-system-name <routing-instance routing-instance-name>
    <topology topology-name>;
port-mirror;
routing-instance routing-instance-name <topology topology-name>;
sample;
syslog;
topology topology-name;

```

Common IPv4 Firewall Actions

This section lists statements that are valid at each of the following hierarchy levels, and is referenced at those levels in “Complete [edit firewall] Hierarchy” on page 80 instead of the statements being repeated.

- [edit firewall family inet filter *filter-name* term *term-name* then]
- [edit firewall filter *filter-name* term *term-name* then]

The common IPv4 firewall actions are as follows:

```

(accept | discard <accounting collector-name> | reject <(administratively-prohibited |
    bad-host-tos | bad-network-tos | fragmentation-needed | host-prohibited |
    host-unknown | host-unreachable | network-prohibited | network-unknown |
    network-unreachable | port-unreachable | precedence-cutoff | precedence-violation |
    protocol-unreachable | source-host-isolated | source-route-failed | tcp-reset)>;
ipsec-sa sa-name;
load-balance sa-name;
next-hop-group group-name;
prefix-action action-name;

```

Common IP Firewall Match Conditions

This section lists statements that are valid at each of the following hierarchy levels, and is referenced at those levels in “Complete [edit firewall] Hierarchy” on page 80 instead of the statements being repeated.

- [edit firewall family inet dialer-filter *filter-name* term *term-name* from] (with the exceptions noted at this level in “Complete [edit firewall] Hierarchy” on page 80)
- [edit firewall family inet filter *filter-name* term *term-name* from]
- [edit firewall family inet6 filter *filter-name* term *term-name* from]
- [edit firewall filter *filter-name* term *term-name* from]

The common IP firewall match conditions are as follows:

```

address ip-prefix</prefix-length>;
destination-address ip-prefix</prefix-length>;
destination-class [ class-names ] | destination-class-except [ class-names ]];
(destination-port [ port-names ] | destination-port-except [ port-names ]]);
destination-prefix-list list-name;
(forwarding-class [ class-names ] | forwarding-class-except [ class-names ]]);
icmp-code [ codes ] | icmp-code-except [ codes ]];
icmp-type [ types ] | icmp-type-except [ types ]];

```

```

interface interface-name;
(interface-group [ group-names ] | interface-group-except [ group-names ]);
interface-set set-name;
(loss-priority [ priorities ] | loss-priority-except [ priorities ]);
(packet-length [ values ] | packet-length-except [ values ]);
(port [ port-names ] | port-except [ port-names ]);
prefix-list list-name;
source-address ip-prefix</prefix-length>;
(source-class [ class-names ] | source-class-except [ class-names ]);
(source-port [ port-names ] | source-port-except [ port-names ]);
source-prefix-list list-name;
tcp-established;
tcp-flags flag;
tcp-initial;

```

Common IPv4 Firewall Match Conditions

This section lists statements that are valid at each of the following hierarchy levels, and is referenced at those levels in “Complete [edit firewall] Hierarchy” on page 80 instead of the statements being repeated.

- [edit firewall family inet dialer-filter *filter-name* term *term-name* from] (with the exceptions noted at this level in “Complete [edit firewall] Hierarchy” on page 80)
- [edit firewall family inet filter *filter-name* term *term-name* from]
- [edit firewall filter *filter-name* term *term-name* from]

The common IPv4 firewall match conditions are as follows:

```

(ah-spi [ values ] | ah-spi-except [ values ]);
(dscp [ code-point-values ] | dscp-except [ code-point-values ]);
(esp-spi [ values ] | esp-spi-except [ values ]);
first-fragment;
fragment-flags flag;
(fragment-offset [ offsets ] | fragment-offset-except [ offsets ]);
(ip-options [ option-names ] | ip-options-except [ option-names ]);
is-fragment;
(precedence [ precedence-names ] | precedence-except [ precedence-names ]);
(protocol [ protocol-names ] | protocol-except [ protocol-names ]);
(ttl [ ttl-values ] | ttl-except [ ttl-values ]);

```

Common Layer 2 Firewall Match Conditions

This section lists statements that are valid at each of the following hierarchy levels, and is referenced at those levels in “Complete [edit firewall] Hierarchy” on page 80 instead of the statements being repeated.

- [edit firewall family bridge filter *filter-name* term *term-name* from]
- [edit firewall family vpls filter *filter-name* term *term-name* from]

The common Layer 2 firewall match conditions are as follows:

```

destination-mac-address mac-address;

```

```

(destination-port [ port-names ] | destination-port-except [ port-names ]);
(dscp [ code-point-values ] | dscp-except [ code-point-values ]);
(ether-type [ protocol-types ] | ether-type-except [ protocol-types ]);
(forwarding-class [ class-names ] | forwarding-class-except [ class-names ]);
 icmp-code [ codes ] | icmp-code-except [ codes ]);
 icmp-type [ types ] | icmp-type-except [ types ]);
(interface-group [ group-names ] | interface-group-except [ group-names ]);
ip-address ip-prefix</prefix-length>;
ip-destination-address ip-prefix</prefix-length>;
(ip-precedence [ precedence-names ] | ip-precedence-except [ precedence-names ]);
(ip-protocol [ protocol-names ] | ip-protocol-except [ protocol-names ]);
ip-source-address ip-prefix</prefix-length>;
(learn-vlan-1p-priority [ priorities ] | learn-vlan-id-except [ priorities ]);
(learn-vlan-id [ vlan-ids ] | learn-vlan-id-except [ vlan-ids ]);
(loss-priority [ priorities ] | loss-priority-except [ priorities ]);
(port [ port-names ] | port-except [ port-names ]);
source-mac-address mac-address;
(source-port [ port-names ] | source-port-except [ port-names ]);
tcp-flags flag;
(traffic-type [ broadcast known-unicast multicast unknown-unicast ] | traffic-type-except [
    broadcast known-unicast multicast unknown-unicast ]);
(user-vlan-1p-priority [ priorities ] | user-vlan-id-except [ priorities ]);
(user-vlan-id [ vlan-ids ] | user-vlan-id-except [ vlan-ids ]);
(vlan-ether-type [ protocol-types ] | vlan-ether-type-except [ protocol-types ]);

```

Complete [edit firewall] Hierarchy

```

firewall {
    family (any | bridge | ccc | inet | inet6 | mpls | vpls) {
        ... family-configuration...
    }
    filter filter-name {
        accounting-profile [ profile-names ];
        interface-specific;
        term term-name {
            filter filter-name;
            from {
                ... statements listed in Common IP Firewall Match Conditions AND ...
                ... statements listed in Common IPv4 Firewall Match Conditions ...
            }
            then {
                ... statements listed in Common Firewall Actions AND ...
                ... statements listed in Common IP Firewall Actions AND ...
                ... statements listed in Common IPv4 Firewall Actions PLUS the following
                    statement...
                service-filter-hit;
            }
        }
    }
}
hierarchical-policer policer-name {
    aggregate {
        if-exceeding {
            bandwidth-limit bps;
            burst-size-limit bytes;
        }
    }
}

```

```

    then {
        discard;
        forwarding-class class-name;
        loss-priority (high | low);
    }
}
premium {
    if-exceeding {
        bandwidth-limit bps;
        burst-size-limit bytes;
    }
    then {
        discard;
        forwarding-class class-name;
        loss-priority (high | low);
    }
}
}
interface-set interface-set-name {
    interface-name;
}
load-balance-group group-name {
    next-hop-group [ group-names ];
}
policer policer-name {
    filter-specific;
    if-exceeding {
        bandwidth-limit bps;
        bandwidth-percent number;
        burst-size-limit bytes;
    }
    logical-bandwidth-policer;
    logical-interface-policer;
    then {
        discard;
        forwarding-class class-name;
        loss-priority (high | low);
    }
}
three-color-policer policer-name {
    action {
        loss-priority high then discard;
    }
    logical-interface-policer;
    single-rate {
        (color-aware | color-blind);
        committed-burst-size bytes;
        committed-information-rate bps;
        excess-burst-size bytes;
    }
    two-rate {
        (color-aware | color-blind);
        committed-burst-size bytes;
        committed-information-rate bps;
        peak-burst-size bytes;
        peak-information-rate bps;
    }
}

```

```

    }
  }
  family any {
    filter filter-name {
      term term-name {
        from {
          (forwarding-class [ class-names ] | forwarding-class-except [ class-names ]);
          interface interface-name;
          interface-set set-name;
          (loss-priority [ priorities ] | loss-priority-except [ priorities ]);
          (packet-length [ values ] | packet-length-except [ values ]);
        }
        then {
          ... statements listed in Common Firewall Actions PLUS the following statement ...
          (accept | discard);
        }
      }
    }
  }
}
family bridge {
  filter filter-name {
    accounting-profile [ profile-names ];
    interface-specific;
    term term-name {
      filter filter-name;
      from {
        ... statements listed in Common Layer 2 Firewall Match Conditions ...
      }
      then {
        ... statements listed in Common Firewall Actions PLUS the following statements ...
        (accept | discard);
        port-mirror;
      }
    }
  }
}
family ccc {
  filter filter-name {
    accounting-profile [ profile-names ];
    interface-specific;
    term term-name {
      filter filter-name;
      from {
        (forwarding-class [ class-names ] | forwarding-class-except [ class-names ]);
        (interface-group [ group-names ] | interface-group-except [ group-names ]);
        (loss-priority [ priorities ] | loss-priority-except [ priorities ]);
      }
      then {
        ... statements listed in Common Firewall Actions PLUS the following statement ...
        (accept | discard);
      }
    }
  }
}

```

```

}
family inet {
    ... family-inet-configuration ...
}
family inet6 {
    filter filter-name {
        accounting-profile [ profile-names ];
        interface-specific;
        term term-name {
            filter filter-name;
            from {
                ... statements listed in Common IP Firewall Match Conditions PLUS the
                    following statements ...
                (next-header [ protocol-types ] | next-header-except [ protocol-types ]);
                (traffic-class [ code-point-values ] | traffic-class-except [ code-point-values ]);
            }
            then {
                ... statements listed in Common Firewall Actions AND ...
                ... statements listed in Common IP Firewall Actions PLUS the following
                    statement ...
                (accept | discard | reject <(address-unreachable |
                    administratively-prohibited | beyond-scope | fragmentation-needed |
                    no-route | port-unreachable | tcp-reset)>);
            }
        }
    }
}
service-filter filter-name {
    term term-name {
        from {
            address ip-prefix</prefix-length>;
            (ah-spi [ values ] | ah-spi-except [ values ]);
            destination-address ip-prefix</prefix-length>;
            (destination-port [ port-names ] | destination-port-except [ port-names ]);
            destination-prefix-list list-name;
            (esp-spi [ values ] | esp-spi-except [ values ]);
            (interface-group [ group-names ] | interface-group-except [ group-names ]);
            (next-header [ protocol-types ] | next-header-except [ protocol-types ]);
            (port [ port-names ] | port-except [ port-names ]);
            prefix-list list-name;
            source-address ip-prefix</prefix-length>;
            (source-port [ port-names ] | source-port-except [ port-names ]);
            source-prefix-list list-name;
        }
        then {
            count counter-name;
            log;
            port-mirror;
            sample;
            (service | skip);
        }
    }
}
}
family mpls {
    filter filter-name {
        accounting-profile [ profile-names ];

```

```

interface-specific;
term term-name {
    filter filter-name;
    from {
        (exp [ exp-bits ] | exp-except [ exp-bits ]);
        (forwarding-class [ class-names ] | forwarding-class-except [ class-names ]);
        interface interface-name;
        interface-set set-name;
        (loss-priority [ priorities ] | loss-priority-except [ priorities ]);
    }
    then {
        ... statements listed in Common Firewall Actions PLUS the following
           statements ...
        (accept | discard);
        sample;
    }
}
}
}
family vpls {
    filter filter-name {
        accounting-profile [ profile-names ];
        interface-specific;
        term term-name {
            filter filter-name;
            from {
                ... statements listed in Common Layer 2 Firewall Match Conditions ...
            }
            then {
                ... statements listed in Common Firewall Actions PLUS the following
                   statements ...
                (accept | discard);
                port-mirror;
            }
        }
    }
}
family inet {
    dialer-filter filter-name {
        accounting-profile [ profile-names ];
        term term-name {
            from {
                ... statements listed in Common IP Firewall Match Conditions AND ...
                ... statements listed in Common IPv4 Firewall Match Conditions EXCEPT
                   FOR the following statements ...
                (ah-spi [ values ] | ah-spi-except [ values ]); # NOT valid at this hierarchy
                                                           level
                (destination-class [ class-names ] |
                 destination-class-except [ class-names ]); # NOT valid at this hierarchy
                                                           level
                interface interface-name; # NOT valid at this hierarchy level
                (loss-priority [ priorities ] | loss-priority-except [ priorities ]); # NOT valid
                                                           at this hierarchy level
                (source-class [ class-names ] | source-class-except [ class-names ]); # NOT
                                                           valid at this hierarchy level
            }
        }
    }
}

```



```

    then {
        (ignore | note);
        log;
        sample;
        syslog;
    }
}
}
filter filter-name {
    accounting-profile [ profile-names ];
    interface-specific;
    term term-name {
        filter filter-name;
        from {
            ... statements listed in Common IP Firewall Match Conditions AND ...
            ... statements listed in Common IPv4 Firewall Match Conditions ...
        }
        then {
            ... statements listed in Common Firewall Actions AND ...
            ... statements listed in Common IP Firewall Actions AND ...
            ... statements listed in Common IPv4 Firewall Actions ...
        }
    }
}
}
prefix-action name {
    count;
    destination-prefix-length prefix-length;
    filter-specific;
    policer policer-name;
    source-prefix-length prefix-length;
    subnet-prefix-length prefix-length;
}
service-filter filter-name {
    term term-name {
        from {
            address ip-prefix</prefix-length>;
            (ah-spi [ values ] | ah-spi-except [ values ]);
            destination-address ip-prefix</prefix-length>;
            (destination-port [ port-names ] | destination-port-except [ port-names ]);
            destination-prefix-list list-name;
            (esp-spi [ values ] | esp-spi-except [ values ]);
            first-fragment;
            fragment-flags flag;
            (fragment-offset [ offsets ] | fragment-offset-except [ offsets ]);
            (interface-group [ group-names ] | interface-group-except [ group-names ]);
            (ip-options [ option-names ] | ip-options-except [ option-names ]);
            is-fragment;
            (loss-priority [ priorities ] | loss-priority-except [ priorities ]);
            (port [ port-names ] | port-except [ port-names ]);
            prefix-list list-name;
            (protocol [ protocol-names ] | protocol-except [ protocol-names ]);
            source-address ip-prefix</prefix-length>;
            (source-port [ port-names ] | source-port-except [ port-names ]);
            source-prefix-list list-name;
        }
        then {

```

```

        count counter-name;
        log;
        port-mirror;
        sample;
        (service | skip);
    }
}
}
simple-filter filter-name {
    interface-specific;
    term term-name {
        from {
            destination-address ip-prefix</prefix-length>;
            destination-port port-name;
            forwarding-class [ class-names ];
            protocol protocol-name;
            source-address ip-prefix</prefix-length>;
            source-port port-name;
        }
        then {
            forwarding-class class-name;
            loss-priority (high | low | medium-high | medium-low);
            policer policer-name;
        }
    }
}
}
}
}

```

[edit forwarding-options] Hierarchy Level

```

forwarding-options {
  accounting group-name {
    output {
      aggregate-export-interval seconds;
      cflowd hostname {
        aggregation {
          autonomous-system;
          destination-prefix;
          protocol-port;
          source-destination-prefix {
            caida-compliant;
          }
          source-prefix;
        }
        autonomous-system-type (origin | peer);
        port port-number;
        version format;
      }
      flow-active-timeout seconds;
      flow-inactive-timeout seconds;
      interface interface-name {
        engine-id number;
        engine-type number;
        source-address address;
      }
    }
  }
}

dhcp-relay {
  active-server-group server-group-name;
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name;
      logical-system-name;
      mac-address;
      option-60;
      option-82 <circuit-id> <remote-id>;
      routing-instance-name;
      user-prefix prefix-string;
    }
  }
}

dynamic-profile profile-name (aggregate-clients | use-primary primary-profile-name);
group group-name {
  ... group-configuration ...
}

overrides {
  always-write-giaddr;
  always-write-option-82;
  client-discover-match;
  disable-relay;
  interface-client-limit number;
}

```

```

    layer2-unicast-replies;
    no-arp;
    trust-option-82;
}
relay-option-60 {
    vendor-option {
        (default-local-server-group group-name | default-relay-server-group group-name |
        drop);
        (equals | starts-with) (ascii text-string | hexadecimal hexadecimal-value) {
            (drop | local-server-group group-name | relay-server-group group-name);
        }
    }
}
relay-option-82 {
    circuit-id {
        prefix {
            host-name;
            logical-system-name;
            routing-instance-name;
        }
    }
}
server-group {
    server-group-name {
        server-ip-address;
    }
}
traceoptions {
    file <filename> <files number> <match regular-expression>
        <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
group group-name {
    active-server-group server-group-name;
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
}
dynamic-profile profile-name (aggregate-clients | use-primary
    primary-profile-name);
interface interface-name <upto interface-name> <exclude>;
overrides {
    always-write-giaddr;
    always-write-option-82;
    client-discover-match;
}

```

```

        disable-relay;
        interface-client-limit number;
        layer2-unicast-replies;
        no-arp;
        trust-option-82;
    }
    relay-option-60 {
        vendor-option {
            (default-local-server-group group-name |
             default-relay-server-group group-name | drop);
            (equals | starts-with) (ascii text-string | hexadecimal hexadecimal-value) {
                (drop | local-server-group group-name | relay-server-group group-name);
            }
        }
    }
    relay-option-82 {
        circuit-id {
            prefix {
                host-name;
                logical-system-name;
                routing-instance-name;
            }
        }
    }
}
family family-name {
    filter {
        input filter-name;
        output filter-name;
    }
    flood {
        input filter-name;
    }
    route-accounting;
}
hash-key {
    family {
        inet {
            layer-3;
            layer-4;
        }
        mpls {
            label-1;
            label-2;
            label-3;
            no-labels;
            payload {
                ether-pseudowire;
                ip {
                    layer-3-only;
                    port-data {
                        destination-lsb;
                        destination-msb;
                        source-lsb;
                        source-msb;
                    }
                }
            }
        }
    }
}

```

```

    }
  }
}
multiservice {
  destination-mac;
  label-1;
  label-2;
  payload {
    ip {
      layer-3-only;
    }
  }
  source-mac;
}
}
}
helpers {
  bootp {
    client-response-ttl number;
    description description-of-service;
    interface interface-name-or-wildcard {
      broadcast;
      client-response-ttl number;
      description description;
      maximum-hop-count number;
      minimum-wait-time seconds;
      no-listen;
      server address {
        logical-system logical-system-name;
        routing-instance [ routing-instance-names ];
      }
      vpn;
    }
    maximum-hop-count number;
    minimum-wait-time seconds;
    relay-agent-option;
    server address {
      logical-system logical-system-name;
      routing-instance [ routing-instance-names ];
    }
    vpn;
  }
}
domain {
  description description-of-service;
  interface interface-name {
    description description;
    no-listen;
    server <address> <logical-system logical-system-name>
      <routing-instance (default | routing-instance-name)>;
  }
  server <address> <logical-system logical-system-name>
    <routing-instance (default | routing-instance-name)>;
}
port port-number {
  description description-of-service;

```

```

interface interface-name {
    description description;
    no-listen;
    server <address> <logical-system logical-system-name>
        <routing-instance (default | routing-instance-name)>;
}
server <address> <logical-system logical-system-name>
    <routing-instance (default | routing-instance-name)>;
}
tftp {
    description description-of-service;
    interface interface-name {
        description description;
        no-listen;
        server <address> <logical-system logical-system-name>
            <routing-instance (default | routing-instance-name)>;
    }
    server <address> <logical-system logical-system-name>
        <routing-instance (default | routing-instance-name)>;
}
traceoptions {
    file filename <files number> <match regular-expression>
        <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag;
    level severity;
    no-remote-trace;
}
}
load-balance {
    indexed-next-hop;
    per-prefix {
        hash-seed number;
    }
}
}
monitoring group-name {
    family inet {
        output {
            cflowd hostname {
                port port-number;
            }
            export-format cflowd-version-5;
            flow-active-timeout seconds;
            flow-export-destination cflowd-collector;
            flow-inactive-timeout seconds;
            interface interface-name {
                engine-id number;
                engine-type number;
                input-interface-index number;
                output-interface-index number;
                source-address address;
            }
        }
    }
}
}
next-hop-group group-name {
    interface interface-name {

```

```

        next-hop address;
    }
}
packet-capture {
    disable;
    file filename filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
}
maximum-capture-size number;
}
port-mirroring {
    family {
        (ccc | vpls) {
            output {
                interface interface-name;
                no-filter-check;
            }
        }
        (inet | inet6) {
            output {
                interface interface-name {
                    next-hop address;
                }
                no-filter-check;
            }
        }
    }
}
input {
    maximum-packet-length bytes;
    rate number;
    run-length number;
}
instance {
    family {
        ... same statements as at the [edit forwarding-options port-mirroring family]
            hierarchy level ...
    }
    input {
        ... same statements as at the [edit forwarding-options port-mirroring input]
            hierarchy level ...
    }
}
traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
}
}
sampling {
    disable;
    input {
        family (inet | mpls) {
            max-packets-per-second number;
            rate number;
            run-length number;
        }
    }
}

```



```

output {
  aggregate-export-interval seconds;
  cflowd hostname {
    aggregation {
      autonomous-system;
      destination-prefix;
      protocol-port;
      source-destination-prefix {
        caida-compliant;
      }
      source-prefix;
    }
    autonomous-system-type (origin | peer);
    (local-dump | no-local-dump);
    port port-number;
    source-address address;
    version (5 | 8);
    version9 {
      template template-name;
    }
  }
  file filename filename <disable> <files number> <size maximum-file-size>
    <stamp | no-stamp> <world-readable | no-world-readable>;
  flow-active-timeout seconds;
  flow-inactive-timeout seconds;
  interface interface-name {
    engine-id number;
    engine-type number;
    source-address address;
  }
}
traceoptions {
  file filename <files number> <size maximum-file-size> <world-readable |
    no-world-readable>;
}
}

```

[edit groups] Hierarchy Level

```
groups {  
  group-name {  
    ... statements from any subhierarchy at the [edit] hierarchy level ...  
  }  
}
```

[edit interfaces] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

interfaces {
  interface-name {
    disable;
    accounting-profile name;
    aggregated-ether-options {
      (flow-control | no-flow-control);
      lacp mode {
        periodic interval;
      }
      link-protection;
      link-speed speed;
      (loopback | no-loopback);
      minimum-links number;
      source-address-filter {
        mac-address;
      }
      (source-filtering | no-source-filtering);
    }
    aggregated-sonet-options {
      link-speed (speed | mixed);
      minimum-links number;
    }
    atm-options {
      cell-bundle-size cells;
      ilmi;
      linear-red-profiles profile-name {
        high-plp-max-threshold percent;
        low-plp-max-threshold percent;
        queue-depth cells high-plp-threshold percent low-plp-threshold percent;
      }
      mpls {
        pop-all-labels {
          required-depth number;
        }
      }
      pic-type (atm1 | atm2);
      plp-to-clp;
      promiscuous-mode {
        vpi vpi-identifier;
      }
      scheduler-maps map-name {
        forwarding-class class-name {
          epd-threshold cells plp1 cells;
          linear-red-profile profile-name;
          priority (high | low);
          transmit-weight (cells number | percent number);
        }
        vc-cos-mode (alternate | strict);
      }
      vpi vpi-identifier {

```

```

        maximum-vcs maximum-vcs;
        oam-liveness {
            down-count cells;
            up-count cells;
        }
        oam-period (disable | seconds);
        shaping {
            (cbr rate | rtvbr peak rate sustained rate burst length |
             vbr peak rate sustained rate burst length);
            queue-length number;
        }
    }
}
clocking clock-source;
data-input (system | interface interface-name);
dce;
description text;
dialer-options {
    pool pool-name priority priority;
}
dsl-options {
    operating-mode mode;
}
ds0-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    byte-encoding (nx56 | nx64);
    fcs (16 | 32);
    idle-cycle-flag (flags | ones);
    invert data;
    loopback (payload | remote);
    start-end-flag (filler | shared);
}
e1-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    fcs (16 | 32);
    framing (g704 | g704-no-crc4 | unframed);
    idle-cycle-flag (flags | ones);
    invert-data;
    loopback (local | remote);
    start-end-flag (filler | shared);
    timeslots time-slot-range;
}
e3-options {
    atm-encapsulation (direct | plcp);
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    buildout feet;
    compatibility-mode (digital-link | kentrox | larscom) <subrate value>;
    fcs (16 | 32);
    framing (g.751 | g.832);
    idle-cycle-flag value;
}

```

```

invert-data;
loopback (local | remote);
(payload-scrambler | no-payload-scrambler);
start-end-flag (filler | shared);
(unframed | no-unframed);
}
encapsulation type;
ether-vpls-over-atm-llc;
es-options {
    backup-interface es-fpc/pic/port;
}
fabric-options {
    member-interfaces interface-name;
}
fastether-options {
    802.3ad aex <backup | primary>;
    (flow-control | no-flow-control);
    ignore-l3-incompletes;
    ingress-rate-limit rate;
    (loopback | no-loopback);
    mpls {
        pop-all-labels {
            required-depth number;
        }
    }
    redundant-parent interface-name;
    source-address-filter {
        mac-address;
    }
    (source-filtering | no-source-filtering);
}
flexible-vlan-tagging;
framing (lan-phy | sdh | sonet | wan-phy);
gigether-options {
    802.3ad aex;
    (asynchronous-notification | no-asynchronous-notification);
    (auto-negotiation <remote-fault (local-interface-online | local-interface-offline)>
    | no-auto-negotiation);
    auto-reconnect seconds;
    ethernet-switch-profile {
        ... ethernet-switch-profile-configuration ...
    }
    (flow-control | no-flow-control);
    ignore-l3-incompletes;
    (loopback | no-loopback);
    mpls {
        pop-all-labels {
            required-depth number;
        }
    }
    redundant-parent interface-name;
    source-address-filter {
        mac-address;
    }
    (source-filtering | no-source-filtering);
    ethernet-switch-profile {

```

```

ethernet-policer-profile {
  input-priority-map {
    ieee802.1p {
      premium [ values ];
    }
  }
  output-priority-map {
    classifier {
      premium {
        forwarding-class class-name {
          loss-priority (high | low);
        }
      }
    }
  }
  policer cos-policer-name {
    aggregate {
      bandwidth-limit bps;
      burst-size-limit bytes;
    }
    premium {
      bandwidth-limit bps;
      burst-size-limit bytes;
    }
  }
}
(mac-learn-enable | no-mac-learn-enable);
tag-protocol-id [ tpids ];
}
}
(gratuitous-arp-reply | no-gratuitous-arp-reply);
hold-time up milliseconds down milliseconds;
isdn-options {
  bchannel-allocation (ascending | descending);
  calling-number number;
  incoming-called-number number <reject>;
  spid1 spid-string;
  spid2 spid-string;
  static-tei-val value;
  switch-type (att5e | etsi | ni1 | ni2 | ntdms100 | ntt);
  t310 seconds;
  tei-option (first-call | power-up);
}
keepalives <down-count number> <interval seconds> <up-count number>;
link-mode mode;
lmi {
  lmi-type (ansi | itu);
  n391dte number;
  n392dce number;
  n392dte number;
  n393dce number;
  n393dte number;
  t391dte seconds;
  t392dce seconds;
}
lsq-failure-options {

```

```

    no-termination-request;
    trigger-link-failure interface-name;
}
mac mac-address;
mlfr-uni-nni-bundle-options {
    acknowledge-retries number;
    acknowledge-timer milliseconds;
    action-red-differential-delay (disable-tx | remove-link);
    cisco-interoperability send-lip-remove-link-for-link-reject;
    drop-timeout milliseconds;
    fragment-threshold bytes;
    hello-timer milliseconds;
    link-layer-overhead percent;
    lmi-type (ansi | itu);
    minimum-links number;
    mrru bytes;
    n391 number;
    n392 number;
    n393 number;
    red-differential-delay milliseconds;
    t391 seconds;
    t392 seconds;
    yellow-differential-delay milliseconds;
}
modem-options {
    dialin (console | routable);
    init-command-string initialization-command-string;
}
mtu bytes;
multiservice-options {
    (core-dump | no-core-dump);
    (syslog | no-syslog);
}
native-vlan-id number;
no-gratuitous-arp-request;
no-keepalives;
no-partition {
    interface-type type;
}
optics-options {
    wavelength nm;
}
partition partition-number interface-type type oc-slice oc-slice-range
    timeslots time-slot-range;
passive-monitor-mode;
per-unit-scheduler;
ppp-options {
    chap {
        access-profile profile-name;
        default-chap-secret secret;
        local-name name;
        passive;
    }
    compression {
        acfc;
        pfc;
    }
}

```

```

    }
    lcp-restart-timer milliseconds;
    loopback-clear-timer seconds;
    ncp-restart-timer milliseconds;
    no-termination-request;
    pap {
        access-profile profile-name;
        local-name name;
        local-password password;
        passive;
    }
}
receive-bucket {
    overflow (discard | tag);
    rate percentage;
    threshold bytes;
}
redundancy-options {
    (hot-standby | warm-standby);
    primary (lsq | sp)-fpc/pic/port;
    secondary (lsq | sp)-fpc/pic/port;
}
redundant-ether-options {
    (flow-control | no-flow-control);
    link-speed (10m | 100m | 1g);
    (loopback | no-loopback);
    redundancy-group group-name;
    source-address-filter mac-address;
    (source-filtering | no-source-filtering);
}
schedulers number;
serial-options {
    clock-rate rate;
    clocking-mode (dce | internal | loop);
    control-polarity (positive | negative);
    cts-polarity (positive | negative);
    dcd-polarity (positive | negative);
    dce-options {
        ... dce-options-configuration ...
    }
    dsr-polarity (positive | negative);
    dte-options {
        ... dte-options-configuration ...
    }
    dtr-circuit (balanced | unbalanced);
    dtr-polarity (positive | negative);
    encoding (nrz | nrzi);
    indication-polarity (positive | negative);
    line-protocol protocol;
    loopback mode;
    rts-polarity (positive | negative);
    tm-polarity (positive | negative);
    transmit-clock invert;
    dce-options {
        control-signal (assert | de-assert | normal);
        cts (ignore | normal | require);
    }
}

```



```

    dcd (ignore | normal | require);
    dsr (ignore | normal | require);
    dtr signal-handling-option;
    ignore-all;
    indication (ignore | normal | require);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
  }
  dte-options {
    control-signal (assert | de-assert | normal);
    cts (ignore | normal | require);
    dcd (ignore | normal | require);
    dsr (ignore | normal | require);
    dtr signal-handling-option;
    ignore-all;
    indication (ignore | normal | require);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
  }
}
services-options {
  inactivity-timeout seconds;
  open-timeout seconds;
  syslog {
    host hostname {
      facility-override facility-name;
      log-prefix prefix-number;
      services priority-level;
    }
  }
}
shared-uplink;
shared-scheduler;
shdsl-options {
  annex (annex-a | annex-b);
  line-rate line-rate;
  loopback (local | remote);
  snr-margin {
    current margin;
    snext margin;
  }
}
sonet-options {
  aggregate asx;
  aps {
    advertise-interval milliseconds;
    authentication-key key;
    force;
    hold-time milliseconds;
    logout;
    neighbor address;
    paired-group group-name;
    preserve-interfaces;
    protect-circuit group-name;
    request;
    revert-time seconds;
  }
}

```

```

        switching-mode (bidirectional | unidirectional);
        working-circuit group-name;
    }
    bytes {
        c2 value;
        e1-quiet value;
        f1 value;
        f2 value;
        s1 value;
        z3 value;
        z4 value;
    }
    fcs (32 | 16);
    loopback (local | remote);
    mpls {
        pop-all-labels {
            required-depth number;
        }
    }
    path-trace trace-string;
    (payload-scrambler | no-payload-scrambler);
    rfc-2615;
    trigger {
        defect ignore;
        hold-time up milliseconds down milliseconds;
    }
}
speed (10m | 100m | 1g | oc3 | oc12 | oc48);
stacked-vlan-tagging;
switch-options {
    switch-port port-number {
        (auto-negotiation | no-auto-negotiation);
        speed (10m | 100m | 1g);
        link-mode (full-duplex | half-duplex);
    }
}
t1-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    buildout value;
    byte-encoding (nx56 | nx64);
    crc-major-alarm-threshold (1e-3 | 5e-4 | 1e-4 | 5e-5 | 1e-5);
    crc-minor-alarm-threshold (1e-3 | 5e-4 | 1e-4 | 5e-5 | 1e-5 | 5e-6 | 1e-6);
    fcs (16 | 32);
    framing (esf | sf);
    idle-cycle-flags (flags | ones);
    invert-data;
    line-encoding (ami | b8zs);
    loopback (local | payload | remote);
    remote-loopback-respond;
    start-end-flag (filler | shared);
    timeslots slot-number;
}
t3-options {
    atm-encapsulation (direct | plcp);
}

```

```

bert-algorithm algorithm;
bert-error-rate rate;
bert-period seconds;
buildout feet;
(cbit-parity | no-cbit-parity);
compatibility-mode (adtran | digital-link | kentrox | larscom | verilink)
    <subrate value>;
fcs (16 | 32);
(feac-loop-respond | no-feac-loop-respond);
idle-cycle-flag value;
(long-buildout | no-long-buildout);
(loop-timing | no-loop-timing);
loopback (local | payload | remote);
(mac | no-mac);
(payload-scrambler | no-payload-scrambler);
start-end-flag value;
}
traceoptions {
    flag flag;
}
transmit-bucket {
    overflow (tag | discard);
    rate percentage;
    threshold bytes;
}
(traps | no-traps);
unidirectional;
unit logical-unit-number {
    ... unit-configuration ...
}
vlan-tagging;
vlan-vci-tagging;
vtmapping (itu-t | klm);
(z0-increment | no-z0-increment);
unit logical-unit-number {
    disable;
    accept-source-mac {
        mac-address mac-address;
        policer {
            input policer-name;
            output policer-name;
        }
    }
}
accounting-profile profile-name;
allow-any-vci;
atm-scheduler-map (default | map-name);
backup-options {
    interface interface-name;
}
bandwidth rate;
cell-bundle-size cells;
clear-dont-fragment-bit;
compression {
    rtp {
        f-max-period number;
        port {

```

```

        maximum port-number;
        minimum port-number;
    }
    queues [ queue-numbers ];
}
compression-device interface-name;
copy-tos-to-outer-ip-header;
demux-destination family;
demux-source family;
demux-options {
    underlying-interface interface-name;
}
description text;
dial-options {
    l2tp-interface-id name;
    ipsec-interface-id name;
    (dedicated | shared);
}
dialer-options {
    activation-delay seconds;
    callback;
    callback-wait-period time;
    deactivation-delay seconds;
    dial-string [ dial-string-numbers ];
    idle-timeout seconds;
    incoming-map {
        (accept-all | caller caller-number);
    }
    initial-route-check seconds;
    load-interval seconds;
    load-threshold number;
    pool pool;
    redial-delay time;
    watch-list {
        routes;
    }
}
disable-mlppp-inner-ppp-pfc;
dlci dlci-identifier;
drop-timeout milliseconds;
dynamic-call-admission-control {
    activation-priority number;
    bearer-bandwidth-limit threshold;
}
encapsulation type;
epd-threshold cells plp1 cells;
family family-name {
    ... family-configuration ...
}
filter filter-name;
fragment-threshold bytes;
inner-vlan-id-range start start-id end end-id;
input-vlan-map {
    (pop | pop-pop | pop-swap | push | push-push | swap | swap-push | swap-swap);
    inner-tag-protocol-id tpid;
}

```

```

    inner-vlan-id number;
    tag-protocol-id tpid;
    vlan-id number;
}
interleave-fragments;
inverse-arp;
(keepalives | no-keepalives);
layer2-policer {
    input-policer policer-name;
    input-three-color policer-name;
    output-policer policer-name;
    output-three-color policer-name;
}
link-layer-overhead percent;
minimum-links number;
mrru bytes;
multicast-dlci dlci-identifier;
multicast-vci vpi-identifier.vci-identifier;
multipoint;
oam-liveness {
    up-count cells;
    down-count cells;
}
oam-period (disable | seconds);
output-vlan-map {
    (pop | pop-pop | pop-swap | push | push-push | swap | swap-push | swap-swap);
    inner-tag-protocol-id tpid;
    inner-vlan-id number;
    tag-protocol-id tpid;
    vlan-id number;
}
passive-monitor-mode;
peer-unit unit-number;
plp-to-clp;
point-to-point;
ppp-options {
    chap {
        access-profile profile-name;
        default-chap-secret secret;
        local-name name;
        passive;
    }
    compression {
        acfc;
        pfc;
    }
    lcp-restart-timer milliseconds;
    loopback-clear-timer seconds;
    ncp-restart-timer milliseconds;
    pap {
        access-profile profile-name;
        default-pap-password password;
        local-name name;
        local-password password;
        passive;
    }
}

```

```

}
pppoe-options {
    access-concentrator name;
    auto-reconnect seconds;
    (client | server);
    service-name name;
    underlying-interface interface-name;
}
proxy-arp;
reassemble-packets;
rpm client;
service-domain (inside | outside);
shaping {
    (cbr rate | rtvbr peak rate sustained rate burst length |
     vbr peak rate sustained rate burst length);
    queue-length number;
}
short-sequence;
transmit-weight number;
(traps | no-traps);
trunk-bandwidth rate;
trunk-id number;
tunnel {
    allow-fragmentation;
    backup-destination address;
    destination destination-address;
    do-not-fragment;
    key number;
    routing-instance {
        destination routing-instance-name;
    }
    source source-address;
    ttl number;
}
uplink-shared-with psdn;
vci vpi-identifier.vci-identifier;
vci-range start start-vci end end-vci;
vpi vpi-identifier;
vlan-id number;
vlan-id-range number-number;
vlan-tags inner tpid.vlan-id outer tpid.vlan-id;
family family-name {
    accounting {
        destination-class-usage;
        source-class-usage {
            (input | output | input output);
        }
    }
}
address address {
    ... address-configuration ...
}
bundle interface-name;
dhcp {
    client-identifier (ascii text | hexadecimal hexadecimal-value);
    lease-time seconds;
    retransmission-attempt number;
}

```

```

    retransmission-interval seconds;
    server-address address;
    update-server;
    vendor-id identifier;
}
filter {
    dialer filter-name;
    group filter-group-number;
    (input filter-name | input-list [ filter-names ]);
    (output filter-name | output-list [ filter-names ]);
}
ipsec-sa sa-name;
interface-mode (access | trunk);
keep-address-and-control;
mac-validate (loose | strict);
mtu bytes;
multicast-only;
negotiate-address;
next-hop-tunnel gateway-address ipsec-vpn vpn-name;
no-redirects;
policer {
    arp policer-template-name;
    input policer-template-name;
    output policer-template-name;
}
primary;
protocols [ inet iso mpls ];
proxy inet-address address;
receive-options-packets;
receive-ttl-exceeded;
remote (inet-address address | mac-address address);
rpf-check <fail-filter filter-name> {
    mode loose;
}
sampling {
    (input | output | input output);
}
service {
    input {
        post-service-filter filter-name;
        service-set service-set-name <service-filter filter-name>;
    }
    output {
        service-set service-set-name <service-filter filter-name>;
    }
}
simple-filter {
    input filter-name;
}
(translate-discard-eligible | no-translate-discard-eligible);
(translate-fecn-and-becn | no-translate-fecn-and-becn);
unnumbered-address interface-name <destination address
    destination-profile profile-name | preferred-source-address address>
vlan-id number;
vlan-id-list [ number number-number ];
address address {

```

```

arp ip-address (mac | multicast-mac) mac-address <publish>;
broadcast address;
destination destination-address;
destination-profile name;
eui-64;
multipoint-destination destination-address (dlci dlci-identifier |
    vci vci-identifier);
multipoint-destination destination-address {
    epd-threshold cells plp1 cells;
    inverse-arp;
    oam-liveness {
        down-count cells;
        up-count cells;
    }
    oam-period (disable | seconds);
    shaping {
        (cbr rate | rtvbr peak rate sustained rate burst length |
            vbr peak rate sustained rate burst length);
        queue-length number;
    }
    transmit-weight number;
    vci vpi-identifier.vci-identifier;
}
preferred;
primary;
vrrp-group group-number {
    (accept-data | no-accept-data);
    advertise-interval seconds;
    authentication-key key;
    authentication-type authentication;
    fast-interval-statement milliseconds;
    (preempt <hold-time seconds> | no-preempt) {
    priority number;
    track {
        interface interface-name {
            bandwidth-threshold bits-per-second priority-cost priority;
            priority-cost priority;
        }
        priority-hold-time seconds;
        route prefix routing-instance instance-name priority-cost priority;
    }
    virtual-address [ addresses ];
}
vrrp-inet6-group group-number {
    (accept-data | no-accept-data);
    fast-interval milliseconds;
    inet6-advertise-interval seconds;
    (preempt <hold-time seconds> | no-preempt) {
    priority number;
    track {
        interface interface-name {
            bandwidth-threshold bits-per-second priority-cost priority;
            priority-cost priority;
        }
        priority-hold-time seconds;
    }
}

```



```

        route prefix routing-instance instance-name priority-cost priority;
    }
    virtual-inet6-address [ addresses ];
    virtual-link-local-address ipv6-address;
}
web-authentication http;
}
}
}
}
interface-set interface-set-name {
    interface ethernet-interface-name {
        (unit unit-number | vlan-tags-outer vlan-tag);
    }
}
traceoptions {
    file <filename> <files number> <match regular-expression>
        <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag <disable>;
    no-remote-trace;
}
}

```

[edit logical-systems] Hierarchy Level

As indicated in the following hierarchy, you can include at this hierarchy level several of the hierarchies that can be included at the [edit] hierarchy level. However, some statements in a subhierarchy are not valid for logical systems. To learn which statements can be included on your platform, issue the **set ?** command at the hierarchy level of interest.

```
logical-systems {
  logical-system-name {
    access {
      address-assignment {
        ... same statements as listed in the address-assignment subhierarchy in [edit
        access] Hierarchy Level ...
      }
    }
    access-profile profile-name;
    firewall {
      ... same statements as listed in several subhierarchies in [edit firewall] Hierarchy
      Level ...
    }
    forwarding-options {
      ... same statements as listed in the dhcp-relay subhierarchy in [edit
      forwarding-options] Hierarchy Level ...
    }
    interfaces {
      interface-name {
        unit logical-unit-number {
          ... some of the statements listed in the unit subhierarchy in [edit interfaces]
          Hierarchy Level ...
        }
      }
    }
    policy-options {
      ... same statements as listed in [edit policy-options] Hierarchy Level ...
    }
    protocols {
      ... same statements as listed in [edit protocols] Hierarchy Level ...
    }
    routing-instances {
      ... most statements listed in [edit routing-instances] Hierarchy Level ...
    }
    routing-options {
      ... most statements listed in [edit routing-options] Hierarchy Level ...
    }
    system {
      services {
        dhcp-local-server {
          ... same statements as listed in the services dhcp-local-server subhierarchy
          in [edit system] Hierarchy Level ...
        }
      }
    }
  }
}
```

[edit multicast-snooping-options] Hierarchy Level

```

multicast-snooping-options {
  flood-groups [ ip-addresses ];
  forwarding-cache {
    threshold suppress value <reuse value>;
  }
  graceful-restart <restart-duration seconds>;
  options {
    syslog {
      level severity-level;
      mark seconds;
      upto severity-level;
    }
  }
  traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
      no-world-readable>;
    flag flag <disable>;
  }
}

```

[edit poe] Hierarchy Level

```
poe {  
  guard-band watts;  
  interface (all | interface-name) {  
    disable;  
    maximum-power watts;  
    priority (high | low);  
    telemetries {  
      disable;  
      duration hours;  
      interval minutes;  
    }  
  }  
  management (class | static);  
  notification-control {  
    fpc fpc-number {  
      disable;  
    }  
  }  
}
```

[edit policy-options] Hierarchy Level

Several statements in the [edit policy-options] hierarchy are valid at numerous locations within the hierarchy. To make the complete hierarchy easier to read, the repeated statements are listed in the following sections, which are referenced at the appropriate locations in “Complete [edit policy-options] Hierarchy” on page 116.

- Common Policy Terms on page 113
- Common Policy Match Conditions on page 114
- Common Ingress Policy Match Conditions on page 115
- Complete [edit policy-options] Hierarchy on page 116

Common Policy Terms

This section lists statements that are valid at each of the following hierarchy levels, and is referenced at those levels in “Common Ingress Policy Match Conditions” on page 115 and “Complete [edit policy-options] Hierarchy” on page 116 instead of the statements being repeated.

- [edit policy-options policy-statement *policy-name* from prefix-list-filter *prefix-list-name* (exact | longer | orlonger)]
- [edit policy-options policy-statement *policy-name* from route-filter *ip-prefix*</*prefix-length*> (exact | longer | orlonger | through *ip-prefix*</*prefix-length*> | upto /*prefix-length*)]
- [edit policy-options policy-statement *policy-name* from source-address-filter *ip-prefix*</*prefix-length*> (exact | longer | orlonger | through *ip-prefix*</*prefix-length*> | upto /*prefix-length*)]
- [edit policy-options policy-statement *policy-name* term *term-name* from prefix-list-filter *prefix-list-name* (exact | longer | orlonger)]
- [edit policy-options policy-statement *policy-name* term *term-name* from route-filter *ip-prefix*</*prefix-length*> (exact | longer | orlonger | through *ip-prefix*</*prefix-length*> | upto /*prefix-length*)]
- [edit policy-options policy-statement *policy-name* term *term-name* from source-address-filter *ip-prefix*</*prefix-length*> (exact | longer | orlonger | through *ip-prefix*</*prefix-length*> | upto /*prefix-length*)]
- [edit policy-options policy-statement *policy-name* then]
- [edit policy-options policy-statement *policy-name* term *term-name* then]

The common policy terms are as follows:

```
(accept | reject);
as-path-expand (as-number | last-as) <count number>;
as-path-prepend as-number;
class class-name;
color (preference | add number | subtract number);
color2 (preference | add number | subtract number);
community (add | delete | set | + | - | =) community-name;
cos-next-hop-map map-name;
```

```

damping list-name;
default-action (accept | reject);
destination-class class-name;
external {
    type (1 | 2);
}
forwarding-class class-name;
install-nexthop <strict> (lsp [ /lsp-names ] | lsp-regex [ regular-expressions ])
    <except (lsp [ /lsp-names ] | lsp-regex [ regular-expressions ])>;
load-balance per-packet;
local-preference (preference | add number | subtract number);
metric (metric-value | add number | igp <metric-offset> | minimum-igp <metric-offset> |
    subtract number | ... the following complex expression ...);
expression {
    metric (multiplier number | offset number | multiplier number offset number);
    metric2 (multiplier number | offset number | multiplier number offset number);
}
metric2 (metric-value | add number | subtract number);
metric3 (metric-value | add number | subtract number);
metric4 (metric-value | add number | subtract number);
next (policy | term);
next-hop (ip-address | discard | next-table routing-table-name | peer-address | reject |
    self);
origin (egp | igp | incomplete);
preference (preference | add number | subtract number);
preference2 (preference | add number | subtract number);
priority (high | low | medium);
source-class class-name;
tag (tag-number | add number | subtract number);
tag2 (tag-number | add number | subtract number);
trace;

```

Common Policy Match Conditions

This section lists statements that are valid at all of the following hierarchy levels, and is referenced at those levels in “Complete [edit policy-options] Hierarchy” on page 116 instead of the statements being repeated.

- [edit policy-options policy-statement *policy-name* from]
- [edit policy-options policy-statement *policy-name* term *term-name* from]
- [edit policy-options policy-statement *policy-name* term *term-name* to]
- [edit policy-options policy-statement *policy-name* to]

The common policy match conditions are as follows:

```

area area-id;
as-path [ regular-expression-names ];
as-path-group [ as-path-group-names ];
color preference;
color2 preference;
community [ community-names ];
external {
    type (1 | 2);
}

```

```

}
family family-name;
instance instance-name;
interface [ interface-names ];
level isis-level;
local-preference value;
metric metric-value;
metric2 metric-value;
metric3 metric-value;
metric4 metric-value;
neighbor [ ip-addresses ];
next-hop [ ip-addresses ];
origin (egp | igp | incomplete);
policy [ policy-names ];
preference preference;
preference2 preference;
protocol [ protocol-names ];
rib routing-table-name;
tag [ tag-numbers ];
tag2 tag-number;

```

Common Ingress Policy Match Conditions

This section lists statements that are valid at each of the following hierarchy levels, and is referenced at those levels in “Complete [edit policy-options] Hierarchy” on page 116 instead of the statements being repeated at each level.

- [edit policy-options policy-statement *policy-name* from]
- [edit policy-options policy-statement *policy-name* term *term-name* from]

The common ingress policy match conditions are as follows:

```

aggregate-contributor;
condition [ conditions ];
multicast-scope (scope-value | global | link-local | node-local | organization-local |
  site-local) <orhigher | orlower>;
next-hop-type merged;
prefix-list prefix-list-name;
prefix-list-filter prefix-list-name (exact | longer | orlonger) {
  ... statements listed in Common Policy Terms ...;
}
route-filter ip-prefix</prefix-length> (exact | longer | orlonger |
  through ip-prefix</prefix-length> | upto /prefix-length) {
  ... statements listed in Common Policy Terms ...;
}
route-type (external | internal);
source-address-filter ip-prefix</prefix-length> (exact | longer | orlonger |
  through ip-prefix</prefix-length> | upto /prefix-length) {
  ... statements listed in Common Policy Terms ...;
}
state (active | inactive);

```

Complete [edit policy-options] Hierarchy

The statement hierarchy in this section can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

policy-options {
  as-path name regular-expression;
  as-path-group group-name {
    as-path name regular-expression;
  }
  community name {
    invert-match;
    members [ community-ids ];
  }
  condition condition-name {
    if-route-exists address table table-name;
    route-active-on (node0 | node1);
  }
  damping name {
    disable;
    half-life minutes;
    max-suppress minutes;
    reuse number;
    suppress number;
  }
  policy-statement policy-name {
    from {
      ... statements listed in Common Policy Match Conditions AND ...
      ... statements listed in Common Ingress Policy Match Conditions ...
    }
    term term-name {
      from {
        ... statements listed in Common Policy Match Conditions AND ...
        ... statements listed in Common Ingress Policy Match Conditions ...
      }
      to {
        ... statements listed in Common Policy Match Conditions ...
      }
      then {
        ... statements listed in Common Policy Terms ...
      }
    }
  }
  to {
    ... statements listed in Common Policy Match Conditions ...
  }
  then {
    ... statements listed in Common Policy Terms ...
  }
}
prefix-list list-name {
  ip-prefix</prefix-length>;
  apply-path path;
}
}

```


[edit protocols] Hierarchy Level

Each of the following sections lists the statements at a subhierarchy of the [edit protocols] hierarchy.

- [edit protocols ancp] Hierarchy Level on page 118
- [edit protocols bfd] Hierarchy Level on page 118
- [edit protocols bgp] Hierarchy Level on page 119
- [edit protocols connections] Hierarchy Level on page 127
- [edit protocols dlsu] Hierarchy Level on page 128
- [edit protocols dot1x] Hierarchy Level on page 129
- [edit protocols dvmrp] Hierarchy Level on page 130
- [edit protocols esis] Hierarchy Level on page 131
- [edit protocols gvrp] Hierarchy Level on page 132
- [edit protocols igmp] Hierarchy Level on page 133
- [edit protocols igmp-snooping] Hierarchy Level on page 134
- [edit protocols ilmi] Hierarchy Level on page 135
- [edit protocols isis] Hierarchy Level on page 136
- [edit protocols l2circuit] Hierarchy Level on page 139
- [edit protocols l2iw] Hierarchy Level on page 140
- [edit protocols l2-learning] Hierarchy Level on page 141
- [edit protocols lacp] Hierarchy Level on page 142
- [edit protocols layer2-control] Hierarchy Level on page 143
- [edit protocols ldp] Hierarchy Level on page 144
- [edit protocols link-management] Hierarchy Level on page 147
- [edit protocols lldp] Hierarchy Level on page 148
- [edit protocols lldp-med] Hierarchy Level on page 149
- [edit protocols mld] Hierarchy Level on page 150
- [edit protocols mpls] Hierarchy Level on page 151
- [edit protocols msdp] Hierarchy Level on page 156
- [edit protocols mstp] Hierarchy Level on page 158
- [edit protocols neighbor-discovery] Hierarchy Level on page 159
- [edit protocols oam] Hierarchy Level on page 160
- [edit protocols ospf] Hierarchy Level on page 162
- [edit protocols ospf3] Hierarchy Level on page 166
- [edit protocols pgm] Hierarchy Level on page 168
- [edit protocols pim] Hierarchy Level on page 169
- [edit protocols ppp] Hierarchy Level on page 172
- [edit protocols protection-group] Hierarchy Level on page 173

- [edit protocols rip] Hierarchy Level on page 174
- [edit protocols ripng] Hierarchy Level on page 176
- [edit protocols router-advertisement] Hierarchy Level on page 177
- [edit protocols router-discovery] Hierarchy Level on page 178
- [edit protocols rstp] Hierarchy Level on page 179
- [edit protocols rsvp] Hierarchy Level on page 180
- [edit protocols sap] Hierarchy Level on page 182
- [edit protocols sflow] Hierarchy Level on page 183
- [edit protocols vrrp] Hierarchy Level on page 184
- [edit protocols vstp] Hierarchy Level on page 185

[edit protocols ancp] Hierarchy Level

```

protocols {
  ancp {
    adjacency-timer seconds;
    interfaces {
      interface-set interface-set-name {
        access-identifier "identifier";
      }
    }
    maximum-helper-restart-time seconds;
    neighbor ip-address;
    pre-ietf-mode;
    qos-adjust;
    traceoptions {
      file <filename> <files number> <match regular-expression>
        <size maximum-file-size> <world-readable | no-world-readable>;
      flag flag;
      level (all | error | info | notice | verbose | warning);
      no-remote-trace;
    }
  }
}

```

[edit protocols bfd] Hierarchy Level

```

protocols {
  bfd {
    no-issu-timer-negotiation;
    traceoptions {
      file <filename> <files number> <match regular-expression>
        <size maximum-file-size> <world-readable | no-world-readable>;
      flag flag;
      no-remote-trace;
    }
  }
}

```

[edit protocols bgp] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  bgp {
    disable;
    accept-remote-nexthop;
    advertise-external <conditional>;
    advertise-inactive;
    advertise-peer-as;
    authentication-algorithm algorithm;
    authentication-key key;
    authentication-key-chain key-chain;
    bfd-liveness-detection {
      detection-time {
        threshold milliseconds;
      }
      holddown-interval milliseconds;
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      version (1 | automatic);
    }
    cluster cluster-identifier;
    damping;
    description text-description;
    export [ policy-names ];
    family {
      ... family-configuration ...
    }
    graceful-restart {
      disable;
      restart-time seconds;
      stale-routes-time seconds;
    }
    group {
      ... group-configuration ...
    }
    hold-time seconds;
    import [ policy-names ];
    include-mp-next-hop;
    ipsec-sa ipsec-sa;
    keep (all | none);
    local-address address;
    local-as autonomous-system <loops number> <private>;
    local-interface interface-name;
    local-preference local-preference;
    log-updown;
  }
}

```

```

metric-out (metric | igp (delay-med-update | offset) | minimum-igp offset);
mtu-discovery;
multihop {
    no-nexthop-change;
    ttl ttl-value;
}
no-advertise-peer-as;
no-aggregator-id;
no-client-reflect;
outbound-route-filter {
    bgp-orf-cisco-mode;
    prefix-based {
        accept {
            inet;
            inet6;
        }
    }
}
out-delay seconds;
passive;
path-selection {
    always-compare-med;
    cisco-non-deterministic;
    external-router-id;
    med-plus-igp {
        igp-multiplier number;
        med-multiplier number;
    }
}
peer-as autonomous-system;
preference preference;
remove-private;
tcp-mss segment-size;
traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
vpn-apply-export;
family {
    family-name {
        (any | flow | multicast | signaling | unicast) {
            accepted-prefix-limit {
                maximum number;
                teardown <percentage> <idle-timeout (forever | minutes)>;
            }
            aggregate-label <community community-name>;
            no-validate [ validation-procedure-names ];
            prefix-limit {
                maximum number;
                teardown <percentage> <idle-timeout (forever | minutes)>;
            }
            rib-group group-name;
            topology name;
            community target identifier;
        }
    }
}

```

```

}
labeled-unicast {
  accepted-prefix-limit {
    maximum number;
    teardown <percentage> <idle-timeout (forever | minutes)>;
  }
  aggregate-label {
    community community-name;
  }
  explicit-null {
    connected-only;
  }
  per-group-label;
  prefix-limit {
    maximum number;
    teardown <percentage> <idle-timeout (forever | minutes)>;
  }
  resolve-vpn;
  rib inet.3;
  rib-group group-name;
  traffic-statistics {
    file filename <files number> <size maximum-file-size> <world-readable |
      no-world-readable>;
    interval seconds;
  }
}
}
route-target {
  accepted-prefix-limit {
    maximum number;
    teardown <percentage> <idle-timeout (forever | minutes)>;
  }
  advertise-default;
  external-paths number;
  prefix-limit {
    maximum number;
    teardown <percentage> <idle-timeout (forever | minutes)>;
  }
}
}
group group-name {
  accept-remote-nexthop;
  advertise-external <conditional>;
  advertise-inactive;
  advertise-peer-as;
  allow [ ip-prefix</prefix-length> ];
  as-override;
  authentication-algorithm algorithm;
  authentication-key key;
  authentication-key-chain key-chain;
  bfd-liveness-detection {
    detection-time {
      threshold milliseconds;
    }
  }
  holddown-interval milliseconds;
  minimum-interval milliseconds;
}

```

```

    minimum-receive-interval milliseconds;
    multiplier number;
    no-adaptation;
    transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
    }
    version (1 | automatic);
}
cluster cluster-identifier;
damping;
description text-description;
export [ policy-names ];
family family-name {
    ... group-family-configuration ...
}
graceful-restart {
    disable;
    restart-time seconds;
    stale-routes-time seconds;
}
hold-time seconds;
import [ policy-names ];
ipsec-sa ipsec-sa;
keep (all | none);
local-address address;
local-as autonomous-system <private>;
local-interface interface-name;
local-preference local-preference;
log-updown;
metric-out (metric | igp (delay-med-update | offset) | minimum-igp offset);
mtu-discovery;
multihop {
    no-nexthop-change;
    ttl tvl-value;
}
multipath <multiple-as>;
neighbor address {
    ... neighbor-configuration ...
}
no-advertise-peer-as;
no-aggregator-id;
no-client-reflect;
outbound-route-filter {
    bgp-orf-cisco-mode;
    prefix-based {
        accept {
            inet;
            inet6;
        }
    }
}
out-delay seconds;
passive;
peer-as autonomous-system;
preference preference;

```

```

remove-private;
tcp-mss segment-size;
traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
type type;
vpn-apply-export;
family {
    (inet | inet-vpn | inet6 | inet6-vpn | iso-vpn) {
        (any | flow | labeled-unicast | multicast | unicast) {
            accepted-prefix-limit {
                maximum number;
                teardown <percentage> <idle-timeout (forever | minutes)>;
            }
            aggregate-label {
                community community-name;
            }
            explicit-null {
                connected-only;
            }
            no-validate [ validation-procedure-names ];
            per-group-label;
            prefix-limit {
                maximum number;
                teardown <percentage> <idle-timeout (forever | minutes)>;
            }
            resolve-vpn;
            rib inet.3;
            rib-group group-name;
            traffic-statistics {
                file filename <files number> <size maximum-file-size> <world-readable |
                    no-world-readable>;
                interval seconds;
            }
        }
    }
}
(inet-mdt | inet-mvpn | inet6-mvpn | l2-vpn) {
    signaling {
        accepted-prefix-limit {
            maximum number;
            teardown <percentage> <idle-timeout (forever | minutes)>;
        }
        prefix-limit {
            maximum number;
            teardown <percentage> <idle-timeout (forever | minutes)>;
        }
        rib-group group-name;
    }
}
route-target {
    accepted-prefix-limit {
        maximum number;
        teardown <percentage> <idle-timeout (forever | minutes)>;
    }
}

```

```

    advertise-default;
    external-paths number;
    prefix-limit {
        maximum number;
        teardown <percentage> <idle-timeout (forever | minutes)>;
    }
}
}
neighbor address {
    accept-remote-nexthop;
    advertise-external <conditional>;
    advertise-inactive;
    advertise-peer-as;
    as-override;
    authentication-algorithm algorithm;
    authentication-key key;
    authentication-key-chain key-chain;
    bfd-liveness-detection {
        detection-time {
            threshold milliseconds;
        }
        holddown-interval milliseconds;
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
        }
        multiplier number;
        version (1 | automatic);
    }
    cluster cluster-identifier;
    damping;
    description text-description;
    export [ policy-names ];
    family family-name {
        ... group-neighbor-family-configuration ...
    }
    graceful-restart {
        disable;
        restart-time seconds;
        stale-routes-time seconds;
    }
    hold-time seconds;
    import [ policy-names ];
    include-mp-next-hop;
    ipsec-sa ipsec-sa;
    keep (all | none);
    local-address address;
    local-as autonomous-system <private>;
    local-interface interface-name;
    local-preference local-preference;
    log-updown;
    metric-out (metric | igp (delay-med-update | offset) | minimum-igp offset);
    mtu-discovery;
    multihop {

```



```

    no-nexthop-change;
    ttl ttl-value;
}
multipath <multiple-as>;
no-advertise-peer-as;
no-aggregator-id;
no-client-reflect;
outbound-route-filter {
    bgp-orf-cisco-mode;
    prefix-based {
        accept {
            inet;
            inet6;
        }
    }
}
out-delay seconds;
passive;
peer-as autonomous-system;
preference preference;
remove-private;
tcp-mss segment-size;
traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
vpn-apply-export;
family {
    (inet | inet-vpn | inet6 | inet6-vpn | iso-vpn) {
        (any | flow | labeled-unicast | multicast | unicast) {
            accepted-prefix-limit {
                maximum number;
                teardown <percentage> <idle-timeout (forever | minutes)>;
            }
            aggregate-label {
                community community-name;
            }
            explicit-null {
                connected-only;
            }
            no-validate [ validation-procedure-names ];
            per-group-label;
            prefix-limit {
                maximum number;
                teardown <percentage> <idle-timeout (forever | minutes)>;
            }
            resolve-vpn;
            rib inet.3;
            rib-group group-name;
            traffic-statistics {
                file filename <files number> <size maximum-file-size>
                    <world-readable | no-world-readable>;
                interval seconds;
            }
        }
    }
}

```

```

}
(inet-mvpn | inet6-mvpn | l2-vpn) {
    signaling {
        prefix-limit {
            maximum number;
            teardown <percentage> <idle-timeout (forever | minutes)>;
        }
        rib-group group-name;
    }
}
route-target {
    accepted-prefix-limit {
        maximum number;
        teardown <percentage> <idle-timeout (forever | minutes)>;
    }
    advertise-default;
    external-paths number;
    prefix-limit {
        maximum number;
        teardown <percentage> <idle-timeout (forever | minutes)>;
    }
}
}
}
}
}
}
```

[edit protocols connections] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  connections {
    interface-switch connection-name {
      interface interface-name.unit-number;
    }
    lsp-switch connection-name {
      receive-lsp label-switched-path;
      transmit-lsp label-switched-path;
    }
    p2mp-receive-switch switch-name {
      output-interface [ interface-name.unit-number ];
      receive-p2mp-lsp lsp-name;
    }
    p2mp-transmit-switch switch-name {
      input-interface interface-name.unit-number;
      transmit-p2mp-lsp lsp-name;
    }
    remote-interface-switch connection-name {
      interface interface-name.unit-number;
      receive-lsp label-switched-path;
      transmit-lsp label-switched-path;
    }
  }
}

```

[edit protocols dlsw] Hierarchy Level

```

protocols {
  dlsw {
    connection-idle-timeout seconds;
    dlsw-cos {
      destination-interface interface-name;
      type-of-service tos-value;
    }
    explorer-wait-time seconds;
    load-balance circuit-weight;
    local-peer ipv4-address;
    multicast-address address;
    promiscuous;
    reachability-cache-timeout seconds;
    receive-initial-pacing count;
    remote-peer peer-address {
      circuit-weight weight;
      cost cost;
      keepalive-interval seconds;
    }
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag;
    }
  }
}

```

[edit protocols dot1x] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  dot1x {
    authenticator {
      authentication-profile-name profile-name;
      interface interface-name {
        disable;
        guest-vlan vlan-name;
        maximum-requests request-number;
        quiet-period seconds;
        (reauthentication seconds | no-reauthentication);
        retries number;
        server-timeout seconds;
        supplicant (multiple | single | single-secure);
        supplicant-timeout seconds;
        transmit-period seconds;
      }
      static mac-address {
        interface interface-name;
        vlan-assignment vlan-identifier;
      }
    }
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <disable>;
    }
  }
}

```

[edit protocols dvmrp] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  dvmrp {
    disable;
    export [ policy-names ];
    import [ policy-names ];
    interface interface-name {
      disable;
      hold-time seconds;
      metric metric;
      mode (forwarding | unicast-routing);
    }
    rib-group group-name;
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
  }
}

```

[edit protocols esis] Hierarchy Level

```

protocols {
  esis {
    disable;
    graceful-restart {
      disable;
      restart-duration seconds;
    }
    interface (interface-name | all) {
      disable;
      end-system-configuration-timer seconds;
      hold-time seconds;
    }
    preference preference;
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
  }
}

```

[edit protocols gvrp] Hierarchy Level

```
protocols {  
  gvrp {  
    disable;  
    interface interface-name {  
      disable;  
    }  
    join-timer milliseconds;  
    leave-timer milliseconds;  
    leaveall-timer milliseconds;  
  }  
}
```


[edit protocols igmp] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  igmp {
    accounting;
    interface interface-name {
      disable;
      (accounting | no-accounting);
      immediate-leave;
      promiscuous-mode;
      ssm-map ssm-map-name:
      static {
        group group {
          source source;
        }
      }
      version version;
    }
    query-interval seconds;
    query-last-member-interval seconds;
    query-response-interval seconds;
    robust-count number;
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
  }
}

```

[edit protocols igmp-snooping] Hierarchy Level

```

protocols {
  igmp-snooping {
    traceoptions {
      file filename <files number> <no-stamp> <replace> <size maximum-file-size>
        <world-readable | no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
    vlan (all | vlan-name) {
      disable;
      immediate-leave;
      interface (all | interface-name) {
        multicast-router-interface;
        static {
          group multicast-ip-address;
        }
      }
      query-interval seconds;
      query-last-member-interval seconds;
      query-response-interval seconds;
      robust-count number;
    }
  }
}

```

[edit protocols ilmi] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  ilmi {
    traceoptions {
      file <filename> <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag;
      no-remote-trace;
    }
  }
}

```

[edit protocols isis] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  isis {
    disable;
    clns-routing;
    export [ policy-names ];
    graceful-restart {
      disable;
      helper-disable;
      restart-duration seconds;
    }
    ignore-attached-bit;
    interface interface-name {
      ... interface-configuration ...
    }
    label-switched-path name level level metric metric;
    level (1 | 2) {
      disable;
      authentication-key key;
      authentication-type authentication;
      external-preference preference;
      no-csnp-authentication;
      no-hello-authentication;
      no-psnp-authentication;
      preference preference;
      prefix-export-limit number;
      wide-metrics-only;
    }
    loose-authentication-check;
    lsp-lifetime seconds;
    max-areas number;
    no-adjacency-holddown;
    no-authentication-check;
    no-ipv4-routing;
    no-ipv6-routing;
    overload {
      advertise-high-metrics;
      <timeout seconds>;
    }
    reference-bandwidth reference-bandwidth;
    rib-group {
      inet group-name;
      inet6 group-name;
    }
    spf-options
      delay milliseconds;
      holddown milliseconds;
      rapid-runs number;
  }
  topologies {
    ipv4-multicast;
  }
}

```

```

    ipv6-multicast;
    ipv6-unicast;
}
traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
traffic-engineering {
    disable;
    ignore-lsp-metrics;
    family inet {
        shortcuts {
            multicast-rpf-routes;
        }
    }
    family inet6 {
        shortcuts;
    }
}
interface interface-name {
    disable;
    bfd-liveness-detection {
        detection-time {
            threshold milliseconds;
        }
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
        }
        version (1 | automatic);
    }
    checksum;
    csnp-interval (seconds | disable);
    hello-padding (adaptive | loose | strict);
    ldp-synchronization {
        disable;
        hold-time seconds;
    }
    level (1 | 2) {
        disable;
        hello-authentication-key key;
        hello-authentication-type authentication;
        hello-interval seconds;
        hold-time seconds;
        ipv4-multicast-metric number;
        ipv6-multicast-metric number;
        ipv6-unicast-metric number;
        metric metric;
        passive;
        priority number;
        te-metric metric;
    }
}

```

```
    lsp-interval milliseconds;  
    mesh-group (value | blocked);  
    no-adjacency-down-notification;  
    no-ipv4-multicast;  
    no-ipv6-multicast;  
    no-ipv6-unicast;  
    no-unicast-topology;  
    passive;  
    point-to-point;  
  }  
}  
}
```

[edit protocols l2circuit] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  l2circuit {
    local-switching {
      interface interface-name {
        description text-description;
        end-interface {
          interface interface-name;
          protect-interface interface-name;
        }
        ignore-mtu-mismatch;
        protect-interface interface-name;
      }
    }
    neighbor address {
      interface interface-name {
        bandwidth {
          bps;
          ct0 bps;
          ct1 bps;
          ct2 bps;
          ct3 bps;
        }
        community community;
        (control-word | no-control-word);
        description text-description;
        ignore-encapsulation-mismatch;
        ignore-mtu-mismatch;
        mtu mtu;
        protect-interface interface-name;
        psn-tunnel-endpoint psn-tunnel-endpoint;
        virtual-circuit-id identifier;
      }
    }
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
  }
}

```

[edit protocols l2iw] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```
protocols {  
  l2iw {  
    traceoptions {  
      file filename <files number> <size maximum-file-size> <world-readable |  
        no-world-readable>;  
      flag flag <flag-modifier> <disable>;  
    }  
  }  
}
```


[edit protocols l2-learning] Hierarchy Level

```
protocols {  
  l2-learning {  
    global-mac-limit {  
      limit;  
      packet-action drop;  
    }  
    global-mac-statistics;  
    global-mac-table-aging-time seconds;  
    global-no-mac-learning;  
  }  
}
```

[edit protocols lacp] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```
protocols {  
  lacp {  
    traceoptions {  
      file <filename> <files number> <match regular-expression>  
        <size maximum-file-size> <world-readable | no-world-readable>;  
      flag flag;  
      no-remote-trace;  
    }  
  }  
}
```

[edit protocols layer2-control] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  layer2-control {
    mac-rewrite {
      interface interface-name {
        protocol {
          cdp;
          stp;
          vtp;
        }
      }
    }
  }
  nonstop-bridging;
  traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
      no-world-readable>;
    flag flag <disable>;
  }
}

```

[edit protocols ldp] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  ldp {
    (deaggregate | no-deaggregate);
    egress-policy [ policy-names ];
    explicit-null;
    export [ policy-names ];
    graceful-restart {
      disable;
      helper-disable;
      maximum-neighbor-reconnect-time seconds;
      maximum-neighbor-recovery-time seconds;
      reconnect-time seconds;
      recovery-time seconds;
    }
    import [ policy-names ];
    interface interface-name {
      disable;
      hello-interval seconds;
      hold-time seconds;
      transport-address (interface | router-id);
    }
    keepalive-interval seconds;
    keepalive-timeout seconds;
    l2-smart-policy;
    log-updown {
      trap disable;
    }
    next-hop {
      merged {
        policy [ policy-names ];
      }
    }
    no-forwarding;
    oam {
      ... oam-configuration ...
    }
    policing {
      fec class-address {
        ingress-traffic filter-name;
        transit-traffic filter-name;
      }
    }
    preference preference;
    session destination-address {
      authentication-algorithm algorithm;
      authentication-key key;
      authentication-key-chain key-chain;
    }
    session-protection <timeout seconds>;
    strict-targeted-hellos;
  }
}

```

```

traceoptions {
  file filename <files number> <size maximum-file-size> <world-readable |
    no-world-readable>;
  flag flag <flag-modifier> <disable>;
}
track-igp-metric;
traffic-statistics {
  file filename <files number> <size maximum-file-size> <world-readable |
    no-world-readable>;
  interval seconds;
  no-penultimate-hop;
}
transport-address (address | interface | router-id);
oam {
  bfd-liveness-detection {
    detection-time {
      threshold milliseconds;
    }
    ecmp;
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    multiplier number;
    no-adaptation;
    transmit-interval {
      minimum-interval milliseconds;
      threshold milliseconds;
    }
    version (1 | automatic);
  }
  fec class-address {
    bfd-liveness-detection {
      detection-time {
        threshold milliseconds;
      }
      ecmp;
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      version (1 | automatic);
    }
  }
  no-bfd-liveness-detection;
  periodic-traceroute {
    disable;
    exp cos-value;
    fanout next-hops;
    frequency minutes;
    paths number;
    retries number;
    source address;
    ttl number;
    wait seconds;
  }
}

```

```
    }  
  }  
  periodic-traceroute {  
    disable;  
    exp cos-value;  
    fanout next-hops;  
    frequency minutes;  
    paths number;  
    retries number;  
    source address;  
    ttl number;  
    wait seconds;  
  }  
}  
}
```

[edit protocols link-management] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  link-management {
    peer peer-name {
      address address;
      control-channel [ control-channel-interfaces ];
      lmp-control-channel interface-name {
        remote-address address;
      }
      lmp-protocol {
        hello-dead-interval milliseconds;
        hello-interval milliseconds;
        passive;
        retransmission-interval milliseconds;
        retry-limit number;
      }
      te-link [ te-link-names ];
    }
    te-link te-link-name {
      disable;
      interface interface-name {
        disable;
        local-address address;
        remote-address address;
        remote-id id-number;
      }
      label-switched-path lsp-name {
        disable;
        local-address address;
        remote-address address;
        remote-id id-number;
      }
      local-address address;
      remote-address address;
      remote-id id-number;
      te-metric metric;
    }
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag;
    }
  }
}

```

[edit protocols lldp] Hierarchy Level

```

protocols {
  lldp {
    disable;
    advertisement-interval seconds;
    hold-multiplier seconds;
    interface (all | interface-name) {
      disable;
    }
    lldp-configuration-notification-interval seconds;
    ptopo-configuration-maximum-hold-time seconds;
    ptopo-configuration-trap-interval seconds;
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <disable>;
    }
    transmit-delay seconds;
  }
}

```


[edit protocols lldp-med] Hierarchy Level

```

protocols {
  lldp-med {
    disable;
    fast-start number;
    interface (all | interface-name) {
      disable;
      location {
        civic-based {
          ca-type {
            index {
              ca-value value;
            }
          }
          country-code two-letter-code;
          what value;
        }
        elin number;
      }
    }
  }
}

```

[edit protocols mld] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  mld {
    interface interface-name {
      disable;
      immediate-leave;
      ssm-map ssm-map-name;
      static {
        group group-address {
          source source-address;
        }
      }
      version (1 | 2);
    }
    query-interval seconds;
    query-last-member-interval seconds;
    query-response-interval seconds;
    robust-count number;
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
  }
}

```

[edit protocols mpls] Hierarchy Level

Several statements in the [edit protocols mpls] hierarchy are valid at numerous locations within the hierarchy. To make the complete hierarchy easier to read, the repeated statements are listed in “Common MPLS Options” on page 151 and that section is referenced at the appropriate locations in “Complete [edit protocols mpls] Hierarchy” on page 152.

Common MPLS Options

This section lists statements that are valid at all of the following hierarchy levels, and is referenced at those levels in “Complete [edit protocols mpls] Hierarchy” on page 152 instead of the statements being repeated.

- [edit protocols mpls]
- [edit protocols mpls label-switched-path *lsp-name*]
- [edit protocols mpls label-switched-path *lsp-name* primary *path-name*]
- [edit protocols mpls label-switched-path *lsp-name* secondary *path-name*]

The common MPLS options are as follows:

```

admin-down;
admin-group {
    exclude [ group-names ];
    include-all [ group-names ];
    include-any [ group-names ];
}
bandwidth {
    bps;
    ct0 bps;
    ct1 bps;
    ct2 bps;
    ct3 bps;
}
class-of-service cos-value;
hop-limit number;
no-cspf;
no-decrement-ttl;
oam {
    ... oam-configuration ...
}
optimize-timer seconds;
preference preference;
priority setup-priority hold-priority;
(record | no-record);
standby;
oam {
    bfd-liveness-detection {
        detection-time threshold milliseconds;
        failure-action teardown;
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
    }
}

```

```

    multiplier detection-time-multiplier;
    no-adaptation;
    transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
    }
    version bfd-version;
}
traceoptions {
    file <filename> <files number> <match regular-expression>
    <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
}

```

Complete [edit protocols mpls] Hierarchy

The statement hierarchy listed in this section can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
    mpls {
        ... statements listed in Common MPLS Options PLUS the following ...
        disable;
        admin-groups {
            group-name group-value;
        }
        advertise-hold-time seconds;
        auto-policing {
            class all (drop | loss-priority-high | loss-priority-low);
            class ctnumber (drop | loss-priority-high | loss-priority-low);
        }
        diffserv-te {
            bandwidth-model (extended-mam | mam | rdm);
            te-class-matrix {
                tnumber traffic-class cnumber priority priority;
            }
        }
        expand-loose-hop;
        explicit-null;
        icmp-tunneling;
        interface (interface-name | all) {
            disable;
            admin-group [ group-names ];
            label-map (in-label | default-route) {
                class-of-service value;
                (discard | next-hop (address | hostname | interface-name) | reject);
                (pop | swap out-label);
                preference preference;
                swap-push swap-label push-label;
            }
        }
        ipv6-tunneling;
        label-switched-path lsp-name {

```

```

... label-switched-path-configuration ...
}
log-updown {
  no-trap {
    mpls-lsp-traps;
    rfc3812-traps;
  }
  (syslog | no-syslog);
  trap;
  trap-path-down;
  trap-path-up;
}
no-propagate-ttl;
optimize-aggressive;
path path-name {
  address <loose | strict>;
}
path-mtu {
  allow-fragmentation;
  rsvp {
    mtu-signaling;
  }
}
revert-timer seconds;
rsvp-error-hold-time seconds;
smart-optimize-timer seconds;
static-path inet {
  (prefix | default) {
    class-of-service value;
    double-push bottom-label top-label;
    next-hop (address | interface-name | address/interface-name);
    push out-label;
    preference preference;
    triple-push bottom-label middle-label top-label;
  }
}
statistics {
  auto-bandwidth;
  file filename <files number> <size maximum-file-size> <world-readable |
    no-world-readable>;
  interval seconds;
}
traceoptions {
  file filename <files number> <size maximum-file-size> <world-readable |
    no-world-readable>;
  flag flag;
}
traffic-engineering (bgp | bgp-igp | bgp-igp-both-ribs | mpls-forwarding);
label-switched-path lsp-name {
  ... statements listed in Common MPLS Options PLUS the following ...
  disable;
  adaptive;
  admin-groups {
    group-name group-value;
  }
  associate-backup-pe-groups;
}

```

```

auto-bandwidth {
    adjust-interval seconds;
    adjust-threshold percent;
    adjust-threshold-overflow-limit count;
    maximum-bandwidth bps;
    minimum-bandwidth bps;
    monitor-bandwidth;
}
description description;
fast-reroute {
    bandwidth bps;
    bandwidth-percent percent;
    (exclude [ group-names ] | no-exclude);
    hop-limit number;
    (include-all [ group-names ] | no-include-all);
    (include-any [ group-names ] | no-include-any);
}
from address;
install destination-prefix</prefix-length> <active>;
ldp-tunneling;
(least-fill | most-fill | random);
link-protection;
lsp-attributes {
    encoding-type (ethernet | packet | pdh | sonet-sdh);
    gp-id (ethernet | hdlc | ipv4 | pos-no-scrambling-crc-16 |
        pos-no-scrambling-crc-32 | pos-scrambling-crc-16 | pos-scrambling-crc-32 |
        ppp);
    signal-bandwidth type;
    switching-type (fiber | lambda | psc-1 | tdm);
}
metric number;
no-install-to-address;
node-link-protection;
p2mp lsp-name;
policing {
    filter filter-name;
    no-automatic-policing;
}
primary path-name {
    ... statements listed in Common MPLS Options PLUS the following ...
    adaptive;
    select (manual | unconditional);
}
retry-limit number;
retry-timer seconds;
revert-timer seconds;
secondary path-name {
    ... statements listed in Common MPLS Options PLUS the following ...
    adaptive;
    select (manual | unconditional);
}
soft-preemption;
template;
to address;
traceoptions {

```

```
file filename <files number> <size maximum-file-size> <world-readable |  
    no-world-readable>;  
flag flag;  
    }  
  }  
}
```

[edit protocols msdp] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  msdp {
    disable;
    active-source-limit {
      maximum number;
      threshold number;
    }
    data-encapsulation (disable | enable);
    export [ policy-names ];
    group group-name {
      ... group-configuration ...
    }
    import [ policy-names ];
    local address address;
    peer address {
      ... peer-configuration ...
    }
    rib-group group-name;
    source ip-prefix</prefix-length>;
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
    group group-name {
      disable;
      export [ policy-names ];
      import [ policy-names ];
      local-address address;
      mode (mesh-group | standard);
      peer address {
        ... same statements as at the [edit protocols msdp peer address] hierarchy
          level shown just below ...
      }
      traceoptions {
        file filename <files number> <size maximum-file-size> <world-readable |
          no-world-readable>;
        flag flag <flag-modifier> <disable>;
      }
    }
    peer address {
      disable;
      active-source-limit {
        maximum number;
        threshold number;
      }
      authentication-key peer-key;
      default-peer;
      export [ policy-names ];
      import [ policy-names ];
    }
  }
}

```



```

local-address address;
traceoptions {
  file filename <files number> <size maximum-file-size> <world-readable |
    no-world-readable>;
  flag flag <flag-modifier> <disable>;
}
}
}

```

[edit protocols mstp] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  mstp {
    disable;
    bpdu-block-on-edge;
    bpdu-destination-mac-address provider-bridge-group;
    bridge-priority priorityk;
    configuration-name configuration-name;
    forward-delay seconds;
    hello-time seconds;
    interface interface-name {
      bpdu-timeout-action {
        alarm;
        block;
      }
      cost cost;
      edge;
      mode (point-to-point | shared);
      no-root-port;
      priority interface-priority;
    }
    max-age seconds;
    max-hops hops;
    msti identifier {
      bridge-priority priority;
      interface interface-name {
        cost cost;
        priority interface-priority;
      }
      vlan [ vlan-ids ];
    }
    revision-level revision-level;
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <disable>;
    }
  }
}

```

[edit protocols neighbor-discovery] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  neighbor-discovery {
    secure {
      cryptographic-address {
        key-length bytes;
        key-pair pathname;
      }
      security-level {
        (default | secure-messages-only);
      }
      timestamp {
        clock-drift number;
        known-peer-window seconds;
        new-peer-window seconds;
      }
      traceoptions {
        file <filename> <files number> <match regular-expression>
          <size maximum-file-size> <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
      }
    }
  }
}

```

[edit protocols oam] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  oam {
    ethernet {
      connectivity-fault-management {
        action-profile profile-name {
          default-actions {
            interface-down;
          }
        }
      }
      linktrace {
        age (10s | 30s | 1m | 10m | 30m);
        path-database-size number;
      }
      maintenance-domain domain-name {
        level number;
        name-format (character-string | dns | mac+2oct | none);
        maintenance-association association-name {
          continuity-check {
            hold-interval minutes;
            interval (100ms | 1s | 10s | 1m | 10m);
            loss-threshold number;
          }
          mep mep-id {
            auto-discovery;
            direction (up | down);
            interface interface-name;
            priority number;
            remote-mep mep-id {
              action-profile profile-name;
            }
          }
          short-name-format (2octet | character-string | rfc-2685-vpn-id | vlan);
        }
      }
    }
    traceoptions {
      file <filename> <files number> <match regular-expression>
        <size maximum-file-size> <world-readable | no-world-readable>;
      flag flag;
      no-remote-trace;
    }
  }
  link-fault-management {
    action-profile profile-name {
      action {
        link-down;
        send-critical-event;
        syslog;
      }
      event {
        link-adjacency-loss;
      }
    }
  }
}

```

```

        link-event-rate {
            frame-error count;
            frame-period count;
            frame-period-summary count;
            symbol-period count;
        }
    protocol-down;
}

interface interface-name {
    apply-action-profile profile-name;
    event-thresholds {
        frame-error count;
        frame-period count;
        frame-period-summary count;
        symbol-period count;
    }
    link-discovery (active | passive);
    negotiation-options {
        allow-remote-loopback;
        no-allow-link-events;
    }
    pdu-interval interval;
    pdu-threshold threshold-value;
    remote-loopback;
}
traceoptions {
    file <filename> <files number> <match regular-expression>
        <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
}
}
}
```

[edit protocols ospf] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  ospf {
    disable;
    area area-id {
      ... area-configuration ...
    }
    export [ policy-names ];
    external-preference preference;
    graceful-restart {
      disable;
      helper-disable;
      notify-duration seconds;
      rest-duration seconds;
    }
    import [ policy-names ];
    no-neighbor-down-notification;
    no-nssa-abr;
    no-rfc-1583;
    overload {
      <timeout seconds>;
    }
    preference preference;
    prefix-export-limit number;
    reference-bandwidth reference-bandwidth;
    rib-group group-name;
    route-type-community (vendor | iana);
    spf-options {
      delay milliseconds;
      holddown milliseconds;
      rapid-runs number;
    }
    topology (default | ipv4-multicast | name) {
      topology-id number;
      overload;
      prefix-export-limit number;
      spf-options {
        delay milliseconds;
        holddown milliseconds;
        rapid-runs number;
      }
    }
  }
  traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
      no-world-readable>;
    flag flag <flag-modifier> <disable>;
  }
  traffic-engineering {
    advertise-unnumbered-interfaces;
    multicast-rpf-routes;
    no-topology;
  }
}

```

```

shortcuts {
    ignore-lsp-metrics;
    lsp-metric-into-summary;
}
}
area area-id {
    area-range ip-prefix</prefix-length> <exact> <override-metric metric> <restrict>;
    interface interface-name {
        ... interface-configuration ...
    }
    label-switched-path name {
        disable;
        metric metric;
        topology (name | default | ipv4-multicast) {
            disable;
            metric metric;
        }
    }
}
nssa {
    area-range ip-prefix</prefix-length> <exact> <override-metric metric>
        <restrict>;
    default-lsa {
        default-metric metric;
        metric-type type;
        type-7;
    }
    (no-summaries | summaries);
}
peer-interface interface-name {
    disable;
    authentication {
        md5 key-id key key-string <start-time YYYY-MM-DD.hh:mm>;
        simple-password key-string;
    }
    dead-interval seconds;
    demand-circuit;
    hello-interval seconds;
    no-neighbor-down-notification;
    retransmit-interval seconds;
    transit-delay seconds;
}
sham-link-remote address {
    demand-circuit;
    ipsec-sa sa-name;
    metric metric;
    topology (name | default | ipv4-multicast) {
        disable;
        metric metric;
    }
}
stub <default-metric metric> <no-summaries | summaries>;
virtual-link neighbor-id router-id transit-area area-id {
    disable;
    authentication {
        md5 key-id key key-string <start-time YYYY-MM-DD.hh:mm>;
        simple-password key-string;
    }
}

```

```

    }
    dead-interval seconds;
    demand-circuit;
    hello-interval seconds;
    ipsec-sa sa-name;
    no-neighbor-down-notification;
    retransmit-interval seconds;
    topology (name | default | ipv4-multicast) {
        disable;
        metric metric;
    }
    transit-delay seconds;
}
interface interface-name {
    disable;
    authentication {
        md5 key-id key key-string <start-time YYYY-MM-DD.hh:mm>;
        simple-password key-string;
    }
    bfd-liveness-detection {
        detection-time {
            threshold milliseconds;
        }
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
        }
        version (1 | automatic);
    }
    dead-interval seconds;
    demand-circuit;
    dynamic-neighbors;
    hello-interval seconds;
    interface-type type;
    ipsec-sa sa-name;
    ldp-synchronization {
        disable;
        hold-time seconds;
    }
    metric metric;
    neighbor address <eligible>;
    network-summary-export [ policy-names ];
    network-summary-import [ policy-names ];
    no-neighbor-down-notification;
    passive {
        traffic-engineering {
            remote-node-id address;
        }
    }
    poll-interval seconds;
    priority number;
    retransmit-interval seconds;
}

```



```

te-metric metric;
topology (name | default | ipv4-multicast) {
  disable;
  metric metric;
}
transit-delay seconds;
}
}
}
}

```

[edit protocols ospf3] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  ospf3 {
    disable;
    area area-id {
      ... area-configuration ...
    }
    export [ policy-names ];
    external-preference preference;
    graceful-restart {
      disable;
      helper-disable;
      no-strict-lsa-checking;
      notify-duration seconds;
      restart-duration seconds;
    }
    import [ policy-names ];
    no-nssa-abr;
    no-rfc-1583;
    overload <timeout seconds>;
    preference preference;
    prefix-export-limit number;
    realm (ipv4-multicast | ipv4-unicast | ipv6-multicast);
    reference-bandwidth reference-bandwidth;
    rib-group group-name;
    spf-options {
      delay milliseconds;
      holddown milliseconds;
      rapid-runs number;
    }
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
    traffic-engineering {
      ignore-lsp-metrics;
      shortcuts {
        lsp-metric-into-summary;
      }
    }
  }
  area area-id {
    area-range ip-prefix</prefix-length> <exact> <override-metric metric> <restrict>;
    interface interface-name {
      ... interface-configuration ...
    }
    inter-area-prefix-export [ policy-names ];
    inter-area-prefix-import [ policy-names ];
    nssa {
      area-range ip-prefix</prefix-length> <exact> <override-metric metric>
        <restrict>;
    }
  }
}

```

```

    default-lsa {
        default-metric metric;
        metric-type type;
        type-7;
    }
    (summaries | no-summaries);
}
stub <default-metric metric> <no-summaries | summaries>;
virtual-link neighbor-id router-id transit-area area-id {
    disable;
    dead-interval seconds;
    hello-interval seconds;
    ipsec-sa name;
    retransmit-interval seconds;
    transit-delay seconds;
}
interface interface-name {
    bfd-liveness-detection {
        detection-time {
            threshold milliseconds;
        }
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
        }
        version (1 | automatic);
    }
    disable;
    dead-interval seconds;
    demand-circuit;
    dynamic-neighbors;
    hello-interval seconds;
    interface-type p2p;
    ipsec-sa name;
    metric metric;
    neighbor address <eligible>;
    passive {
        traffic-engineering {
            remote-node-id address;
        }
    }
    priority number;
    retransmit-interval seconds;
    transit-delay seconds;
}
}
}
}

```

[edit protocols *pgm*] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```
protocols {  
  pgm {  
    traceoptions {  
      flag flag <flag-modifier> <disable>;  
    }  
  }  
}
```

[edit protocols pim] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  pim {
    disable;
    assert-timeout seconds;
    dense-groups {
      address <announce | reject>;
    }
    graceful-restart {
      disable;
      restart-duration seconds;
    }
    import [ policy-names ];
    interface interface-name {
      disable;
      bfd-liveness-detection {
        detection-time {
          threshold milliseconds;
        }
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
      }
      version (1 | automatic);
    }
    hello-interval seconds;
    neighbor-policy [ policy-names ];
    mode (dense | sparse | sparse-dense);
    priority number;
    version version;
  }
  join-load-balance;
  rib-group {
    inet group-name;
    inet6 group-name;
  }
  rp {
    ... rp-configuration ...
  }
  spt-threshold {
    infinity [ policy-names ];
  }
  traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
      no-world-readable>;
    flag flag <flag-modifier> <disable>;
  }
}

```

```

    flag (route | state) <flag-modifier> <disable> <filter <match-on prefix>
      <policy [ policy-names ]>;
  }
rp {
  auto-rp {
    (announce | discovery | mapping);
    (mapping-agent-election | no-mapping-agent-election);
  }
  bootstrap {
    family (inet | inet6) {
      export [ policy-names ];
      import [ policy-names ];
      priority number;
    }
  }
  bootstrap-export [ policy-names ];
  bootstrap-import [ policy-names ];
  bootstrap-priority number;
  dr-register-policy [ policy-names ];
  embedded-rp {
    group-ranges {
      ip-prefix</prefix-length>;
    }
    maximum-rps limit;
  }
  local {
    ... local-configuration ...
  }
  rp-register-policy [ policy-names ];
  static {
    address address {
      group-ranges {
        ip-prefix</prefix-length>;
      }
      version (1 | 2);
    }
  }
  local {
    disable;
    address address;
    family {
      ... family-configuration ...
    }
    group-ranges {
      ip-prefix</prefix-length>;
    }
    hold-time seconds;
    priority number;
    family (inet | inet6) {
      disable;
      address address;
      anycast-pim {
        local-address address;
        rp-set {
          address address <forward-msdp-sa>;
        }
      }
    }
  }
}

```

```
    }  
    group-ranges {  
        destination-mask;  
    }  
    hold-time seconds;  
    priority number;  
  }  
}  
}
```

[edit protocols ppp] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```
protocols {  
  ppp {  
    monitor-session (interface-name | all);  
    traceoptions {  
      file <filename> <files number> <match regular-expression>  
        <size maximum-file-size> <world-readable | no-world-readable>;  
      flag flag;  
      level severity;  
      no-remote-trace;  
    }  
  }  
}
```


[edit protocols protection-group] Hierarchy Level

```

protocols {
  protection-group {
    ethernet-ring ring-name {
      east-interface {
        control-channel {
          interface-name;
          vlan vlan-id;
        }
        ring-protection-link-end;
      }
      guard-interval milliseconds;
      hold-interval milliseconds;
      node-id node-id;
      restore-interval minutes;
      ring-protection-link-owner;
      west-interface {
        control-channel {
          interface-name;
          vlan vlan-id;
        }
        ring-protection-link-end;
      }
    }
  }
}

```

[edit protocols rip] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  rip {
    authentication-key password;
    authentication-type type;
    (check-zero | no-check-zero);
    graceful-restart {
      disable;
      restart-time seconds;
    }
    group group-name {
      ... group-configuration ...
    }
    holddown seconds;
    import [ policy-names ];
    message-size number;
    metric-in metric;
    receive (both | none | version-1 | version-2);
    rib-group group-name;
    route-timeout seconds;
    send (broadcast | multicast | none | version-1);
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
    update-interval seconds;
    group group-name {
      bfd-liveness-detection {
        detection-time {
          threshold milliseconds;
        }
        minimum-interval milliseconds;
        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
          minimum-interval milliseconds;
          threshold milliseconds;
        }
        version (1 | automatic);
      }
      export [ policy-names ];
      import [ policy-names ];
      metric-out metric;
      neighbor neighbor-name {
        ...neighbor-configuration ...
      }
      preference preference;
      route-timeout seconds;
      update-interval seconds;
    }
  }
}

```

```

neighbor interface-name {
  any-sender;
  authentication-key password;
  authentication-type type;
  bfd-liveness-detection {
    detection-time {
      threshold milliseconds;
    }
    minimum-interval milliseconds;
    minimum-receive-interval milliseconds;
    multiplier number;
    no-adaptation;
    transmit-interval {
      minimum-interval milliseconds;
      threshold milliseconds;
    }
    version (1 | automatic);
  }
  (check-zero | no-check-zero);
  import [ policy-names ];
  message-size number;
  metric-in metric;
  receive (both | none | version-1 | version-2);
  route-timeout seconds;
  send (broadcast | multicast | none | version-1);
  update-interval seconds;
}
}
}
}

```

[edit protocols ripng] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  ripng {
    graceful-restart {
      disable;
      restart-time seconds;
    }
    group group-name {
      ...group-configuration ...
    }
    holddown seconds;
    import [ policy-names ];
    metric-in metric;
    receive <none>;
    route-timeout seconds;
    send <none>;
    update-interval seconds;
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
    group group-name {
      export [ policy-names ];
      import [ policy-names ];
      metric-out metric;
      neighbor interface-name {
        import [ policy-names ];
        metric-in metric;
        receive <none>;
        route-timeout seconds;
        send <none>;
        update-interval seconds;
      }
      preference number;
      route-timeout seconds;
      update-interval seconds;
    }
  }
}

```

[edit protocols router-advertisement] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  router-advertisement {
    interface interface-name {
      current-hop-limit number;
      default-lifetime seconds;
      (managed-configuration | no-managed-configuration);
      max-advertisement-interval seconds;
      min-advertisement-interval seconds;
      (other-stateful-configuration | no-other-stateful-configuration);
      prefix prefix {
        (autonomous | no-autonomous);
        (on-link | no-on-link);
        preferred-lifetime seconds;
        valid-lifetime seconds;
      }
      reachable-time milliseconds;
      retransmit-timer milliseconds;
    }
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag;
    }
  }
}

```

[edit protocols router-discovery] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  router-discovery {
    disable;
    address address {
      (advertise | ignore);
      (broadcast | multicast);
      ( ineligible | priority number);
    }
    interface interface-name {
      lifetime seconds;
      min-advertisement-interval seconds;
      max-advertisement-interval seconds;
    }
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag;
    }
  }
}

```

[edit protocols rstp] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  rstp {
    disable;
    bpdu-block-on-edge;
    bpdu-destination-mac-address provider-bridge-group;
    bridge-priority priority;
    extended-system-id id;
    force-version;
    forward-delay seconds;
    hello-time seconds;
    interface interface-name {
      bpdu-timeout-action {
        alarm;
        block;
      }
      cost cost;
      edge;
      mode (point-to-point | shared);
      no-root-port;
      priority interface-priority;
    }
    max-age seconds;
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <disable>;
    }
  }
}

```

[edit protocols rsvp] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  rsvp {
    disable;
    fast-reroute optimize-timer seconds;
    graceful-deletion-timeout seconds;
    graceful-restart {
      disable;
      helper-disable;
      maximum-helper-recovery-time seconds;
      maximum-helper-restart-time seconds;
    }
    interface interface-name {
      ... interface-configuration ...
    }
    keep-multiplier number;
    load-balance bandwidth;
    peer-interface peer-interface-name {
      disable;
      (aggregate | no-aggregate);
      authentication-key key;
      hello-interval seconds;
      (reliable | no-reliable);
    }
    preemption {
      (aggressive | disabled | normal);
      soft-preemption cleanup-timer seconds;
    }
    refresh-time seconds;
    traceoptions {
      file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
    tunnel-services {
      devices device-names;
    }
    interface interface-name {
      disable;
      (aggregate | no-aggregate);
      authentication-key key;
      bandwidth bps;
      hello-interval seconds;
      link-protection {
        ... link-protection-configuration ...
      }
      (reliable | no-reliable);
      subscription {
        percentage;
        ct0 percentage;
        ct1 percentage;
      }
    }
  }
}

```



```

        ct2 percentage;
        ct3 percentage;
    }
    update-threshold percentage;
    link-protection {
        disable;
        admin-group {
            exclude group-names;
            include-all group-names;
            include-any group-names;
        }
        bandwidth {
            bps;
            ct0 bps;
            ct1 bps;
            ct2 bps;
            ct3 bps;
        }
        bypass bypass-name {
            ... bypass-configuration ...
        }
        class-of-service cos-value;
        hop-limit number;
        max-bypasses number;
        no-cspf;
        no-node-protection;
        optimize-timer seconds;
        path address <strict | loose>;
        priority setup-priority reservation-priority;
        subscription percentage;
        bypass bypass-name {
            admin-group {
                exclude group-names;
                include-all group-names;
                include-any group-names;
            }
            bandwidth {
                bps;
                ct0 bps;
                ct1 bps;
                ct2 bps;
                ct3 bps;
            }
            class-of-service cos-value;
            hop-limit number;
            no-cspf;
            path address <strict | loose>;
            priority setup-priority reservation-priority;
            to address;
        }
    }
}
}
}
}
}

```

[edit protocols sap] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```
protocols {  
  sap {  
    disable;  
    listen address <port port>;  
  }  
}
```

[edit protocols sflow] Hierarchy Level

```
protocols {  
  sflow {  
    disable;  
    collector ip-address;  
    interfaces interface-name;  
    polling-interval seconds;  
    sample-limit packets;  
    sample-rate number;  
  }  
}
```

[edit protocols vrrp] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  vrrp {
    failover-delay milliseconds;
    startup-silent-period seconds;
    traceoptions {
      file <filename> <files number> <match regular-expression>
        <microsecond-stamp> <size maximum-file-size> <world-readable |
          no-world-readable>;
      flag flag;
      no-remote-trace;
    }
  }
}

```

[edit protocols vstp] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

protocols {
  vstp {
    disable;
    force-version stp;
    interface interface-name {
      bpdu-timeout-action {
        alarm;
        block;
      }
      cost cost;
      edge;
      mode (p2p | shared);
      no-root-port;
      priority interface-priority;
    }
    vlan vlan-id {
      bridge-priority priority;
      forward-delay seconds;
      hello-time seconds;
      interface interface-name {
        bpdu-timeout-action {
          alarm;
          block;
        }
        cost cost;
        edge;
        mode (point-to-point | shared);
        no-root-port;
        priority interface-priority;
      }
      max-age seconds;
      traceoptions {
        file filename <files number> <size maximum-file-size> <world-readable |
          no-world-readable>;
        flag flag <disable>;
      }
    }
  }
}

```

[edit routing-instances] Hierarchy Level

The following statement hierarchy can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```

routing-instances {
  routing-instance-name {
    access {
      address-assignment {
        ... same statements as listed in the address-assignment subhierarchy in [edit
        access] Hierarchy Level ...
      }
      access-profile profile-name;
      bridge-domains bridge-domain-name {
        ... same statements as listed in [edit bridge-domains] Hierarchy Level ...
      }
      description text;
      forwarding-options {
        ... same statements as listed in [edit forwarding-options] Hierarchy Level EXCEPT
        for the following ...
        hash-key {...} # NOT valid at this hierarchy level
      }
      instance-type (forwarding | l2vpn | layer2-control | no-forwarding | virtual-router |
        virtual-switch | vpls | vrf);
      interface interface-name;
      multicast-snooping-options {
        ... same statements as listed in [edit multicast-snooping-options] Hierarchy Level
        EXCEPT for the following ...
        traceoptions {...} # NOT valid at this hierarchy level
      }
      no-local-switching;
      no-vrf-advertise;
      protocols {
        ... protocols-configuration ...
      }
      provider-tunnel {
        ... provider-tunnel-configuration ...
      }
      route-distinguisher (as-number:number | ip-address:number);
      routing-interface interface-name;
      routing-options {
        ... routing-options-configuration ...
      }
      switch-options {
        ... same statements as listed in [edit switch-options] Hierarchy Level ...
      }
      system {
        services {
          dhcp-local-server {
            ... same statements as listed in the services dhcp-local-server subhierarchy
            in [edit system] Hierarchy Level...
          }
        }
      }
    }
    vlan-id (id | all | none);
  }
}

```

```

vlan-tags outer <tpid.>vlan-id inner <tpid.>vlan-id;
vrf-export [ policy-names ];
vrf-import [ policy-names ];
vrf-table-label;
vrf-target {
    target:community-identifier;
    export target:community-identifier;
    import target:community-identifier;
}
protocols {
    bgp {
        ... same statements as listed in [edit protocols bgp] Hierarchy Level EXCEPT
        the following ...
        group group-name {
            vpn-apply-export;    # NOT valid at this hierarchy level
        }
        neighbor address {
            group group-name {
                vpn-apply-export;    # NOT valid at this hierarchy level
            }
        }
        vpn-apply-export;    # NOT valid at this hierarchy level
    }
    esis {
        ... same statements as listed in [edit protocols esis] Hierarchy Level EXCEPT
        the following ...
        graceful-restart {...}    # NOT valid at this hierarchy level
    }
    igmp-snooping {
        ... igmp-snooping-configuration ...
    }
    isis {
        ... same statements as listed in [edit protocols isis] Hierarchy Level EXCEPT
        the following ...
        graceful-restart {...}    # NOT valid at this hierarchy level
        interface interface-name {
            level (1 | 2) {
                te-metric metric;    # NOT valid at this hierarchy level
            }
        }
        label-switched-path name level level metric metric;    # NOT valid at this
        hierarchy level
        traffic-engineering {...}    # NOT valid at this hierarchy level
    }
    l2vpn {
        ... l2vpn-configuration ...
    }
    ldp {
        ... same statements as listed in [edit protocols ldp] Hierarchy Level EXCEPT
        the following ...
        oam {...}    # NOT valid at this hierarchy level
    }
    msdp {
        ... same statements as listed in [edit protocols msdp] Hierarchy Level ...
    }
    mstp {

```

```

... same statements as listed in [edit protocols mstp] Hierarchy Level ...
}
mvpn {
  autodiscovery-only {
    intra-as {
      inclusive;
    }
  }
  receiver-site;
  route-target {
    export-target {
      target target-community;
      unicast;
    }
    import-target {
      target <target:number:number> <receiver | sender>;
      unicast <receiver | sender>;
    }
  }
  sender-site;
  traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
      no-world-readable>;
    flag flag <flag-modifier> <disable>;
  }
}
ospf {
  ... same statements as listed in [edit protocols ospf] Hierarchy Level PLUS
  the following ...
  domain-id (domain-id | disable);
  domain-vpn-tag number;
  route-type-community (iana | vendor);
  ... but NOT the following ...
  area area-id {
    interface interface-name {
      te-metric metric; # NOT valid at this hierarchy level
    }
    peer-interface {...} # NOT valid at this hierarchy level
  }
  traffic-engineering {...} # NOT valid at this hierarchy level
}
ospf3 {
  ... same statements as listed in [edit protocols ospf3] Hierarchy Level PLUS
  the following ...
  domain-id (domain-id | disable);
  domain-vpn-tag number;
  route-type-community (iana | vendor);
  ... but NOT the following ...
  traffic-engineering {...} # NOT valid at this hierarchy level
}
pim {
  ... same statements as listed in [edit protocols pim] Hierarchy Level PLUS the
  following ...
  mdt {
    group-range multicast-prefix;
    threshold {

```



```

        group group-address {
            source source-address {
                rate threshold-rate;
            }
        }
        tunnel-limit limit;
    }
}
mvpn {
    autodiscovery {
        inet-mdt;
    }
}
}
rip {
    ... same statements as listed in [edit protocols rip] Hierarchy Level ...
}
ripng {
    ... same statements as listed in [edit protocols ripng] Hierarchy Level ...
}
router-discovery {
    ... same statements as listed in [edit protocols router-discovery] Hierarchy
    Level ...
}
rstp {
    ... same statements as listed in [edit protocols rstp] Hierarchy Level ...
}
vpls {
    ... vpls-configuration ...
}
vstp {
    ... same statements as listed in [edit protocols vstp] Hierarchy Level ...
}
igmp-snooping {
    immediate-leave;
    interface interface-name {
        group-limit number;
        host-only-interface;
        immediate-leave;
        multicast-router-interface;
        static {
            group multicast-ip-address {
                source multicast-ip-address;
            }
        }
    }
}
proxy {
    source-address ip-address;
}
query-interval seconds;
query-last-member-interval seconds;
query-response-interval seconds;
robust-count number;
traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
    no-world-readable>;
}

```

```

    flag flag <flag-modifier> <disable>;
  }
  vlan vlan-id {
    ... same statements as at the [edit routing-instances routing-instance-name
        protocols igmp-snooping] hierarchy level EXCEPT the following ...
    traceoptions {...} # NOT valid at this hierarchy level
    vlan vlan-id {...} # NOT valid at this hierarchy level
  }
}
l2vpn {
  (control-word | no-control-word);
  encapsulation-type name;
  interface interface-name {
    description text-description;
    remote-site-id number;
  }
  site site-name {
    interface interface-name {
      description text-description;
      remote-site-id number;
    }
    site-identifier number;
    site-preference number;
  }
  traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
    flag flag <flag-modifier> <disable>;
  }
}
vpls {
  community name;
  connectivity-type (ce | irb);
  encapsulation-type (ethernet | ethernet-vlan);
  ignore-encapsulation-mismatch;
  ignore-mtu-mismatch;
  interface interface-name {
    interface-mac-limit {
      limit;
      packet-action drop;
    }
    no-mac-learning;
    static-mac mac-address {
      vlan-id number;
    }
  }
  interface-mac-limit {
    limit;
    packet-action drop;
  }
  mac-statistics;
  mac-table-aging-time seconds;
  mac-table-size {
    number-of-addresses;
    packet-action drop;
  }
}

```

```

mac-tlv-receive;
mac-tlv-send;
mesh-group group-name {
    ... mesh-group-configuration ...
}
mtu mtu-number;
neighbor address {
    associate-profile profile-name;
    backup-neighbor address {
        community name;
        psn-tunnel-endpoint address;
        standby;
    }
    community name;
    encapsulation-type (ethernet | ethernet-vlan);
    ignore-encapsulation-mismatch;
    psn-tunnel-endpoint address;
    switchover-delay seconds;
}
no-mac-learning;
no-tunnel-services;
site site-name {
    ... site-configuration ...
}
site-range number;
traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
tunnel-services {
    devices [ tunnel-interface-names ];
    primary tunnel-interface-name;
}
vpls-id vpls-id;
mesh-group group-name {
    associate-profile profile-name;
    interface interface-name;
    local-switching;
    mac-tlv-receive;
    mac-tlv-send;
    neighbor address {
        ... same statements as at the [edit routing-instances
            routing-instance-name protocols vpls neighbor address] hierarchy level
            shown just above ...
    }
}
peer-as {
    all;
}
vpls-id name;
}
site site-name {
    active-interface (any | primary interface-name);
    automatic-site-id {
        collision-detect-time seconds;
        new-site-wait-time seconds;
    }
}

```

```

        reclaim-wait-time minimum seconds maximum seconds;
        startup-wait-time seconds;
    }
    interface interface-name {
        ... same statements as at the [edit routing-instances
            routing-instance-name protocols vpls interface interface-name] hierarchy
            level shown above ...
    }
    mesh-group group-name;
    multi-homing;
    site-identifier number;
    site-preference number;
}
}
}
provider-tunnel {
    mdt {
        group-range multicast-prefix;
        threshold {
            group group-address {
                source source-address {
                    rate kbps;
                }
            }
        }
        tunnel-limit number;
    }
}
pim-asm {
    group-address address;
}
pim-ssm {
    group-address address;
}
rsvp-te {
    label-switched-path-template {
        (default-template | lsp-template-name);
    }
    static-lsp point-to-multipoint-lsp-name;
}
selective {
    group multicast-group-address-prefix {
        source address {
            rsvp-te {
                label-switched-path-template {
                    (default-template | lsp-template-name);
                }
                static-lsp point-to-multipoint-lsp-name;
            }
            threshold-rate kbps;
        }
    }
    tunnel-limit number;
}
}
routing-options {

```

```

... same statements as listed in [edit routing-options] Hierarchy Level PLUS the
  following ...
autonomous-system autonomous-system <independent-domain> <loops
  number>;
  multipath {
    vpn-unequal-cost <equal-external-internal>;
  }
... but NOT the following ...
confederation confederation-autonomous-system
  members autonomous-system; # NOT valid at this hierarchy level
dynamic-tunnels tunnel-name {...} # NOT valid at this hierarchy level
forwarding-table {
  export [ policy-names ]; # NOT valid at this hierarchy level
  (indirect-next-hop | no-indirect-next-hop); # NOT valid at this hierarchy
  level
}
med-igp-update-interval minutes; # NOT valid at this hierarchy level
nonstop-routing; # NOT valid at this hierarchy level
ppm {...} # NOT valid at this hierarchy level
resolution {
  tracefilter [ filter-names ]; # NOT valid at this hierarchy level
  traceoptions {...} # NOT valid at this hierarchy level
}
rib-groups {...} # NOT valid at this hierarchy level
route-distinguisher-id address; # NOT valid at this hierarchy level
route-record; # NOT valid at this hierarchy level
source-routing {...} # NOT valid at this hierarchy level
traceoptions {...} # NOT valid at this hierarchy level
}
}
}

```

[edit routing-options] Hierarchy Level

Several statements in the [edit routing-options] hierarchy are valid at numerous locations within the hierarchy. To make the complete hierarchy easier to read, the repeated statements are listed in “Common Routing Options” on page 194 and that section is referenced at the appropriate locations in “Complete [edit routing-options] Hierarchy” on page 194.

Common Routing Options

This section lists statements that are valid at all of the following hierarchy levels, and is referenced at those levels in “Complete [edit routing-options] Hierarchy” on page 194 instead of the statements being repeated.

- [edit routing-options aggregate defaults]
- [edit routing-options aggregate route *ip-prefix*</*prefix-length*>]
- [edit routing-options generate defaults]
- [edit routing-options generate route *ip-prefix*</*prefix-length*>]
- [edit routing-options static defaults]
- [edit routing-options static route *ip-prefix*</*prefix-length*>]

The common routing options are as follows:

```
(active | passive);
as-path {
    aggregator as-number address;
    atomic-aggregate;
    origin (egp | igp | incomplete);
    path path-identifier;
}
color metric <type metric-type>;
color2 metric <type metric-type>;
community [ no-advertise no-export no-export-subconfed ];
metric metric <type metric-type>;
metric2 metric <type metric-type>;
metric3 metric <type metric-type>;
metric4 metric <type metric-type>;
preference preference-value <type metric-type>;
preference2 preference-value <type metric-type>;
tag metric <type metric-type>;
tag2 metric <type metric-type>;
```

Complete [edit routing-options] Hierarchy

The statement hierarchy listed in this section can also be included at the [edit logical-systems *logical-system-name*] hierarchy level.

```
routing-options {
    aggregate {
        defaults {
```

```

... statements listed in Common Routing Options PLUS the following ...
(brief | full);
discard;
}
route ip-prefix</prefix-length> {
... statements listed in Common Routing Options PLUS the following ...
(brief | full);
discard;
policy [ policy-names ];
}
}
auto-export {
disable;
family {
inet {
disable;
flow {
disable;
rib-group rib-group;
}
multicast {
disable;
rib-group rib-group;
}
unicast {
disable;
rib-group rib-group;
}
}
}
inet6 {
disable;
multicast {
disable;
rib-group rib-group;
}
unicast {
disable;
rib-group rib-group;
}
}
}
iso {
disable;
unicast {
disable;
rib-group rib-group;
}
}
}
traceoptions {
file filename <files number> <size maximum-file-size> <world-readable |
no-world-readable>;
flag flag <flag-modifier> <disable>;
}
}
autonomous-system autonomous-system <loops number>;
bgp-orf-cisco-mode;

```

```

confederation as-number members [ as-numbers ];
dynamic-tunnels tunnel-name {
    destination-networks prefix;
    source-address address;
    tunnel-type tunnel-type;
}
fate-sharing {
    group group-name {
        cost value;
        from {
            address <to address>;
        }
    }
}
flow {
    route name {
        match {
            destination address;
            destination-port [ afs bgp biff bootpc bootps cmd cvspserver dhcp domain
                eklogin ekshell exec finger ftp ftp-data http https ident imap kerberos-sec
                klogin kpasswd krb-prop krbupdate kshell ldap ldp login mobileip-agent
                mobilip-mn msdp netbios-dgm netbios-ns netbios-ssn nfsd nntp ntalk ntp
                pop3 pptp printer radacct radius rip rkinit smtp snmp snmptrap snpp socks
                ssh sunrpc syslog tacacs tacacs-ds talk telnet tftp timed who xmcp ];
            dscp [ code-points ];
            fragment [ don't-fragment first-fragment is-fragment last-fragment
                not-a-fragment ];
            icmp-code [ communication-prohibited-by-filtering destination-host-prohibited
                destination-host-unknown fragmentation-needed host-precedence-violation
                host-unreachable host-unreachable-for-tos ip-header-bad
                network-unreachable network-unreachable-for-tos port-unreachable
                precedence-cutoff-in-effect protocol-unreachable redirect-for-host
                redirect-for-network redirect-for-tos-and-host redirect-for-tos-and-net
                required-option-missing source-host-isolated source-route-failed
                ttl-eq-zero-during-reassembly ttl-eq-zero-during-transit ];
            icmp-type [ echo-reply echo-request info-reply info-request mask-reply
                mask-request parameter-problem redirect router-advertisement router-solicit
                source-quench time-exceeded timestamp timestamp-reply unreachable ];
            packet-length [ values ];
            port [ ... same values as for the destination-port statement ... ];
            protocol [ ah egp esp gre icmp igmp ipip ospf pim rsvp sctp tcp udp ];
            source address;
            source-port [ ... same values as for the destination-port statement ... ];
            tcp-flags [ ack fin push rst syn urgent ];
        }
        then {
            (accept | discard);
            community community-name;
            next-term;
            rate-limit value;
            routing-instance routing-instance-name;
            sample;
        }
    }
}
validation {
    traceoptions {

```



```

        file filename <files number> <size maximum-file-size> <world-readable |
            no-world-readable>;
        flag flag <flag-modifier> <disable>;
    }
}
forwarding-table {
    export [ policy-names ];
    (indirect-next-hop | no-indirect-next-hop);
    unicast-reverse-path (active-paths | feasible-paths);
}
generate {
    defaults {
        ... statements listed in Common Routing Options PLUS the following ...
        (brief | full);
        discard;
    }
    route ip-prefix</prefix-length> {
        ... statements listed in Common Routing Options PLUS the following ...
        (brief | full);
        discard;
        policy [ policy-names ];
    }
}
graceful-restart {
    disable;
    restart-duration seconds;
}
instance-export [ policy-names ];
instance-import [ policy-names ];
interface-routes {
    family (inet | inet6) {
        export {
            lan;
            point-to-point;
        }
        import [ policy-names ];
    }
}
rib-group {
    inet group-name;
    inet6 group-name;
}
}
martians {
    ip-prefix</prefix-length> (exact | longer | orlonger |
        prefix-length-range /minimum-prefix-length-/maximum-prefix-length |
        through ip-prefix</prefix-length> | upto /prefix-length> <allow>;
}
maximum-paths path-limit <log-only | threshold value> <log-interval seconds>;
maximum-prefixes prefix-limit <log-only | threshold value> <log-interval seconds>;
med-igp-update-interval minutes;
multicast {
    ... multicast-configuration ...
}
nonstop-routing;
options {

```

```

    mark seconds;
    syslog {
        level level;
        upto level;
    }
}
ppm {
    no-delegate-processing;
}
resolution {
    rib routing-table-name {
        import [ policy-names ];
        resolution-ribs [ routing-table-names ];
    }
    tracefilter [ filter-policy-names ];
    traceoptions {
        file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
        flag flag <flag-modifier> <disable>;
    }
}
rib routing-table-name {
    aggregate {
        ... same statements as at the [edit routing-options aggregate] hierarchy level ...
    }
    generate {
        ... same statements as at the [edit routing-options generate] hierarchy level ...
    }
    martians {
        ip-prefix</prefix-length> (exact | longer | orlonger |
        prefix-length-range /minimum-prefix-length~/maximum-prefix-length |
        through ip-prefix</prefix-length> | upto /prefix-length) <allow>;
    }
    maximum-paths path-limit <log-only | threshold value> <log-interval seconds>;
    maximum-prefixes prefix-limit <log-only | threshold value> <log-interval seconds>;
    static {
        ... same statements as at the [edit routing-options static] hierarchy level ...
    }
}
rib-groups {
    group-name {
        export-rib table-name;
        import-policy [ policy-names ];
        import-rib [ table-names ];
    }
}
route-distinguisher-id address;
route-record;
router-id address;
source-routing {
    ip;
    ipv6;
}
static {
    ... static-configuration ...
}

```

```

topologies {
    family (inet | inet6) {
        topology topology-name;
    }
}
traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
    flag flag <disable>;
}
multicast {
    asm-override-ssm;
    backup-pe-group group-name {
        backups [ addresses ];
        local-address address;
    }
    flow-map flow-map-name {
        bandwidth <bps> <adaptive>;
        forwarding-cache {
            timeout (never | minutes);
        }
        policy [ policy-names ];
        redundant-sources [ addresses ];
    }
    forwarding-cache {
        threshold {
            reuse threshold-value;
            suppress threshold-value;
        }
        timeout minutes;
    }
    interface interface-name {
        maximum-bandwidth bps;
    }
    rpf-check-policy [ policy-names ];
    scope scope-name {
        interface [ interface-names ];
        prefix ip-prefix</prefix-length>;
    }
    scope-policy [ policy-names ];
    ssm-groups [ ip-prefix</prefix-length> ];
    ssm-map ssm-map-name {
        policy [ policy-names ];
        source [ addresses ];
    }
    traceoptions {
        file filename <files number> <size maximum-file-size> <world-readable |
            no-world-readable>;
        flag flag <disable>;
    }
}
static {
    defaults {
        ... statements listed in Common Routing Options PLUS the following ...
        (install | no-install);
        (readvertise | no-readvertise);
    }
}

```

```

        (resolve | no-resolve);
        (retain | no-retain);
    }
    rib-group group-name;
    route destination-prefix {
        ... statements listed in Common Routing Options PLUS the following ...
        backup-pe-group group-name;
        bfd-liveness-detection {
            ... bfd-liveness-detection-configuration ...
        }
        discard;
        (install | no-install);
        lsp-next-hop lsp-name {
            metric metric;
            preference preference-value;
        }
        (next-hop [ addresses ] | next-table address);
        p2mp-lsp-next-hop lsp-name {
            metric metric;
            preference preference-value;
        }
        (readvertise | no-readvertise);
        (receive | reject);
        (resolve | no-resolve);
        (retain | no-retain);
        bfd-liveness-detection {
            detection-time {
                threshold milliseconds;
            }
            holddown-interval milliseconds;
            local-address ip-address;
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            minimum-receive-ttl milliseconds;
            multiplier number;
            neighbor address;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            version (1 | automatic);
        }
    }
}
}
}

```

[edit schedulers] Hierarchy Level

```
schedulers {  
  scheduler scheduler-name {  
    start-date date-time stop-date date-time;  
    daily (all-day | exclude | start-time time stop-time time);  
    friday (all-day | exclude | start-time time stop-time time);  
    monday (all-day | exclude | start-time time stop-time time);  
    saturday (all-day | exclude | start-time time stop-time time);  
    sunday (all-day | exclude | start-time time stop-time time);  
    thursday (all-day | exclude | start-time time stop-time time);  
    tuesday (all-day | exclude | start-time time stop-time time);  
    wednesday (all-day | exclude | start-time time stop-time time);  
  }  
}
```

[edit security] Hierarchy Level

```

security {
  alg {
    dns {
      disable;
      traceoptions flag all <extensive>;
    }
    ftp {
      disable;
      traceoptions flag all <extensive>;
    }
    h323 {
      disable;
      application-screen {
        message-flood {
          gatekeeper threshold messages-per-second;
        }
        unknown-message {
          permit-nat-applied;
          permit-routed;
        }
      }
      endpoint-registration-timeout seconds;
      media-source-port-any;
      traceoptions {
        flag flag <flag-modifier>;
      }
    }
  }
  mgcp {
    disable;
    application-screen {
      connection-flood threshold requests-per-second;
      message-flood threshold messages-per-second;
      unknown-message {
        permit-nat-applied;
        permit-routed;
      }
    }
    inactive-media-timeout seconds;
    maximum-call-duration minutes;
    traceoptions {
      flag flag <extensive>;
    }
    transaction-timeout seconds;
  }
  msrpc {
    disable;
    traceoptions flag all <extensive>;
  }
  pptp {
    disable;
    traceoptions flag all <extensive>;
  }
  real {

```

```

        disable;
        traceoptions flag all <extensive>;
    }
    rsh {
        disable;
        traceoptions flag all <extensive>;
    }
    rtsp {
        disable;
        traceoptions flag all <extensive>;
    }
    sccp {
        disable;
        application-screen {
            call-flood threshold calls-per-second;
            unknown-message {
                permit-nat-applied;
                permit-routed;
            }
        }
        inactive-media-timeout seconds;
        traceoptions {
            flag flag <extensive>;
        }
    }
    sip {
        disable;
        application-screen {
            protect {
                deny {
                    all;
                    destination-ip {
                        address;
                    }
                }
                timeout seconds;
            }
        }
        unknown-message {
            permit-nat-applied;
            permit-routed;
        }
    }
    c-timeout minutes;
    disable-call-id-hiding;
    inactive-media-timeout seconds;
    maximum-call-duration minutes;
    retain-hold-resource;
    t1-interval milliseconds;
    t4-interval seconds;
    traceoptions {
        flag flag <flag-modifier>;
    }
}
sql {
    disable;
    traceoptions flag all <extensive>;

```

```

    }
    sunrpc {
        disable;
        traceoptions flag all <extensive>;
    }
    talk {
        disable;
        traceoptions flag all <extensive>;
    }
    tftp {
        disable;
        traceoptions flag all <extensive>;
    }
}
authentication-key-chains {
    key-chain key-chain-name {
        description text-description;
        key key-id {
            secret secret-data;
            start-time YYYY-MM-DD.hh:mm;
        }
        tolerance seconds;
    }
}
certificates {
    cache-size bytes;
    cache-timeout-negative seconds;
    certification-authority ca-profile-name {
        ca-name certificate-authority-name;
        crl filename;
        encoding (binary | pem);
        enrollment-url url-name;
        file certificate-filename;
        ldap-url url-name;
    }
    enrollment-retry number;
    local certificate-filename;
    maximum-certificates number;
    path-length bytes;
}
firewall-authentication {
    traceoptions {
        flag flag <flag-modifier>;
    }
}
flow {
    aging {
        early-ageout seconds;
        high-watermark percentage;
        low-watermark percentage;
    }
    allow-dns-reply;
    route-change-timeout seconds;
    syn-flood-protection-mode (syn-cookie | syn-proxy);
    tcp-mss {
        all-tcp {

```



```

        mss number;
    }
    gre-in {
        mss number;
    }
    gre-out {
        mss number;
    }
    ipsec-vpn {
        mss number;
    }
}
tcp-session {
    no-sequence-check;
    no-syn-check;
    no-syn-check-in-tunnel;
    rst-invalidate-session;
    rst-sequence-check;
    tcp-initial-timeout seconds;
}
traceoptions {
    file <filename> <files number> <match regular-expression>
        <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
    packet-filter filter-name {
        destination-port port-identifier;
        destination-prefix address;
        interface interface-name;
        protocol protocol-identifier;
        source-port port-identifier;
        source-prefix address;
    }
    rate-limit messages-per-second;
}
}
idp {
    active-policy policy-name;
    custom-attack {
        ... custom-attack-configuration ...
    }
    custom-attack-group group-name {
        group-members [ group-and-attack-names ];
    }
    dynamic-attack-group group-name {
        filters {
            category {
                values [ values ];
            }
        }
        direction {
            values [ any client-to-server exclude-any exclude-client-to-server
                exclude-server-to-client server-to-client ];
        }
        false-positives {
            values [ frequently occasionally rarely unknown ];
        }
    }
}

```

```

performance {
    values [ fast normal slow unknown ];
}
products {
    values [ values ];
}
recommended;
service {
    values [ values ];
}
severity {
    values [ critical info major minor warning ];
}
type {
    values [ anomaly signature ];
}
}
idp-policy policy-name {
    ... idp-policy-configuration ...
}
security-package {
    automatic {
        enable;
        interval hours;
        start-time MM-DD.hh:mm;
    }
    url url;
}
sensor-configuration {
    ... sensor-configuration-configuration ...
}
ssl-inspection {
    sessions number;
}
traceoptions {
    file <filename> <files number> <match regular-expression>
    <size maximum-file-size> <world-readable | no-world-readable>;
}
flag all;
level severity;
no-remote-trace;
}
custom-attack attack-name {
    attack-type {
        anomaly {
            direction (any | client-to-server | server-to-client);
            service service-name;
            shellcode (all | intel | no-shellcode | sparc);
            test test-condition;
        }
        chain {
            expression boolean-expression;
            member member-name {
                attack-type {
                    (anomaly | signature);
                }
            }
        }
    }
}

```

```

}
order;
protocol-binding {
  application application-name;
  icmp;
  ip {
    protocol-number transport-layer-protocol-number;
  }
  rpc {
    program-number rpc-program-number;
  }
  tcp {
    minimum-port port-number maximum-port port-number;
  }
  udp {
    minimum-port port-number maximum-port port-number;
  }
}
reset;
scope (session | transaction);
}
signature {
  context context-name;
  direction (any | client-to-server | server-to-client);
  negate;
  pattern signature-pattern;
  protocol {
    icmp {
      code {
        match (equal | greater-than | less-than | not-equal);
        value code-value;
      }
      data-length {
        match (equal | greater-than | less-than | not-equal);
        value data-length;
      }
      identification {
        match (equal | greater-than | less-than | not-equal);
        value identification-value;
      }
      sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number;
      }
      type {
        match (equal | greater-than | less-than | not-equal);
        value type-value;
      }
    }
  }
  ip {
    destination {
      match (equal | greater-than | less-than | not-equal);
      value hostname;
    }
    identification {
      match (equal | greater-than | less-than | not-equal);

```

```

        value identification-value;
    }
    ip-flags {
        (df | no-df);
        (mf | no-mf);
        (rb | no-rb);
    }
    protocol {
        match (equal | greater-than | less-than | not-equal);
        value transport-layer-protocol-id;
    }
    source {
        match (equal | greater-than | less-than | not-equal);
        value hostname;
    }
    tos {
        match (equal | greater-than | less-than | not-equal);
        value type-of-service-in-decimal;
    }
    total-length {
        match (equal | greater-than | less-than | not-equal);
        value length-of-ip-datagram;
    }
    ttl {
        match (equal | greater-than | less-than | not-equal);
        value time-to-live;
    }
}
tcp {
    ack-number {
        match (equal | greater-than | less-than | not-equal);
        value acknowledgment-number;
    }
    data-length {
        match (equal | greater-than | less-than | not-equal);
        value tcp-data-length;
    }
    destination-port {
        match (equal | greater-than | less-than | not-equal);
        value port-number;
    }
    header-length {
        match (equal | greater-than | less-than | not-equal);
        value header-length;
    }
    mss {
        match (equal | greater-than | less-than | not-equal);
        value maximum-segment-size;
    }
    option {
        match (equal | greater-than | less-than | not-equal);
        value tpc-option;
    }
    sequence-number {
        match (equal | greater-than | less-than | not-equal);
        value sequence-number;
    }
}

```

```

    }
    source-port {
        match (equal | greater-than | less-than | not-equal);
        value port-number;
    }
    tcp-flags {
        (ack | no-ack);
        (fin | no-fin);
        (psh | no-psh);
        (r1 | no-r1);
        (r2 | no-r2);
        (rst | no-rst);
        (syn | no-syn);
        (urg | no-urg);
    }
    urgent-pointer {
        match (equal | greater-than | less-than | not-equal);
        value urgent-pointer;
    }
    window-scale {
        match (equal | greater-than | less-than | not-equal);
        value window-scale-factor;
    }
    window-size {
        match (equal | greater-than | less-than | not-equal);
        value window-size;
    }
}
udp {
    data-length {
        match (equal | greater-than | less-than | not-equal);
        value udp-data-length;
    }
    destination-port {
        match (equal | greater-than | less-than | not-equal);
        value port-number;
    }
    source-port {
        match (equal | greater-than | less-than | not-equal);
        value port-number;
    }
}
}
protocol-binding {
    application application-name;
    icmp;
    ip {
        protocol-number transport-layer-protocol-number;
    }
    rpc {
        program-number rpc-program-number;
    }
    tcp {
        minimum-port port-number maximum-port port-number;
    }
    udp {

```

```

        minimum-port port-number maximum-port port-number;
    }
}
regex regular-expression;
shell-code (all | intel | no-shellcode | sparc);
}
recommended-action (close | close-client | close-server | drop | drop-packet |
    ignore | none);
severity (critical | info | major | minor | warning);
time-binding {
    count count-value;
    scope (destination | peer | source);
}
}
}
idp-policy policy-name {
    rulebase-exempt {
        rule rule-name {
            description text;
            match {
                attacks {
                    custom-attack-groups [ group-names ];
                    custom-attacks [ attack-names ];
                    dynamic-attack-groups [ group-names ];
                    predefined-attack-groups [ group-names ];
                    predefined-attacks [ attack-names ];
                }
                destination-address [ names ];
                destination-except [ names ];
                from-zone zone-name;
                source-address [ names ];
                source-except [ names ];
                to-zone zone-name;
            }
        }
    }
}
rulebase-ips {
    rule rule-name {
        description text;
        match {
            application application-name;
            attacks {
                custom-attack-groups [ group-names ];
                custom-attacks [ attack-names ];
                dynamic-attack-groups [ group-names ];
                predefined-attack-groups [ group-names ];
                predefined-attacks [ attack-names ];
            }
            destination-address [ addresses ];
            destination-except [ addresses ];
            from-zone zone-name;
            source-address [ addresses ];
            source-except [ addresses ];
            to-zone zone-name;
        }
    }
}
terminal;

```

```

    then {
        action {
            (close-client | close-client-and-server | close-server | drop-connection |
             drop-packet | ignore-connection | mark-diffserv value | no-action |
             recommended);
        }
        ip-action {
            (ip-block | ip-close | ip-notify);
            log;
            target (destination-address | service | source-address | source-zone |
                    zone-service);
            timeout seconds;
        }
        notification {
            log-attacks {
                alert;
            }
        }
        severity (critical | info | major | minor | warning);
    }
}
}
}
}
sensor-configuration {
    application-identification {
        disable;
        (application-system-cache | no-application-system-cache);
        application-system-cache-timeout value;
        max-packet-memory value;
        max-sessions value;
        max-tcp-session-packet-memory value;
        max-udp-session-packet-memory value;
    }
    detector {
        protocol-name protocol-name {
            tunable-name tunable-name {
                tunable-value value;
            }
        }
    }
}
}
flow {
    (allow-icmp-without-flow | no-allow-icmp-without-flow);
    fifo-max-size value;
    hash-table-size bytes;
    (log-errors | no-log-errors);
    max-timers-poll-ticks value;
    reject-timeout value;
    (reset-on-policy | no-reset-on-policy);
    udp-anticipated-timeout value;
}
global {
    (enable-all-qmodules | no-enable-all-qmodules);
    (enable-packet-pool | no-enable-packet-pool);
    memory-limit-percent percentage;
    (policy-lookup-cache | no-policy-lookup-cache);
}
}

```

```

ips {
  (detect-shellcode | no-detect-shellcode);
  fifo-max-size value;
  (ignore-regular-expression | no-ignore-regular-expression);
  log-supercede-min minimum-value;
  (pre-filter-shellcode | no-pre-filter-shellcode);
  (process-ignore-s2c | no-process-ignore-s2c);
  (process-override | no-process-override);
  process-port port-number;
}
log {
  cache-size size;
  suppression {
    disable;
    (include-destination-address | no-include-destination-address);
    max-logs-operate value;
    max-time-report value;
    start-log value;
  }
}
re-assembler {
  (ignore-memory-overflow | no-ignore-memory-overflow);
  ignore-reassembly-overflow;
  max-flow-mem value;
  max-packet-mem value;
}
}
ike {
  gateway gateway-name {
    address [ addresses-or-hostnames ];
    dead-peer-detection {
      always-send;
      interval seconds;
      threshold number;
    }
    dynamic {
      connections-limit number;
      distinguished-name {
        container container-name;
        wildcard wildcard;
      }
      hostname hostname;
      ike-user-type (group-ike-id | shared-ike-id);
      inet ipv4-address;
      user-at-hostname "email-address";
    }
    external-interface interface-name;
    ike-policy policy-name;
    local-identity (distinguished-name | hostname hostname | inet ipv4-address |
      user-at-hostname "email-address");
    nat-keepalive seconds;
    no-nat-traversal;
    xauth access-profile profile-name;
  }
  policy (address | policy-name) {

```



```

certificate {
    local-certificate certificate-identifier;
    peer-certificate-type (pkcs7 | x509-signature);
    trusted-ca (ca-index | use-all);
}
description policy-description;
encoding (binary | pem);
identity identity-name;
local-certificate certificate-filename;
local-key-pair private-public-key-file;
mode (aggressive | main);
pre-shared-key (ascii-text key | hexadecimal key);
proposal-set (basic | compatible | standard);
proposals [ proposal-names ];
}
proposal ike-proposal-name {
    authentication-algorithm (md5 | sha1 | sha-256);
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    description description;
    dh-group (group1 | group2 | group5);
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc |
        des-cbc);
    lifetime-seconds seconds;
}
respond-bad-spi number;
traceoptions {
    file <filename> <files number> <match regular-expression>
        <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
}
ipsec {
    policy ipsec-policy-name {
        description description;
        perfect-forward-secrecy {
            keys (group1 | group2 | group5);
        }
        proposal-set (basic | compatible | standard);
        proposals [ proposal-names ];
    }
    proposal ipsec-proposal-name {
        authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
        description description;
        encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc |
            des-cbc);
        lifetime-kilobytes kilobytes;
        lifetime-seconds seconds;
        protocol (ah | bundle | esp);
    }
    security-association sa-name {
        description description;
        dynamic {
            ipsec-policy policy-name;
            replay-window-size (32 | 64);
        }
    }
}

```

```

manual {
  direction (bidirectional | inbound | outbound) {
    authentication {
      algorithm (hmac-md5-96 | hmac-sha1-96);
      key (ascii-text key | hexadecimal key);
    }
    auxiliary-spi spi-index;
    encryption {
      encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc |
        aes-256-cbc | des-cbc);
      key (ascii-text key | hexadecimal key);
    }
    protocol (ah | bundle | esp);
    spi spi-index;
  }
}
mode (transport | tunnel);
}
traceoptions {
  flag flag;
}
vpn vpn-name {
  bind-interface interface-name;
  df-bit (clear | copy | set);
  establish-tunnels (immediately | on-traffic);
  ike {
    gateway gateway-name;
    idle-time seconds;
    install-interval seconds;
    ipsec-policy policy-name;
    no-anti-replay;
    proxy-identity {
      local ip-prefix</prefix-length>;
      remote ip-prefix</prefix-length>;
      service service-name;
    }
  }
}
manual {
  authentication {
    algorithm (hmac-md5-96 | hmac-sha1-96);
    key (ascii-text key | hexadecimal key);
  }
  encryption {
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc |
      des-cbc);
    key (ascii-text key | hexadecimal key);
  }
  external-interface interface-name;
  gateway address;
  protocol (ah | esp);
  spi spi-index;
}
vpn-monitor {
  destination-ip address;
  optimized;
  source-interface interface-name;
}

```

```

    }
    vpn-monitor-options {
        interval seconds;
        threshold failures;
    }
}
nat {
    destination {
        ... destination-configuration ...
    }
    destination-nat nat-name (address address <port port-number> |
        address-range low address high address);
    interface interface-name {
        allow-incoming;
        proxy-arp {
            address {
                address;
            }
            address-range {
                low address high address;
            }
        }
        source-nat {
            pool pool-name {
                address {
                    address;
                }
                address-range {
                    low address high address;
                }
                allow-incoming;
                host-address-low address-prefix;
                no-port-translation;
                overflow-pool (interface | pool-name);
            }
        }
        static-nat ip-prefix/prefix-length host ip-prefix</prefix-length>
            <virtual-router hostname>;
    }
    proxy-arp {
        interface interface-name {
            address ip-address to ip-address;
        }
    }
    source {
        ... source-configuration ...
    }
    source-nat {
        address-persistent;
        pool-set pool-set-name {
            pool pool-name;
        }
        pool-utilization-alarm {
            clear-threshold number;
            raise-threshold number;
        }
    }
}

```

```

    }
  }
  traceoptions {
    file <filename> <files number> <match regular-expression>
      <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag <syslog>;
    no-remote-trace;
  }
  destination {
    pool pool-name {
      address <ip-address> (to ip-address | port port-number);
      routing-instance routing-instance-name;
    }
    rule-set rule-set-name {
      from (interface [ interface-names ] |
        routing-instance [ routing-instance-names ] | zone [ zone-names ]);
      rule rule-name {
        match {
          destination-address destination-address;
          destination-port port-number;
          source-address [ source-addresses ];
        }
        then {
          destination-nat (off | pool pool-name);
        }
      }
    }
  }
}
source {
  address-persistent;
  pool pool-name {
    address ip-address to ip-address;
    host-address-base ip-address;
    overflow-pool (interface | ip-address);
    port no-translation | range high ip-address low ip-address;
    routing-instance ip-address;
  }
  pool-utilization-alarm {
    clear-threshold threshold-value;
    raise-threshold threshold-value;
  }
  rule-set rule-set-name {
    from (interface [ interface-names ] |
      routing-instance [ routing-instance-names ] | zone [ zone-names ]);
    rule rule-name {
      match {
        destination-address destination-address;
        source-address [ source-addresses ];
      }
      then {
        source-nat (off | pool pool-name);
      }
    }
  }
  to (interface [ interface-names ] | routing-instance [ routing-instance-names ] |
    zone [ zone-names ]);
}

```

```

    }
  }
  pki {
    auto-re-enrollment {
      certificate-id certificate-id {
        ca-profile-name profile-name;
        challenge-password password;
        re-enroll-trigger-time-percentage percentage;
        re-generate-keypair;
      }
    }
    ca-profile ca-profile-name {
      administrator {
        email-address email-address;
      }
      ca-identity ca-identifier;
      enrollment {
        retry attempts;
        retry-interval seconds;
        url url;
      }
      revocation-check {
        disable;
        crl {
          disable on-download-failure;
          refresh-interval hours;
          url url-name {
            password password;
          }
        }
      }
    }
  }
  traceoptions {
    file <filename> <files number> <match regular-expression>
      <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
policies {
  default-policy {
    (deny-all | permit-all);
  }
  from-zone zone-name to-zone zone-name {
    ... from-zone-configuration ...
  }
  policy-rematch;
  traceoptions {
    file <filename> <files number> <match regular-expression>
      <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
  }
  from-zone zone-name to-zone zone-name {
    policy policy-name {
      match {

```

```

        application [ application-names-or-sets ];
        destination-address [ addresses <any> ];
        source-address [ addresses <any> ];
    }
    scheduler-name scheduler-name;
    then {
        count {
            alarm per-second-threshold bytes per-minute-threshold kilobytes;
        }
        (deny | permit {... permit-configuration ...} | reject);
        permit {
            application-services {
                idp;
                redirect-wx;
                reverse-redirect-wx;
                utm-policy;
            }
            destination-address {
                drop-translated;
                drop-untranslated;
            }
            destination-nat nat-name;
            firewall-authentication {
                pass-through {
                    access-profile profile-name;
                    client-match user-or-group-name;
                    web-redirect;
                }
                web-authentication (
                    client-match user-or-group-name;
                )
            }
        }
        source-nat {
            (interface | pool pool-name | pool-set pool-set-name);
        }
        tunnel {
            ipsec-vpn vpn-name;
            pair-policy policy-name;
        }
    }
    log {
        session-close;
        session-init;
    }
}
}
}
}
screen {
    ids-option screen-name {
        alarm-without-drop;
        icmp {
            flood <threshold packets-per-second>;
            fragment;
            ip-sweep <threshold packets-per-microsecond>;
            large;
        }
    }
}

```

```

    ping-death;
  }
  ip {
    bad-options;
    block-frag;
    loose-source-route-option;
    record-route-option;
    security-option;
    source-route-option;
    spoofing;
    stream-option;
    strict-source-route-option;
    tear-drop;
    timestamp-option;
    unknown-protocol;
  }
  limit-session {
    destination-ip-based number-of-sessions;
    source-ip-based number-of-sessions;
  }
  tcp {
    fin-no-ack;
    land;
    port-scan <threshold packets-per-microsecond>;
    syn-ack-ack-proxy <threshold number-of-connections>;
    syn-fin;
    syn-flood {
      alarm-threshold requests-per-second;
      attack-threshold requests-per-second;
      destination-threshold packets-per-second;
      source-threshold packets-per-second;
      timeout seconds;
    }
    syn-frag;
    tcp-no-flag;
    winnuke;
  }
  udp {
    flood <threshold packets-per-second>;
  }
}
traceoptions {
  file <filename> <files number> <match regular-expression>
    <size maximum-file-size> <world-readable | no-world-readable>;
  flag flag;
  no-remote-trace;
}
}
ssh-known-hosts {
  fetch-from-server (hostname | address);
  host (hostname | address) {
    dsa-key key;
    rsa-key key;
    rsa1-key key;
  }
  load-key-file filename;
}

```

```

}
traceoptions {
  file <filename> <files number> <match regular-expression>
    <size maximum-file-size> <world-readable | no-world-readable>;
  flag flag;
  no-remote-trace;
  rate-limit rate;
}
zones {
  functional-zone management {
    host-inbound-traffic {
      protocols {
        protocol-name <except>;
      }
      system-services {
        service-name <except>;
      }
    }
  }
  interfaces {
    interface-name {
      host-inbound-traffic {
        protocols {
          protocol-name <except>;
        }
        system-services {
          service-name <except>;
        }
      }
    }
  }
}
screen screen-name;
}
security-zone zone-name {
  address-book {
    address address-name (ip-prefix</prefix-length> |
      dns-name dns-address-name);
    address-set set-name {
      address address-name;
    }
  }
  host-inbound-traffic {
    protocols {
      protocol-name <except>;
    }
    system-services {
      service-name <except>;
    }
  }
  interfaces {
    interface-name {
      host-inbound-traffic {
        protocols {
          protocol-name <except>;
        }
        system-services {
          service-name <except>;
        }
      }
    }
  }
}

```



```
    }  
  }  
}  
screen object-name;  
tcp-rst;  
}  
}
```

[edit services] Hierarchy Level

```

services {
  adaptive-services-pics {
    traceoptions {
      file <filename> <files number> <match regular-expression>
        <size maximum-file-size> <world-readable | no-world-readable>;
      flag flag;
      no-remote-trace;
    }
  }
  border-signaling-gateway {
    gateway gateway-name {
      embedded-spdp {
        service-class service-class-name {
          term term-name {
            from {
              media-type (any | audio | video);
            }
            then {
              committed-burst-size bytes;
              committed-information-rate bytes-per-second;
              dscp (alias | do-not-change | dscp-value);
              reject;
            }
          }
        }
      }
    }
  }
  service-interface name;
  service-point service-point-name {
    service-point-type service-point-type;
    port-number {
      ip-address ip-address;
      transport-protocol (tcp | udp);
    }
    service-interface name.number;
    service-policies {
      new-call-usage-policies [ policy-and-policy-set-names ];
      new-transaction-policies [ policy-and-policy-set-names ];
    }
  }
  sip {
    new-call-usage-policy policy-name {
      term term-name {
        from {
          contact [ contact-fields ];
          method {
            method-invite;
          }
          request-uri [ uri-fields ];
          source-address [ ip-addresses ];
        }
        then {
          (accept | reject);
          media-policy service-class-name;
        }
      }
    }
  }
}

```

```

        trace;
    }
}
}
new-call-usage-policy-set policy-set-name {
    policy-name [ policy-names ];
}
new-transaction-policy policy-name {
    term term-name {
        from {
            contact [ contact-fields ];
            method {
                method-invite;
                method-message;
                method-options;
                method-publish;
                method-refer;
                method-register;
                method-subscribe;
            }
            request-uri [ uri-fields ];
            source-address [ ip-addresses ];
        }
        then {
            (accept | reject);
            route {
                egress-service-point service-point-name;
                next-hop (request-uri | address ipv4-address <port port-number>
                    <transport-protocol (tcp | udp)>);
            }
            trace;
        }
    }
}
}
new-transaction-policy-set policy-set-name {
    policy-name [ policy-names ];
}
timers {
    maximum-call-duration seconds;
    timer-c seconds;
}
}
traceoptions {
    file {
        filename filename;
        files number-of-files;
        match regular-expression;
        size maximum-trace-file-size;
    }
    flag {
        datastore {
            data flag-modifier;
            db flag-modifier;
            handle flag-modifier;
            minimum flag-modifier;
        }
    }
}

```

```

framework {
    action flag-modifier;
    event flag-modifier;
    executor flag-modifier;
    freezer flag-modifier;
    minimum flag-modifier;
    memory-pool flag-modifier;
}
minimum flag-modifier;
sbc-utils {
    common flag-modifier;
    configuration flag-modifier;
    device-monitor flag-modifier;
    ipc flag-modifier;
    memory-management flag-modifier;
    message flag-modifier;
    minimum flag-modifier;
    user-interface flag-modifier;
}
session-trace flag-modifier;
signaling {
    b2b flag-modifier;
    b2b-wrapper flag-modifier;
    minimum flag-modifier;
    policy flag-modifier;
    sip-stack-wrapper flag-modifier;
    topology-hiding flag-modifier;
    ua flag-modifier;
}
sip-stack {
    dev-logging;
    event-tracing;
    ips-tracing;
    pd-log-detail (full | summary);
    pd-log-level (audit | exception | problem);
    per-tracing;
    verbose-logging;
}
}
}
}
cos {
    application-profile profile-name {
        sip-text {
            dscp (alias | bits);
            forwarding-class class-name;
        }
        sip-video {
            dscp (alias | bits);
            forwarding-class class-name;
        }
        sip-voice {
            dscp (alias | bits);
            forwarding-class class-name;
        }
    }
}

```

```

}
rule rule-name {
  match-direction (input | output | input-output);
  term term-name {
    from {
      application-sets set-name;
      applications [ application-names ];
      destination-address address <except>;
      destination-address-range low minimum-value high maximum-value
        <except>;
      destination-prefix-list list-name <except>;
      source-address (address | any-unicast) <except>;
      source-address-range low minimum-value high maximum-value <except>;
      source-prefix-list list-name <except>;
    }
    then {
      application-profile profile-name;
      dscp (alias | bits);
      forwarding-class class-name;
      syslog;
      (reflexive | reverse) {
        application-profile profile-name;
        dscp (alias | bits);
        forwarding-class class-name;
        syslog;
      }
    }
  }
}
rule-set rule-set-name {
  rule rule-name;
}
}
dynamic-flow-capture {
  capture-group client-name {
    content-destination identifier {
      address address;
      hard-limit bandwidth;
      hard-limit-target bandwidth;
      soft-limit bandwidth;
      soft-limit-clear bandwidth;
      ttl hops;
    }
    control-source identifier {
      allowed-destinations [ destinations ];
      minimum-priority value;
      no-syslog;
      notification-targets address port port-number;
      service-port port-number;
      shared-key value;
      source-addresses [ addresses ];
    }
  }
  duplicates-dropped-periodicity seconds;
  max-duplicates number;
  input-packet-rate-threshold rate;
}

```

```

        interfaces interface-name;
        pic-memory-threshold percentage percentage;
    }
    g-duplicates-dropped-periodicity seconds;
    g-max-duplicates number;
}
flow-collector {
    analyzer-address address;
    analyzer-id name;
    destinations {
        ftp:url {
            password "password";
        }
    }
    file-specification {
        variant variant-number {
            data-format format;
            name-format format;
            transfer {
                record-level number;
                timeout seconds;
            }
        }
    }
}
interface-map {
    collector interface-name;
    file-specification variant-number;
    interface-name {
        file-specification variant-number;
        collector interface-name;
    }
}
retry number;
retry-delay seconds;
transfer-log-archive {
    archive-sites {
        ftp:url {
            password "password";
            username username;
        }
    }
    filename-prefix prefix;
    maximum-age minutes;
}
}
flow-monitoring {
    version9 {
        template template-name {
            flow-active-timeout seconds;
            flow-inactive-timeout seconds;
            ipv4-template;
            mpls-template {
                label-position [ positions ];
            }
            mpls-ipv4-template {
                label-position [ positions ];
            }
        }
    }
}

```

```

    }
    option-refresh-rate packets;
    template-refresh-rate packets;
  }
}
}
flow-tap {
  interface interface-name;
}
ids {
  rule rule-name {
    match-direction (input | output | input-output);
    term term-name {
      from {
        application-sets set-name;
        applications [ application-names ];
        destination-address address <except>;
        destination-address-range low minimum-value high maximum-value
          <except>;
        destination-prefix-list list-name <except>;
        source-address (address | any-unicast) <except>;
        source-address-range low minimum-value high maximum-value <except>;
        source-prefix-list list-name <except>;
      }
      then {
        aggregation {
          destination-prefix prefix-value;
          destination-prefix-ipv6 prefix-value;
          source-prefix prefix-value;
          source-prefix-ipv6 prefix-value;
        }
      }
    }
    (force-entry | ignore entry);
    logging {
      syslog;
      threshold rate;
    }
    session-limit {
      by-destination {
        hold-time seconds;
        maximum number;
        packets number;
        rate number;
      }
      by-pair {
        maximum number;
        packets number;
        rate number;
      }
      by-source {
        hold-time seconds;
        maximum number;
        packets number;
        rate number;
      }
    }
  }
}

```

```

        syn-cookie {
            mss value;
            threshold rate;
        }
    }
}
rule-set rule-set-name {
    rule rule-name;
}
}
ipsec-vpn {
    clear-ike-sas-on-pic-restart;
    clear-ipsec-sas-on-pic-restart;
    establish-tunnels (immediately | on-traffic);
    ike {
        policy policy-name {
            description description;
            local-certificate certificate-identifier;
            local-id (fqdn domain-name | ipv4_addr ipv4-address | ipv6_addr ipv6-address |
                key-id identifier);
            mode (aggressive | main);
            pre-shared-key (ascii-text key | hexadecimal key);
            proposals [ proposal-names ];
            remote-id {
                (any-remote-id | one or more of the following four statements);
                fqdn [ domain-names ];
                ipv4_addr [ ipv4-addresses ];
                ipv6_addr [ ipv6-addresses ];
                key-id [ identifiers ];
            }
        }
    }
    proposal proposal-name {
        authentication-algorithm (md5 | sha1 | sha256);
        authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
        description description;
        dh-group (group1 | group2);
        encryption-algorithm algorithm;
        lifetime-seconds seconds;
    }
}
ipsec {
    proposal proposal-name {
        authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
        description description;
        encryption-algorithm algorithm;
        lifetime-seconds seconds;
        protocol (ah | esp | bundle);
    }
    policy policy-name {
        description description;
        perfect-forward-secrecy {
            keys (group1 | group2);
        }
        proposals [ proposal-names ];
    }
}

```



```

rule rule-name {
  match-direction (input | output);
  term term-name {
    from {
      destination-address address;
      ipsec-inside-interface interface-name;
      source-address address;
    }
    then {
      backup-remote-gateway address;
      clear-don't-fragment-bit;
      dynamic {
        ike-policy policy-name;
        ipsec-policy policy-name;
      }
      initiate-dead-peer-detection;
      no-anti-replay;
      remote-gateway address;
      syslog;
      tunnel-mtu bytes;
      manual {
        direction (inbound | outbound | bidirectional) {
          authentication {
            algorithm (hmac-md5-96 | hmac-sha1-96);
            key (ascii-text key | hexadecimal key);
          }
        }
        auxiliary-spi spi-value;
        encryption {
          algorithm algorithm;
          key (ascii-text key | hexadecimal key);
        }
        protocol (ah | bundle | esp);
        spi spi-value;
      }
    }
  }
}

rule-set rule-set-name {
  rule rule-name;
}

traceoptions {
  file <filename> <files number> <match regular-expression>
  <size maximum-file-size> <world-readable | no-world-readable>;
  flag flag;
  no-remote-trace;
}

l2tp {
  tunnel-group group-name {
    hello-interval seconds;
    hide-avps;
    l2tp-access-profile profile-name;
    local-gateway address address;
    maximum-send-window packets;
  }
}

```

```

    ppp-access-profile profile-name;
    receive-window packets;
    retransmit-interval seconds;
    service-interface interface-name;
    syslog {
        host hostname {
            facility-override facility-name;
            log-prefix prefix-number;
            services severity-level;
        }
    }
    tunnel-timeout seconds;
}
traceoptions {
    debug-level level;
    filter {
        protocol name;
        user-name username;
    }
    flag flag;
    interfaces interface-name {
        debug-level severity;
        flag flag;
    }
}
}
logging {
    traceoptions {
        file <filename> <files number> <match regular-expression>
            <size maximum-file-size> <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
    }
}
mobile-ip {
    authenticate {
        order (aaa | local);
    }
    dynamic-home-assignment {
        home-agent {
            nai (name@domain.com | @domain.com) {
                home-agent ip-address;
            }
        }
    }
}
home-agent {
    enable-service interface-name;
}
virtual-network {
    home-agent-address ip-address {
        registration-lifetime seconds;
        revocation-required;
        timestamp-tolerance seconds;
    }
}
}
}

```

```

peer {
  (ip-address address | nai user@domain) {
    spi hexadecimal-value {
      algorithm (hmac-md5 | md5);
      entity-type (host | mobility-agent);
      key (hex | ascii) string;
      replay-method (none | timestamp seconds);
    }
  }
}
}
traceoptions {
  file <filename> <files number> <match regular-expression>
    <size maximum-file-size> <world-readable | no-world-readable>;
  flag flag;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
}
nat {
  pool nat-pool-name {
    address ip-prefix</prefix-length>;
    address-range low minimum-value high maximum-value;
    pgcp {
      hint [ hint-strings ];
      ports-per-session ports;
      remotely-controlled;
      transport [ rtp-avp tcp udp ];
    }
    port (automatic <auto> | range low minimum-value high maximum-value)
      <random-allocation>;
  }
}
rule rule-name {
  match-direction (input | output);
  term term-name {
    nat-type (full-cone | symmetric)
    from {
      application-sets set-name;
      applications [ application-names ];
      destination-address (address | any-unicast) <except>;
      destination-address-range low minimum-value high maximum-value
        <except>;
      destination-prefix-list list-name <except>;
      source-address (address | any-unicast) <except>;
      source-address-range low minimum-value high maximum-value <except>;
      source-prefix-list list-name <except>;
    }
    then {
      no-translation;
      translated {
        destination-pool nat-pool-name;
        destination-prefix destination-prefix;
        overload-pool overload-pool-name;
        overload-prefix overload-prefix;
        source-pool nat-pool-name;
        source-prefix source-prefix;
        translation-type (destination type | source type);
      }
    }
  }
}

```

```

    }
    syslog;
  }
}
rule-set rule-set-name {
  rule rule-name;
}
}
pgcp {
  gateway gateway-name {
    ... gateway-configuration ...
  }
  media-service media-service-name {
    nat-pool nat-pool-name;
  }
  rule rule-name {
    gateway gateway-name;
    media-service [ service-names ];
  }
  rule-set rule-set-name {
    rule rule-name;
  }
  session-mirroring {
    delivery-function function-name {
      destination-address destination-address;
      destination-port destination-port;
      network-operator-id network-operator-id;
      source-address source-address;
      source-port source-port;
    }
    disable-session-mirroring;
  }
  traceoptions {
    file <filename> <files number> <match regular-expression>
      <microsecond-stamp> <size maximum-file-size> <world-readable |
      no-world-readable>;
    flag flag;
    no-remote-trace;
  }
  virtual-interface interface-number {
    interface interface-identifier;
    media-service [ service-names ];
    routing-instance instance-name {
      service-interface name.number;
    }
    service-state (in-service | out-of-service-forced | out-of-service-graceful);
  }
  gateway gateway-name {
    cleanup-timeout seconds;
    data-inactivity-detection {
      inactivity-delay;
      inactivity-duration seconds;
      latch-deadlock-delay seconds;
      report-service-change {
        service-change-type (forced-906 | forced-910);
      }
    }
  }
}

```

```

    }
    send-notification-on-delay;
    stop-detection-on-drop;
  }
  fast-update-filters {
    maximum-terms number-of-terms;
    maximum-fuf-percentage percentage;
  }
  gateway-address gateway-address;
  gateway-controller gateway-controller-name {
    (local-controller | remote-controller);
    controller-address ip-address;
    controller-port port-number;
    interim-ah-scheme {
      algorithm algorithm;
    }
  }
  gateway-port gateway-port;
  graceful-restart {
    maximum-synchronization-mismatches number-of-mismatches;
    maximum-synchronization-time seconds;
  }
  h248-options {
    ... h248-options-configuration ...
  }
  h248-properties {
    ... h248-properties-configuration ...
  }
  h248-timers {
    initial-average-ack-delay milliseconds;
    maximum-net-propagation-delay milliseconds;
    maximum-waiting-delay milliseconds;
    tmax-retransmission-delay milliseconds;
  }
  max-concurrent-calls number;
  monitor {
    media {
      rtcp;
      rtp;
    }
  }
  service-state (in-service | out-of-service-forced | out-of-service-graceful);
  session-mirroring {
    delivery-function [ function-names ];
    disable-session-mirroring;
  }
  h248-options {
    audit-observed-events-returns-history;
    encoding {
      no-dscp-bit-mirroring;
    }
    service-change {
      context-indications {
        state-loss (forced-910 | forced-915 | none);
      }
      control-association-indications {

```

```

    disconnect {
        controller-failure (failover-909 | restart-902);
        reconnect (disconnected-900 | restart-902);
    }
    down {
        administrative (forced-905 | forced-908 | none);
        failure (forced-904 | forced-908 | none);
        graceful (graceful-905 | none);
    }
    up {
        cancel-graceful (none | restart-918);
        failover-cold (failover-920 | restart-901);
        failover-warm (failover-919 | restart-902);
    }
}
virtual-interface-indications {
    virtual-interface-down {
        administrative (forced-905 | forced-906 | none);
        failure (forced-904 | forced-906 | none);
        graceful (graceful-905 | none);
        link-loss (forced-906 | none);
    }
    virtual-interface-up {
        cancel-graceful (none | restart-918);
        warm (none | restart-900);
    }
}
}
wildcard-response-service-change;
}
h248-properties {
    base-root {
        mg-originated-pending-limit default number;
        mg-provisional-response-timer-value default milliseconds;
        mgc-originated-pending-limit default number;
        mgc-provisional-response-timer-value default milliseconds;
        normal-mg-execution-time default milliseconds;
        normal-mgc-execution-time default milliseconds;
    }
    diffserv {
        dscp default (dscp-value | alias | do-not-change);
    }
    event-timestamp-notification {
        request-timestamp (requested | suppressed | autonomous);
    }
    hanging-termination-detection {
        timerx seconds;
    }
    notification-behavior {
        notification-regulation default (once | percentage);
    }
    segmentation {
        mg-maximum-pdu-size default bytes;
        mg-segmentation-timer default milliseconds;
        mgc-maximum-pdu-size default bytes;
        mgc-segmentation-timer default milliseconds;
    }
}

```

```

    }
    traffic-management {
        max-burst-size {
            default bps;
            rtcp {
                (fixed-value bytes | percentage percentage);
            }
        }
        peak-data-rate {
            default bps;
            rtcp {
                (fixed-value bytes | percentage percentage);
            }
        }
        sustained-data-rate {
            default bps;
            rtcp {
                (fixed-value bytes | percentage percentage);
            }
        }
    }
}
}
}
}
}
radius-flow-tap {
    forwarding-class class-name;
    interfaces interface-name;
    source-ipv4-address ipv4-address;
}
rpm {
    bgp {
        data-fill data;
        data-size size;
        destination-port port;
        history-size size;
        logical-system logical-system-name <routing-instances routing-instance-name>;
        moving-average-size number-of-samples;
        probe-count count;
        probe-interval seconds;
        probe-type type;
        routing-instances {
            routing-instance-name;
        }
        test-interval seconds;
    }
    probe owner {
        test test-name {
            data-fill data;
            data-size size;
            destination-interface output-interface-name;
            destination-port port;
            dscp-code-points dscp-bits;
            hardware-timestamp;
            history-size size;
            moving-average-size number-of-samples;
            one-way-hardware-timestamp;
        }
    }
}

```

```

    probe-count count;
    probe-interval seconds;
    probe-type type;
    routing-instance routing-instance-name;
    source-address address;
    target (address address | url url);
    test-interval seconds;
    thresholds {
        egress-time microseconds;
        ingress-time microseconds;
        jitter-egress microseconds;
        jitter-ingress microseconds;
        jitter-rtt microseconds;
        rtt microseconds;
        std-dev-egress microseconds;
        std-dev-ingress microseconds;
        std-dev-rtt microseconds;
        successive-loss count;
        total-loss count;
    }
    traps [ trap-names ];
}
}
probe-limit number;
probe-server {
    probe-server {
        tcp {
            destination-interface interface-name;
            port port-number;
        }
        udp {
            destination-interface interface-name;
            port port-number;
        }
    }
}
}
service-set service-set-name {
    allow-multicast;
    (cos-rules rule-name | cos-rule-sets rule-set-name);
    extension-service service-name {
        provider-specific-rules;
    }
    (ids-rules rule-names | ids-rule-sets rule-set-name);
    interface-service {
        service-interface interface-name;
    }
    (ipsec-vpn-rules rule-names | ipsec-vpn-rule-sets rule-set-name);
    ipsec-vpn-options {
        ike-access-profile profile-name;
        local-gateway address;
    }
    max-flows number;
    (nat-rules rule-names | nat-rule-sets rule-set-name);
    next-hop-service {
        inside-service-interface name.number;
        outside-service-interface name.number;
    }
}

```



```

}
(pgcp-rules rule-names | pgcp-rule-sets rule-set-name);
service-order {
    forward-flow [ service-names ];
    reverse-flow [ service-names ];
}
(stateful-firewall-rules rule-names | stateful-firewall-rule-sets rule-set-name);
syslog {
    host hostname {
        facility-override facility-name;
        log-prefix prefix-number;
        services priority-level;
    }
}
}
stateful-firewall {
    rule rule-name {
        match-direction (input | output | input-output);
        term term-name {
            from {
                application-sets set-name;
                applications [ application-names ];
                destination-address (address | any-unicast) <except>;
                destination-address-range low minimum-value high maximum-value
                    <except>;
                destination-prefix-list list-name <except>;
                source-address (address | any-unicast) <except>;
                source-address-range low minimum-value high maximum-value <except>;
                source-prefix-list list-name <except>;
            }
            then {
                (accept | discard | reject);
                allow-ip-options [ values ];
                syslog;
            }
        }
    }
    rule-set rule-set-name {
        rule rule-name;
    }
}
unified-access-control {
    infranet-controller hostname {
        address ip-address;
        ca-profile ca-profile;
        interface interface-name;
        port port-number;
        password password;
        server-certificate-subject subject;
    }
    interval seconds;
    test-only-mode (false | true);
    timeout seconds;
    timeout-action (close | no-change | open);
    traceoptions {
        flag flag;
    }
}

```

```
}  
}  
}
```

[edit snmp] Hierarchy Level

```

snmp {
  client-list list-name;
  community community-name {
    authorization (read-only | read-write);
    client-list-name list-name;
    clients {
      address <restrict>;
    }
    routing-instances routing-instance-name {
      client-list-name list-name;
      clients {
        address <restrict>;
      }
    }
  }
  view view-name;
}
contact contact-information;
description description;
engine-id {
  (local engine-id | use-default-ip-address | use-mac-address);
}
filter-duplicates;
health-monitor {
  falling-threshold percentage;
  interval seconds;
  rising-threshold percentage;
}
interface [ interface-names ];
location location;
logical-system-trap-filter;
name system-name;
nonvolatile {
  commit-delay seconds;
}
rmon {
  alarm index {
    description description;
    falling-event-index index;
    falling-threshold integer;
    falling-threshold-interval seconds;
    interval seconds;
    request-type (get-next-request | get-request | walk-request);
    rising-event-index index;
    rising-threshold integer;
    sample-type (absolute-value | delta-value);
    startup-alarm (falling-alarm | rising-alarm | rising-or-falling alarm);
    syslog-subtag text-string;
    variable oid-variable;
  }
  event index {
    community community-name;
    description description;
    type (log | log-and-trap | none | snmptrap);
  }
}

```

```

    }
  }
  routing-instance-access {
    access-list {
      routing-instance-name;
    }
  }
  traceoptions {
    file <files number> <match regular-expression> <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
  }
  trap-group group-name {
    categories {
      authentication;
      chassis;
      configuration;
      link;
      remote-operations;
      rmon-alarm;
      routing;
      services;
      sonet-alarms {
        alarm-name;
      }
      startup;
      vrrp-events;
    }
    destination-port port-number;
    routing-instance instance-name;
    targets {
      address;
    }
    version (all | v1 | v2);
  }
  trap-options {
    agent-address outgoing-interface;
    routing-instances instance-name {
      source-address address;
    }
    source-address address;
  }
  v3 {
    notify name {
      tag tag-name;
      type (inform | trap);
    }
    notify-filter name {
      oid oid <exclude | include>;
    }
    snmp-community community-index {
      community-name community-name;
      context context-name;
      security-name security-name;
      tag tag-name;
    }
  }

```

```

}
target-address target-address-name {
  address address;
  address-mask address-mask;
  port port-number;
  retry-count number;
  routing-instance instance-name;
  tag-list tag-list;
  target-parameters parameter-name;
  timeout seconds;
}
target-parameters parameter-name {
  notify-filter name;
  parameters {
    message-processing-model (v1 | v2c | v3);
    security-level (authentication | none | privacy);
    security-model (usm | v1 | v2c);
    security-name security-name;
  }
}
}
usm {
  local-engine {
    user username {
      authentication-md5 {
        authentication-password password;
      }
      authentication-none;
      authentication-sha {
        authentication-password password;
      }
      privacy-3des {
        privacy-password password;
      }
      privacy-aes128 {
        privacy-password password;
      }
      privacy-des {
        privacy-password password;
      }
      privacy-none;
    }
  }
}
remote-engine engine-name {
  user username {
    authentication-md5 {
      authentication-password password;
    }
    authentication-none;
    authentication-sha {
      authentication-password password;
    }
    privacy-3des {
      privacy-password password;
    }
    privacy-aes128 {
      privacy-password password;
    }
  }
}

```

```

    }
    privacy-des {
        privacy-password password;
    }
    privacy-none;
}
}
}
vacm {
    access {
        group group-name {
            context-prefix prefix {
                security-model (any | usm | v1 | v2c) {
                    security-level (authentication | none | privacy) {
                        context-match (exact | prefix);
                        notify-view view-name;
                        read-view view-name;
                        write-view view-name;
                    }
                }
            }
        }
    }
    default-context-prefix {
        security-model (any | usm | v1 | v2c) {
            security-level (authentication | none | privacy) {
                context-match (exact | prefix);
                notify-view view-name;
                read-view view-name;
                write-view view-name;
            }
        }
    }
}
}
}
}
security-to-group {
    security-model (usm | v1 | v2c) {
        security-name security-name {
            group group-name;
        }
    }
}
}
}
}
view view-name {
    oid object-identifier (exclude | include);
}
}

```

[edit switch-options] Hierarchy Level

```
switch-options {  
  interface interface-name {  
    interface-mac-limit {  
      number-of-addresses;  
      packet-action drop;  
    }  
    no-mac-learning;  
  }  
  interface-mac-limit {  
    number-of-addresses;  
    packet-action drop;  
  }  
  mac-statistics;  
  mac-table-size {  
    number-of-addresses;  
    packet-action drop;  
  }  
  no-mac-learning;  
}
```

[edit system] Hierarchy Level

```

system {
  accounting {
    destination {
      radius {
        server {
          server-address {
            accounting-port port-number;
            retry number;
            port port-number;
            secret password;
            source-address address;
            timeout seconds;
          }
        }
      }
    }
  }
  tacplus {
    server {
      server-address {
        port port-number;
        secret password;
        single-connection;
        timeout seconds;
      }
    }
  }
  events [ change-log interactive-commands login ];
}
archival {
  configuration {
    archive-sites {
      ftp://<username>:<password>@<host>:<port>/<url-path>;
    }
    transfer-interval interval;
    transfer-on-commit;
  }
}
arp {
  aging-timer {
    minutes;
    interface logical-interface-name;
  }
  passive-learning;
}
authentication-order [ authentication-methods ];
autoinstallation {
  configuration-servers {
    server-url <password password>;
  }
  interfaces {
    interface-name {
      bootp;
      rarp;
    }
  }
}

```



```

    }
  }
}
backup-router address <destination [ destination-addresses ]>;
commit synchronize;
(compress-configuration-files | no-compress-configuration-files);
default-address-selection;
diag-port-authentication (encrypted-password "password" | plain-text-password);
domain-name domain-name;
domain-search [ domain-list ];
dump-device (boot-device | compact-flash | removable-compact-flash | usb);
encrypt-configuration-files;
extensions {
  provider {
    provider-id;
  }
}
host-name hostname;
inet6-backup-router ipv6-address <destination address>;
internet-options {
  (gre-path-mtu-discovery | no-gre-path-mtu-discovery);
  icmpv4-rate-limit {
    bucket-size number;
    packet-rate rate;
  }
  icmpv6-rate-limit {
    bucket-size number;
    packet-rate rate;
  }
  (ipip-path-mtu-discovery | no-ipip-path-mtu-discovery);
  (ipv6-path-mtu-discovery | no-ipv6-path-mtu-discovery);
  ipv6-path-mtu-discovery-timeout;
  no-tcp-rfc1323;
  no-tcp-rfc1323-paws;
  (path-mtu-discovery | no-path-mtu-discovery);
  source-port upper-limit upper-limit;
  source-quench;
  tcp-drop-synfin-set;
}
location {
  altitude feet;
  building name;
  country-code code;
  floor number;
  hcoord horizontal-coordinate;
  lata service-area;
  latitude degrees;
  longitude degrees;
  npa-nxx number;
  postal-code postal-code;
  rack number;
  vcoord vertical-coordinate;
}
login {
  announcement "text";
  class class-name {

```

```

    allow-commands "regular-expression";
    allow-configuration "regular-expression";
    deny-commands "regular-expression";
    deny-configuration "regular-expression";
    idle-timeout minutes;
    login-alarms;
    login-tip;
    permissions [ permissions ];
}
message "text";
password {
    change-type (character-sets | set-transitions);
    format (des | md5 | sha1);
    maximum-length length;
    minimum-changes number;
    minimum-length length;
}
retry-options {
    backoff-factor number;
    backoff-threshold number;
    minimum-time number;
    tries-before-disconnect number;
}
user username {
    authentication {
        (encrypted-password "password" | plain-text-password);
        load-key-file filename;
        ssh-dsa "public-key" <from hostname>;
        ssh-rsa "public-key" <from hostname>;
    }
    class class-name;
    full-name "complete-name";
    uid uid-value;
}
}
max-configurations-on-flash number;
mirror-flash-on-disk;
name-server {
    address;
}
no-multicast-echo;
no-redirects;
no-ping-record-route;
no-ping-time-stamp;
ntp {
    authentication-key key-number type md5 value password;
    boot-server address;
    broadcast <address> <key key-number> <version value> <ttl value>;
    broadcast-client;
    multicast-client <address>;
    peer address <key key-number> <version value> <prefer>;
    server address <key key-number> <version value> <prefer>;
    trusted-key [ key-numbers ];
}
pic-console-authentication {
    (encrypted-password encrypted-password | plain-text-password);

```

```

}
ports {
  auxiliary {
    disable;
    insecure;
    type (ansi | small-xterm | vt100 | xterm);
  }
  console {
    disable;
    insecure;
    log-out-on-disconnect;
    type (ansi | small-xterm | vt100 | xterm);
  }
}
processes {
  ... the following statement represents the syntax for most processes on EX-series
  and MX-series platforms; processes with different syntax follow ...
  process-name <disable> <command pathname> <failover (alternate-media |
  other-routing-engine)>;
  ... the following statement represents the syntax for most processes on M-series
  and T-series routing platforms; processes with different syntax follow ...
  process-name <disable> <command pathname>;
  (cfm | send) disable;
  (chassis-control | ntp | routing) <disable> <failover alternate-media>;
  (dhcp | ethernet-switching | kernel-replication | l2-learning | lacp |
  multicast-snooping) <disable> <command pathname>; #nondefault syntax
  for process on EX-series platforms
  (diameter-service | general-authentication-service) {
    disable;
    traceoptions {
      file <filename> <files number> <match regular-expression>
      <size maximum-file-size> <world-readable | no-world-readable>;
      flag flag;
      no-remote-trace;
    }
  }
  (process-monitor | resource-cleanup) {
    disable;
    traceoptions {
      file <filename> <files number> <match regular-expression>
      <size maximum-file-size> <world-readable | no-world-readable>;
      flag flag;
      level severity;
      no-remote-trace;
    }
  }
}
sbc-configuration-process {
  disable;
  failover alternate-media;
  traceoptions {
    file <filename> <files number> <match regular-expression>
    <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}

```

```

    watchdog <enable | disable> <timeout seconds>;
}
radius-options {
  attributes {
    nas-ip-address address;
  }
}
radius-server {
  server-address {
    accounting-port port-number;
    port port-number;
    retry number;
    secret password;
    source-address source-address;
    timeout seconds;
  }
}
root-authentication {
  (encrypted-password "password" | plain-text-password);
  load-key-file filename;
  ssh-dsa "public-key" <from hostname>;
  ssh-rsa "public-key" <from hostname>;
}
(saved-core-context | no-saved-core-context);
saved-core-files saved-core-files;
scripts {
  commit {
    allow-transients;
    file filename.xml {
      optional;
      refresh;
      refresh-from url;
      source url;
    }
  }
  refresh;
  refresh-from url;
  traceoptions {
    file <filename> <files number> <size maximum-file-size> <world-readable |
      no-world-readable>;
    flag flag;
    no-remote-trace;
  }
}
op {
  file filename.xml {
    arguments {
      argument-name <description description>;
    }
    command filename-alias;
    description description;
    refresh;
    refresh-from url;
    source url;
  }
  refresh;
  refresh-from url;
}

```

```

    traceoptions {
        file <filename> <files number> <size maximum-file-size> <world-readable |
            no-world-readable>;
        flag flag;
        no-remote-trace;
    }
}
}
services {
    database-replication {
        traceoptions {
            file <filename> <files number> <match regular-expression>
                <size maximum-file-size> <world-readable | no-world-readable>;
            flag flag;
            no-remote-trace;
        }
    }
}
dhcp {
    boot-file filename;
    boot-server hostname;
    default-lease-time (seconds | infinite);
    domain-name domain-name;
    domain-search {
        domain-suffix;
    }
    maximum-lease-time (seconds | infinite);
    name-server {
        address;
    }
    next-server address;
    option option-index (array type-name [ type-values ] | byte 8-bit-value | flag (false |
        off | on | true) | integer signed-32-bit-value | ip-address address |
        short signed-16-bit-value | string text-string | unsigned-integer 32-bit-value |
        unsigned-short 16-bit-value);
    pool {
        ... pool-configuration ...
    }
    propagate-settings interface-name;
    router {
        address;
    }
    server-identifier identifier;
    static-binding {
        ... static-binding-configuration ...
    }
    traceoptions {
        file <filename> <files number> <match regular-expression>
            <size maximum-file-size> <world-readable | no-world-readable>;
        flag flag;
        level severity;
        no-remote-trace;
    }
    wins-server {
        address;
    }
    pool ip-prefix/prefix-length {

```

```

address-range low address high address;
boot-file filename;
boot-server hostname;
default-lease-time (seconds | infinite);
domain-name domain-name;
domain-search {
    domain-suffix;
}
exclude-address {
    ipv4-address;
}
maximum-lease-time (seconds | infinite);
name-server {
    address;
}
next-server address;
option option-index (array type-name type-values ] | byte 8-bit-value |
    flag (false | off | on | true) | integer signed-32-bit-value | ip-address address |
    short signed-16-bit-value | string text-string | unsigned-integer 32-bit-value |
    unsigned-short 16-bit-value);
propagate-settings interface-name;
router {
    address;
}
server-identifier identifier;
wins-server {
    address;
}
}
static-binding mac-address {
    boot-file filename;
    boot-server hostname;
    client-identifier (ascii ascii-text | hexadecimal hexadecimal-value);
    domain-name domain-name;
    domain-search {
        domain-suffix;
    }
    fixed-address {
        ipv4-address;
    }
    host-name hostname;
    name-server {
        address;
    }
    next-server address;
    option option-index (array type-name type-values ] | byte 8-bit-value |
        flag (false | off | on | true) | integer signed-32-bit-value | ip-address address |
        short signed-16-bit-value | string text-string | unsigned-integer 32-bit-value |
        unsigned-short 16-bit-value);
    router {
        address;
    }
    server-identifier identifier;
    wins-server {
        address;
    }
}

```

```

    }
  }
}
dhcp-local-server {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name;
      logical-system-name;
      mac-address;
      option-60;
      option-82 <circuit-id> <remote-id>;
      routing-instance-name;
      user-prefix prefix-string;
    }
  }
  dynamic-profile profile-name (aggregate-clients |
    use-primary primary-profile-name);
  group {
    ... group-configuration ...
  }
  overrides {
    client-discover-match;
    interface-client-limit number;
    no-arp;
  }
  pool-match-order {
    ip-address-first;
    option-82;
  }
  traceoptions {
    file <filename> <files number> <match regular-expression>
      <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
  }
  group group-name {
    authentication {
      password password-string;
      username-include {
        circuit-type;
        delimiter delimiter-character;
        domain-name domain-name;
        logical-system-name;
        mac-address;
        option-60;
        option-82 <circuit-id> <remote-id>;
        routing-instance-name;
        user-prefix prefix-string;
      }
    }
  }
  dynamic-profile profile-name (aggregate-clients |
    use-primary primary-profile-name);
  interface interface-name <exclude> <upto interface-name>;

```

```

        overrides {
            client-discover-match;
            interface-client-limit number;
            no-arp;
        }
    }
}
dns-proxy {
    cache {
        hostname inet address;
    }
    interface {
        interface-name;
    }
    server-select list-identifier {
        domain-name domain-name;
        name-server {
            address;
        }
    }
    traceoptions {
        file filename <files number> <match regular-expression>
            <size maximum-file-size> <world-readable | no-world-readable>;
        flag flag;
    }
}
dynamic-dns {
    client hostname {
        agent agent-name;
        interface interface-name;
        password password;
        server (ddo | dyndns);
        username server-username;
    }
}
finger {
    connection-limit limit;
    rate-limit limit;
}
flow-tap-dtcp {
    ssh {
        connection-limit limit;
        rate-limit limit;
    }
}
ftp {
    connection-limit limit;
    rate-limit limit;
}
netconf {
    ssh {
        connection-limit limit;
        rate-limit limit;
    }
}
outbound-ssh {

```



```

application-id application-id {
    address {
        port port-number;
        retry number;
        timeout seconds;
    }
    device-id device-id;
    keep-alive {
        retry number;
        timeout seconds;
    }
    reconnect-strategy (in-order | sticky);
    secret secret;
    services netconf;
}
traceoptions {
    file <filename> <files number> <match regular-expression>
        <size maximum-file-size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
}
service-deployment {
    local-certificate certificate-name;
    servers {
        server-address {
            port port-number;
            security-options (ssl3 | tls);
            user username;
        }
    }
    source-address address;
    traceoptions {
        flag flag;
    }
}
}
ssh {
    connection-limit limit;
    protocol-version [ v1 v2 ];
    rate-limit limit;
    root-login (allow | deny | deny-password);
}
telnet {
    connection-limit limit;
    rate-limit limit;
}
web-management {
    control {
        max-threads number;
    }
    http {
        interface [ interface-names ];
        port port-number;
    }
    https {
        interface [ interface-names ];
    }
}

```

```

        (local-certificate certificate-name | pki-local-certificate certificate-name |
         system-generated-certificate);
        port port-number;
    }
    session {
        idle-timeout minutes;
        session-limit number;
    }
}
xnm-clear-text {
    connection-limit limit;
    rate-limit limit;
}
xnm-ssl {
    connection-limit limit;
    local-certificate certificate-name;
    rate-limit limit;
}
}
static-host-mapping {
    hostname {
        alias [ aliases ];
        inet [ addresses ];
        inet6 [ addresses ];
        sysid system-identifier;
    }
}
syslog {
    archive {
        files number;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    console {
        facility severity;
    }
    file filename {
        facility severity;
        explicit-priority;
        match "regular-expression";
        archive {
            files number;
            size maximum-file-size;
            (world-readable | no-world-readable);
        }
    }
}
host (hostname | other-routing-engine | scc-master) {
    facility severity;
    explicit-priority;
    facility-override facility;
    log-prefix string;
    match "regular-expression";
}
source-address source-address;
time-format (year | millisecond | year millisecond);
user (username | *) {

```

```

        facility severity;
        match "regular-expression";
    }
}
tacplus-options {
    (exclude-cmd-attribute | no-cmd-attribute-value);
    service-name service-name;
}
tacplus-server {
    server-address {
        port port-number;
        secret password;
        single-connection;
        source-address address;
        timeout seconds;
    }
}
time-zone (GMT | GMT+hour-offset | GMT-hour-offset | zone-name);
}

```

[edit virtual-chassis] Hierarchy Level

```
virtual-chassis {  
  fast-failover (ge | vcp disable | xe);  
  id id;  
  mac-persistence-timer minutes;  
  member member-id {  
    mastership-priority number;  
    no-management-vlan;  
    role (line-card | routing-engine);  
    serial-number number;  
  }  
  preprovisioned;  
  traceoptions {  
    file filename <files number> <no-stamp> <replace> <size maximum-file-size>  
      <world-readable | no-world-readable>;  
    flag flag <disable>;  
  }  
}
```

[edit vlans] Hierarchy Level

```

vlans {
  vlan-name {
    description text-description;
    dot1q-tunnelling {
      customer-vlans (vlan-id | vlan-id-range);
    }
    filter {
      input filter-name;
      output filter-name;
    }
    l3-interface vlan.logical-interface-number;
    mac-limit number;
    mac-table-aging-time seconds;
    no-local-switching;
    primary-vlan vlan-id;
    vlan-id vlan-tag;
    vlan-range lower-vlan-id-higher-vlan-id;
  }
}

```


Part 3

Indexes

- Index on page 261
- Index of Supported Software Standards on page 263

Index

Symbols

#, comments in configuration statements.....xix
 (), in syntax descriptions.....xix
 < >, in syntax descriptions.....xix
 [], in configuration statements.....xix
 { }, in configuration statements.....xix
 | (pipe), in syntax descriptions.....xix

A

adaptive services
 supported software standards.....17
 ANSI standards supported *See* Index of Supported
 Software Standards
 ATM interfaces
 supported software standards.....20

B

BGP
 supported software standards.....33
 BOOTP
 supported software standards.....16
 braces, in configuration statements.....xix
 brackets
 angle, in syntax descriptions.....xix
 square, in configuration statements.....xix

C

CLI configuration mode command summary.....49
 comments, in configuration statements.....xix
 configuration statements, hierarchy.....51
 conventions
 text and syntax.....xviii
 curly braces, in configuration statements.....xix
 customer support.....xxvii
 contacting JTAC.....xxvii

D

data link switching *See* DLSw
 DHCP
 supported software standards.....16

DLSw

 supported software standards.....20
 documentation set
 comments on.....xxvi
 DTCP
 supported software standards.....17

E

ESO Consortium standards supported *See* Index of
 Supported Software Standards
 Ethernet
 supported software standards.....44

F

font conventions.....xviii
 Frame Relay interfaces
 supported software standards.....20
 FRF (MFA Forum) standards supported *See* Index of
 Supported Software Standards

G

GMPLS
 supported software standards.....36
 GR (Generic Requirements) standards supported *See*
 Index of Supported Software Standards
 GRE interfaces
 supported software standards.....21

I

IANA standards supported *See* Index of Supported
 Software Standards
 ICMP
 supported software standards.....33
 icons defined, notice.....xviii
 IEEE standards supported *See* Index of Supported
 Software Standards
 interface encapsulation
 supported software standards.....20
 Internet drafts supported *See* Index of Supported
 Software Standards
 IP multicast
 supported software standards.....34

IP-IP interfaces	
supported software standards.....	21
IPv6	
supported software standards.....	28
IS-IS	
supported software standards.....	30
ISO/IEC standards supported <i>See</i> Index of Supported Software Standards	
ITU-T Recommendations supported <i>See</i> Index of Supported Software Standards	

L

LDP	
supported software standards.....	36

M

manuals	
comments on.....	xxvi
MPLS	
supported software standards.....	37
MPLS applications	
supported software standards.....	35

N

neighbor discovery	
supported software standards.....	33
network management	
supported software standards.....	8
notice icons defined.....	xviii
NTP	
supported software standards.....	16

O

OSPF	
supported software standards.....	31

P

packet filters	
supported software standards.....	40
parentheses, in syntax descriptions.....	xix
policers	
supported software standards.....	41
PPP interfaces	
supported software standards.....	21

R

RFCs supported <i>See</i> Index of Supported Software Standards	
RIP	
supported software standards.....	32

RSVP	
supported software standards.....	38

S

SDH	
supported software standards.....	43
serial interfaces	
supported software standards.....	22
SONET	
supported software standards.....	43
support, technical <i>See</i> technical support	
syntax conventions.....	xviii
system access and access management	
supported software standards.....	15

T

T3 interfaces	
supported software standards.....	22
TCP/IPv4	
supported software standards.....	27
technical support	
contacting JTAC.....	xxvii
time synchronization	
supported software standards.....	16

V

VPNs	
supported software standards.....	42

Index of Supported Software Standards

A

ANSI T1.105-2001, Synchronous Optical Network (SONET) – Basic Description including Multiplex Structure, Rates, and Formats.....	43
ANSI T1.105.02-2001, Synchronous Optical Network (SONET) – Payload Mappings.....	43
ANSI T1.105.06-2002, Synchronous Optical Network (SONET): Physical Layer Specifications.....	43
ANSI T1.617-1991, Annex D, Additional Procedures for Permanent Virtual Connections (PVCs) Using Unnumbered Information Frames.....	20

E

ESO Consortium MIB.....	9
-------------------------	---

F

FRF.12, Frame Relay Fragmentation Implementation Agreement.....	20
FRF.15, End-to-End Multilink Frame Relay Implementation Agreement.....	20
FRF.16.1, Multilink Frame Relay UNI/NNI Implementation Agreement.....	21

G

GR-253-CORE, Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria.....	43
GR-499-CORE, Transport Systems Generic Requirements (TSGR): Common Requirements.....	43

I

IANA, IANAiftype Textual Convention MIB.....	9
IEEE 802.1Q, Virtual LANs.....	44
IEEE 802.3, Carrier Sense Multiple Access with Collision Detection (CSMA/CD).....	44
IEEE 802.3ad, Aggregation of Multiple Link Segments.....	9, 44
Internet draft draft-cavuto-dtcp-01.txt, DTCP: Dynamic Tasking Control Protocol.....	17
Internet draft draft-eastlake-sha2-02.txt, US Secure Hash Algorithms (SHA and HMAC-SHA).....	18
Internet draft draft-holbrook-idmr-igmpv3-ssm-07.txt, Using IGMPv3 and MLDv2 for Source-Specific Multicast.....	35
Internet draft draft-ietf-bfd-base-05.txt, Bidirectional Forwarding Detection.....	31
Internet draft draft-ietf-bfd-mib-02.txt, Bidirectional Forwarding Detection Management Information Base.....	13
Internet draft draft-ietf-bfd-mpls-02.txt, BFD for MPLS LSPs.....	37
Internet draft draft-ietf-ccamp-gmpls-routing-09.txt, Routing Extensions in Support of Generalized Multi-Protocol Label Switching.....	36
Internet draft draft-ietf-ccamp-gmpls-rsvp-te-ason-02.txt, Generalized MPLS (GMPLS) RSVP-TE Signalling in support of Automatically Switched Optical Network (ASON).....	36
Internet draft draft-ietf-ccamp-gmpls-sonet-sdh-08.txt, Generalized Multi-Protocol Label Switching Extensions for SONET and SDH Control.....	36
Internet draft draft-ietf-ccamp-imp-09.txt, Link Management Protocol (LMP).....	36
Internet draft draft-ietf-ccamp-ospf-gmpls-extensions-12.txt, OSPF Extensions in Support of Generalized Multi-Protocol Label Switching.....	32, 37

Internet draft draft-ietf-dhc-dhcpv6-16.txt, Dynamic Host Configuration Protocol for IPv6 (DHCPv6).....	30
Internet draft draft-ietf-idmr-dvmrp-v3-11.txt, Distance Vector Multicast Routing Protocol.....	35
Internet draft draft-ietf-idr-bgp4-mibv2-04.txt, Definitions of Managed Objects for the Fourth Version of Border Gateway Protocol (BGP-4), Second Version.....	14
Internet draft draft-ietf-idr-flow-spec-00.txt, Dissemination of flow specification rules.....	30, 34
Internet draft draft-ietf-isis-igp-p2p-over-lan-03.txt, Point-to-point operation over LAN in link-state routing protocols.....	32
Internet draft draft-ietf-isis-igp-p2p-over-lan-06.txt, Point-to-point operation over LAN in link-state routing protocols.....	31
Internet draft draft-ietf-isis-ipv6-06.txt, Routing IPv6 with IS-IS.....	30, 31
Internet draft draft-ietf-isis-wg-255adj-02.txt, Maintaining more than 255 circuits in IS-IS.....	31
Internet draft draft-ietf-isis-wg-mib-16.txt, Management Information Base for IS-IS.....	14
Internet draft draft-ietf-l3vpn-2547bis-mcast-02.txt, Multicast in MPLS/BGP IP VPNs.....	42
Internet draft draft-ietf-l3vpn-2547bis-mcast-bgp-03.txt, BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs.....	42
Internet draft draft-ietf-l3vpn-bgp-ipv6-07.txt, BGP-MPLS IP VPN extension for IPv6 VPN.....	30, 34
Internet draft draft-ietf-l3vpn-rfc2547bis-03.txt, BGP/MPLS IP VPNs.....	34
Internet draft draft-ietf-l3vpn-rfc2547bis-04.txt, BGP/MPLS IP VPNs.....	37
Internet draft draft-ietf-mboned-ssm232-08.txt, Source-Specific Protocol Independent Multicast in 232/8.....	35
Internet draft draft-ietf-mmusic-sap-00.txt, SAP: Session Announcement Protocol.....	35
Internet draft draft-ietf-mpls-bundle-04.txt, Link Bundling in MPLS Traffic Engineering.....	37
Internet draft draft-ietf-mpls-icmp-01.txt, ICMP Extensions for MultiProtocol [sic] Label Switching.....	37
Internet draft draft-ietf-mpls-label-encaps-07.txt, MPLS Label Stack Encoding.....	38
Internet draft draft-ietf-mpls-rsvp-lsp-fastreroute-03.txt, Fast Reroute Extensions to RSVP-TE for LSP Tunnels.....	38
Internet draft draft-ietf-mpls-rsvp-te-p2mp-01.txt, Extensions to RSVP-TE for Point to Multipoint TE LSPs.....	39
Internet draft draft-ietf-mpls-soft-preemption-00.txt, MPLS Traffic Engineering Soft preemption.....	38
Internet draft draft-ietf-msdp-mib-08.txt, Multicast Source Discovery protocol MIB.....	14
Internet draft draft-ietf-ngtrans-bgp-tunnel-04.txt, Connecting IPv6 Islands across IPv4 Clouds with BGP.....	30, 34
Internet draft draft-ietf-ospf-ospfv3-mib-11.txt, Management Information Base for OSPFv3.....	14
Internet draft draft-ietf-pim-sm-bsr-05.txt, Bootstrap Router (BSR) Mechanism for PIM.....	35
Internet draft draft-ietf-ppvpn-mpls-vpn-mib-05.txt, MPLS/BGP Virtual Private Network Management Information Base Using SMIPv2.....	14
Internet draft draft-ietf-ppvpn-rfc2547bis-00.txt, BGP/MPLS IP VPNs.....	34
Internet draft draft-ietf-ppvpn-rfc2547bis-03.txt, BGP/MPLS VPNs.....	38
Internet draft draft-ietf-ssm-arch-06.txt, Source-Specific Multicast for IP.....	35
Internet draft draft-kato-bgp-ipv6-link-local-00.txt, BGP4 + Peering Using IPv6 Link-local Address.....	30, 34
Internet draft draft-katz-ward-bfd-02.txt, Bidirectional Forwarding Detection.....	32
Internet draft draft-kompella-ppvpn-l2vpn-03.txt, Layer 2 VPNs Over Tunnels.....	42
Internet draft draft-marques-ppvpn-ibgp-00.txt, RFC2547bis networks using internal BGP as PE-CE protocol.....	42
Internet draft draft-martini-frame-encap-mpls-01.txt, Frame Relay Encapsulation over Pseudo-Wires.....	21
Internet draft draft-martini-l2circuit-encap-mpls-07.txt, Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks.....	38, 43
Internet draft draft-martini-l2circuit-trans-mpls-14.txt, Transport of Layer 2 Frames Over MPLS.....	38, 43
Internet draft draft-ooms-v6ops-bgp-tunnel-06.txt, Connecting IPv6 Islands over IPv4 MPLS using IPv6 Provider Edge Routers (6PE).....	30, 34
Internet draft draft-raggarwa-l3vpn-2547-mvpn-00.txt, Base Specification for Multicast in BGP/MPLS VPNs.....	35
Internet draft draft-raggarwa-mpls-p2mp-te-02.txt, Establishing Point to Multipoint MPLS TE LSPs.....	38
Internet draft draft-reeder-snmv3-usm-3desede-00.txt, Extension to the User-Based Security Model (USM) to Support Triple-DES EDE in "Outside" CBC Mode.....	14
Internet draft draft-rosen-vpn-mcast-06.txt, Multicast in MPLS/BGP VPNs.....	35
Internet draft draft-rosen-vpn-mcast-07.txt, Multicast in MPLS/BGP VPNs.....	35
ISO/IEC 10589, Information technology — Telecommunications and information exchange between systems — Intermediate System to Intermediate System intra-domain routeing [sic] information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473).....	30
ISO/IEC 8473, Information technology — Protocol for providing the connectionless-mode network service.....	30
ISO/IEC 9542, Information processing systems — Telecommunications and information exchange between systems — End system to Intermediate system routeing [sic] exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473).....	30

ITU Recommendation Q.933a: Additional procedures for Permanent Virtual Connection (PVC) status management (using Unnumbered Information frames).....	21
ITU-T Recommendation G.691, Optical interfaces for single channel STM-64 and other SDH systems with optical amplifiers.....	43
ITU-T Recommendation G.703, Physical/electrical characteristics of hierarchical digital interfaces.....	22
ITU-T Recommendation G.707, Network node interface for the synchronous digital hierarchy (SDH).....	43
ITU-T Recommendation G.783, Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks.....	43
ITU-T Recommendation G.813, Timing characteristics of SDH equipment slave clocks (SEC).....	43
ITU-T Recommendation G.825, The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH).....	44
ITU-T Recommendation G.826, Error performance parameters and objectives for international, constant bit-rate digital paths at or above the primary rate.....	44
ITU-T Recommendation G.831, Management capabilities of transport networks based on the synchronous digital hierarchy (SDH).....	44
ITU-T Recommendation G.957, Optical interfaces for equipments and systems relating to the synchronous digital hierarchy.....	44
ITU-T Recommendation G.958, Digital line systems based on the synchronous digital hierarchy for use on optical fibre cables.....	44
ITU-T Recommendation I.432, B-ISDN user-network interface – Physical layer specification.....	44
ITU-T Recommendation I.432.3, B-ISDN user-network interface - Physical layer specification: 1544 kbit/s and 2048 kbit/s operation.....	20
ITU-T Recommendation V.35, Data transmission at 48 kilobits per second using 60-108 kHz group band circuits.....	22
ITU-T Recommendation X.21, Interface between Data Terminal Equipment and Data Circuit-terminating Equipment for synchronous operation on public data networks.....	22

R

RFC 0768, User Datagram Protocol.....	27
RFC 0791, INTERNET PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION.....	27
RFC 0792, INTERNET CONTROL MESSAGE PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION.....	27, 40
RFC 0793, TRANSMISSION CONTROL PROTOCOL - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION.....	27
RFC 0826, An Ethernet Address Resolution Protocol.....	27
RFC 0854, TELNET PROTOCOL SPECIFICATION.....	28
RFC 0862, Echo Protocol.....	28
RFC 0863, Discard Protocol.....	28
RFC 0896, Congestion Control in IP/TCP Internetworks.....	28
RFC 0919, BROADCASTING INTERNET DATAGRAMS.....	28
RFC 0922, BROADCASTING INTERNET DATAGRAMS IN THE PRESENCE OF SUBNETS.....	28
RFC 0951, BOOTSTRAP PROTOCOL (BOOTP).....	16
RFC 0959, FILE TRANSFER PROTOCOL (FTP).....	28
RFC 1001, PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: CONCEPTS AND METHODS.....	16
RFC 1002, PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: DETAILED SPECIFICATIONS.....	16
RFC 1027, Using ARP to Implement Transparent Subnet Gateways.....	28
RFC 1035, DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION.....	16
RFC 1042, A Standard for the Transmission of IP Datagrams over IEEE 802 Networks.....	28
RFC 1058, Routing Information Protocol.....	32
RFC 1112, Host Extensions for IP Multicasting.....	34
RFC 1155, Structure and Identification of Management Information for TCP/IP-based Internets.....	9
RFC 1156, Management Information Base for Network Management of TCP/IP-based internets.....	9
RFC 1157, A Simple Network Management Protocol (SNMP).....	9, 28
RFC 1166, INTERNET NUMBERS.....	28
RFC 1195, Use of OSI IS-IS for Routing in TCP/IP and Dual Environments.....	9, 28, 30
RFC 1212, Concise MIB Definitions.....	9

RFC 1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II.....	10, 28
RFC 1215, A Convention for Defining Traps for use with the SNMP.....	10, 29
RFC 1256, ICMP Router Discovery Messages.....	28, 33
RFC 1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis.....	16, 28
RFC 1319, The MD2 Message-Digest Algorithm.....	16
RFC 1321, The MD5 Message-Digest Algorithm.....	16
RFC 1332, The PPP Internet Protocol Control Protocol (IPCP).....	21
RFC 1334, PPP Authentication Protocols.....	21
RFC 1406, Definitions of Managed Objects for the DS1 and E1 Interface Types.....	10
RFC 1407, Definitions of Managed Objects for the DS3/E3 Interface Type.....	10
RFC 1472, The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol.....	10
RFC 1473, The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol.....	10
RFC 1483, Multiprotocol Encapsulation over ATM Adaptation Layer 5.....	20
RFC 1490 <i>See</i> RFC 2427	
RFC 1492, An Access Control Protocol, Sometimes Called TACACS.....	15
RFC 1519, Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy.....	28
RFC 1534, Interoperation Between DHCP and BOOTP.....	16
RFC 1583, OSPF Version 2.....	31
RFC 1587, The OSPF NSSA Option.....	31
RFC 1619, PPP over SONET/SDH.....	44
RFC 1631, The IP Network Address Translator (NAT).....	19
RFC 1657, Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2.....	10
RFC 1661, The Point-to-Point Protocol (PPP).....	21
RFC 1662, PPP in HDLC-like Framing.....	21
RFC 1695, Definitions of Managed Objects for ATM Management Version 8.0 using SMIv2.....	10
RFC 1700, ASSIGNED NUMBERS.....	16
RFC 1701, Generic Routing Encapsulation (GRE).....	21
RFC 1702, Generic Routing Encapsulation over IPv4 networks.....	21
RFC 1717, The PPP Multilink Protocol (MP).....	21
RFC 1724, RIP Version 2 MIB Extension.....	10
RFC 1745, BGP4/IDRP for IP—OSPF Interaction.....	33
RFC 1771, A Border Gateway Protocol 4 (BGP-4).....	29
RFC 1772, Application of the Border Gateway Protocol in the Internet.....	29, 33
RFC 1793, Extending OSPF to Support Demand Circuits.....	31
RFC 1795, Data Link Switching: Switch-to-Switch Protocol AIW DLSw RIG: DLSw Closed Pages, DLSw Standard Version 1.0.....	20
RFC 1812, Requirements for IP Version 4 Routers.....	28
RFC 1850, OSPF Version 2 Management Information Base.....	10
RFC 1877, PPP Internet Protocol Control Protocol Extensions for Name Server Addresses.....	21
RFC 1878, Variable Length Subnet Table For IPv4.....	28
RFC 1901, Introduction to Community-based SNMPv2.....	10, 29
RFC 1902, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2).....	29
RFC 1905, Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2).....	10, 29
RFC 1907, Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2).....	10
RFC 1918, Address Allocation for Private Internets.....	42
RFC 1948, Defending Against Sequence Number Attacks.....	28
RFC 1965, Autonomous System Confederations for BGP.....	33
RFC 1966, BGP Route Reflection—An alternative to full mesh IBGP.....	33
RFC 1973, PPP in Frame Relay.....	21
RFC 1981, Path MTU Discovery for IP version 6.....	29
RFC 1989, PPP Link Quality Monitoring.....	21
RFC 1990, The PPP Multilink Protocol (MP).....	19, 21
RFC 1994, PPP Challenge Handshake Authentication Protocol (CHAP).....	16
RFC 1997, BGP Communities Attribute.....	33

RFC 2003, IP Encapsulation within IP.....	21
RFC 2011, SNMPv2 Management Information Base for the Internet Protocol using SMIv2.....	10
RFC 2012, SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2.....	11
RFC 2013, SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2.....	11
RFC 2024, Definitions of Managed Objects for Data Link Switching using SMIv2.....	11
RFC 2080, RIPng for IPv6.....	29, 32
RFC 2081, RIPng Protocol Applicability Statement.....	29, 32
RFC 2082, RIP-2 MD5 Authentication.....	33
RFC 2085, HMAC-MD5 IP Authentication with Replay Prevention.....	18
RFC 2096, IP Forwarding Table MIB.....	11
RFC 2104, HMAC: Keyed-Hashing for Message Authentication.....	30
RFC 2115, Management Information Base for Frame Relay DTEs Using SMIv2.....	11
RFC 2131, Dynamic Host Configuration Protocol.....	17
RFC 2132, DHCP Options and BOOTP Vendor Extensions.....	17
RFC 2153, PPP Vendor Extensions.....	21
RFC 2166, APPN Implementer's Workshop Closed Pages Document—DLSw v2.0 Enhancements.....	20
RFC 2205, Resource ReSerVation Protocol (RSVP)—Version 1 Functional Specification.....	38
RFC 2209, Resource ReSerVation Protocol (RSVP)—Version 1 Message Processing Rules.....	38
RFC 2210, The Use of RSVP with IETF Integrated Services.....	38
RFC 2211, Specification of the Controlled-Load Network Element Service.....	38
RFC 2212, Specification of Guaranteed Quality of Service.....	38
RFC 2215, General Characterization Parameters for Integrated Service Network Elements.....	38
RFC 2216, Network Element Service Specification Template.....	38
RFC 2225, Classical IP and ARP over ATM.....	20
RFC 2233, The Interfaces Group MIB using SMIv2.....	11
RFC 2236, Internet Group Management Protocol, Version 2.....	34
RFC 2246, The TLS Protocol Version 1.0.....	16
RFC 2270, Using a Dedicated AS for Sites Homed to a Single Provider.....	33
RFC 2283, Multiprotocol Extensions for BGP-4.....	29, 33, 42
RFC 2287, Definitions of System-Level Managed Objects for Applications.....	11
RFC 2327, SDP: Session Description Protocol.....	34
RFC 2328, OSPF Version 2.....	31
RFC 2338, Virtual Router Redundancy Protocol.....	28
RFC 2362, Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification.....	34
RFC 2364, PPP Over AAL5.....	19, 21
RFC 2365, Administratively Scoped IP Multicast.....	34
RFC 2370, The OSPF Opaque LSA Option.....	32
RFC 2373, IP Version 6 Addressing Architecture.....	29
RFC 2385, Protection of BGP Sessions via the TCP MD5 Signature Option.....	33
RFC 2401, Security Architecture for the Internet Protocol.....	18
RFC 2402, IP Authentication Header.....	18
RFC 2403, The Use of HMAC-MD5-96 within ESP and AH.....	18
RFC 2404, The Use of HMAC-SHA-1-96 within ESP and AH.....	18
RFC 2405, The ESP DES-CBC Cipher Algorithm With Explicit IV.....	18
RFC 2406, IP Encapsulating Security Payload (ESP).....	18
RFC 2407, The Internet IP Security Domain of Interpretation for ISAKMP.....	18
RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP).....	18
RFC 2409, The Internet Key Exchange (IKE).....	18
RFC 2410, The NULL Encryption Algorithm and Its Use With IPsec [sic].....	18
RFC 2412, The OAKLEY Key Determination Protocol.....	18
RFC 2427, Multiprotocol Interconnect over Frame Relay.....	21
RFC 2439, BGP Route Flap Damping.....	33
RFC 2453, RIP Version 2.....	33
RFC 2460, Internet Protocol, Version 6 (IPv6) Specification.....	29, 40
RFC 2461, Neighbor Discovery for IP Version 6 (IPv6).....	29, 33
RFC 2462, IPv6 Stateless Address Autoconfiguration.....	29, 33

RFC 2463, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification.....	29, 33
RFC 2464, Transmission of IPv6 Packets over Ethernet Networks.....	29
RFC 2465, Management Information Base for IP Version 6: Textual Conventions and General Group.....	11
RFC 2466, Management Information Base for IP Version 6: ICMPv6 Group.....	11
RFC 2472, IP Version 6 over PPP.....	29
RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.....	17, 25, 29, 40
RFC 2475, An Architecture for Differentiated Services.....	17, 25, 40
RFC 2491, IPv6 Over Non-Broadcast Multiple Access (NBMA) networks.....	29
RFC 2492, IPv6 over ATM Networks.....	29
RFC 2495, Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types.....	11
RFC 2496, Definitions of Managed Objects for the DS3/E3 Interface Type.....	11
RFC 2508, Compressing IP/UDP/RTP Headers for Low-Speed Serial Links.....	19
RFC 2509, IP Header Compression over PPP.....	19
RFC 2515, Definitions of Managed Objects for ATM Management.....	11
RFC 2526, Reserved IPv6 Subnet Anycast Addresses.....	29
RFC 2545, Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing.....	29, 33
RFC 2547, BGP/MPLS VPNs.....	21, 34, 37
RFC 2558, Definitions of Managed Objects for the SONET/SDH Interface Type.....	11
RFC 2570, Introduction to Version 3 of the Internet-standard Network Management Framework.....	11
RFC 2571, An Architecture for Describing SNMP Management Frameworks.....	11
RFC 2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP).....	11
RFC 2576, Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework.....	11
RFC 2578, Structure of Management Information Version 2 (SMIv2).....	11, 29
RFC 2579, Textual Conventions for SMIv2.....	11
RFC 2580, Conformance Statements for SMIv2.....	12
RFC 2590, Transmission of IPv6 Packets over Frame Relay Networks Specification.....	21
RFC 2597, Assured Forwarding PHB Group.....	25, 41
RFC 2598, An Expedited Forwarding PHB.....	25, 41
RFC 2615, PPP over SONET/SDH.....	22
RFC 2661, Layer Two Tunneling Protocol "L2TP".....	18
RFC 2662, Definitions of Managed Objects for the ADSL Lines.....	12
RFC 2663, IP Network Address Translator (NAT) Terminology and Considerations.....	19
RFC 2665, Definitions of Managed Objects for the Ethernet-like Interface Types.....	12
RFC 2667, IP Tunnel MIB.....	12
RFC 2675, IPv6 Jumbograms.....	29
RFC 2684, Multiprotocol Encapsulation over ATM Adaptation Layer 5.....	20
RFC 2685, Virtual Private Networks Identifier.....	42
RFC 2686, The Multi-Class Extension to Multi-Link PPP.....	19, 22
RFC 2697, A Single Rate Three Color Marker.....	25
RFC 2698, A Two Rate Three Color Marker.....	23, 25, 41
RFC 2702, Requirements for Traffic Engineering Over MPLS.....	37
RFC 2710, Multicast Listener Discovery (MLD) for IPv6.....	34
RFC 2711, IPv6 Router Alert Option.....	29
RFC 2740, OSPF for IPv6.....	30, 32
RFC 2745, RSVP Diagnostic Messages.....	38
RFC 2747, RSVP Cryptographic Authentication.....	38
RFC 2763, Dynamic Hostname Exchange Mechanism for IS-IS.....	30
RFC 2767, Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS).....	30
RFC 2784, Generic Routing Encapsulation (GRE).....	21
RFC 2787, Definitions of Managed Objects for the Virtual Router Redundancy Protocol.....	12
RFC 2790, Host Resources MIB.....	12
RFC 2796, BGP Route Reflection – An Alternative to Full Mesh IBGP.....	33
RFC 2819, Remote Network Monitoring Management Information Base.....	12
RFC 2858, Multiprotocol Extensions for BGP-4.....	33, 34, 37, 42
RFC 2863, The Interfaces Group MIB.....	12

RFC 2864, The Inverted Stack Table Extension to the Interfaces Group MIB.....	12
RFC 2865, Remote Authentication Dial In User Service (RADIUS).....	15
RFC 2866, RADIUS Accounting.....	15, 18
RFC 2869, RADIUS Extensions.....	16
RFC 2873, TCP Processing of the IPv4 Precedence Field.....	28
RFC 2878, PPP Bridging Control Protocol (BCP).....	30
RFC 2890, Key and Sequence Number Extensions to GRE.....	21
RFC 2893, Transition Mechanisms for IPv6 Hosts and Routers.....	30
RFC 2918, Route Refresh Capability for BGP-4.....	33
RFC 2925, Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations.....	12, 19
RFC 2932, IPv4 Multicast Routing MIB.....	12
RFC 2933, Internet Group Management Protocol MIB.....	12
RFC 2934, Protocol Independent Multicast MIB for IPv4.....	12
RFC 2961, RSVP Refresh Overhead Reduction Extensions.....	38
RFC 2966, Domain-wide Prefix Distribution with Two-Level IS-IS.....	30
RFC 2973, IS-IS Mesh Groups.....	31
RFC 2974, Session Announcement Protocol.....	34
RFC 2981, Event MIB.....	12
RFC 3014, Notification Log MIB.....	12
RFC 3019, IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol.....	12
RFC 3021, Using 31-Bit Prefixes on IPv4 Point-to-Point Links.....	28
RFC 3022, Traditional IP Network Address Translator (Traditional NAT).....	19
RFC 3031, Multiprotocol Label Switching Architecture.....	34, 37
RFC 3032, MPLS Label Stack Encoding.....	37
RFC 3036, LDP Specification.....	36
RFC 3046, DHCP Relay Agent Information Option.....	17
RFC 3063, MPLS Loop Prevention Mechanism.....	37
RFC 3065, Autonomous System Confederations for BGP.....	33
RFC 3097, RSVP Cryptographic Authentication—Updated Message Type Value.....	38
RFC 3101, The OSPF Not-So-Stubby Area (NSSA) Option.....	32
RFC 3107, Carrying Label Information in BGP-4.....	33, 42
RFC 3137, OSPF Stub Router Advertisement.....	32
RFC 3140, Per Hop Behavior Identification Codes.....	37
RFC 3208, PGM Reliable Transport Protocol Specification.....	34, 37
RFC 3209, RSVP-TE: Extensions to RSVP for LSP Tunnels.....	39
RFC 3212, Constraint-Based LSP Setup using LDP.....	36
RFC 3215, LDP State Machine.....	36
RFC 3246, An Expedited Forwarding PHB (Per-Hop Behavior).....	28
RFC 3270, Multi-Protocol Label Switching (MPLS) Support of Differentiated Services.....	37
RFC 3277, Intermediate System to Intermediate System (IS-IS) Transient Blackhole Avoidance.....	31
RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.....	16
RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6).....	17
RFC 3358, Optional Checksums in Intermediate System to Intermediate System (ISIS).....	31
RFC 3359, Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System.....	31
RFC 3373, Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies.....	31
RFC 3376, Internet Group Management Protocol, Version 3.....	35
RFC 3392, Capabilities Advertisement with BGP-4.....	33
RFC 3397, Dynamic Host Configuration Protocol (DHCP) Domain Search Option.....	17
RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.....	12
RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP).....	12
RFC 3413, Simple Network Management Protocol (SNMP) Applications.....	12
RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).....	12
RFC 3415, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).....	12
RFC 3416, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP).....	13
RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP).....	13
RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP).....	13

RFC 3443, Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks.....	37
RFC 3446, Anycast Rendevous [sic] Point (RP) Mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP).....	35
RFC 3469, Framework for Multi-Protocol Label Switching (MPLS)-based Recovery.....	37
RFC 3471, Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description.....	36
RFC 3473, Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation [sic] Protocol-Traffic Engineering (RSVP-TE) Extensions.....	36, 39
RFC 3477, Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE).....	39
RFC 3478, Graceful Restart Mechanism for Label Distribution Protocol.....	36
RFC 3484, Default Address Selection for Internet Protocol version 6 (IPv6).....	30
RFC 3498, Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures.....	13
RFC 3509, Alternative Implementations of OSPF Area Border Routers.....	32
RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture.....	30
RFC 3515, The Session Initiation Protocol (SIP) Refer Method.....	30
RFC 3564, Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering.....	37
RFC 3567, Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication.....	31
RFC 3569, An Overview of Source-Specific Multicast (SSM).....	35
RFC 3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS).....	16
RFC 3590, Source Address Selection for the Multicast Listener Discovery (MLD) Protocol.....	35
RFC 3592, Definitions of Managed Objects for the Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) Interface Type.....	13
RFC 3602, The AES-CBC Cipher Algorithm and Its Use with IPsec [sic].....	18
RFC 3618, Multicast Source Discovery Protocol (MSDP).....	35
RFC 3623, Graceful OSPF Restart.....	32
RFC 3630, Traffic Engineering (TE) Extensions to OSPF Version 2.....	32
RFC 3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers.....	18
RFC 3768, Virtual Router Redundancy Protocol (VRRP).....	30
RFC 3784, Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE).....	31
RFC 3787, Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS).....	31
RFC 3811, Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management.....	13
RFC 3812, Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB).....	13
RFC 3813, Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB).....	13
RFC 3815, Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP).....	13
RFC 3826, The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model.....	13
RFC 3847, Restart Signaling for Intermediate System to Intermediate System (IS-IS).....	31
RFC 3925, Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4).....	17
RFC 3954, Cisco Systems NetFlow Services Export Version 9.....	17
RFC 3973, Protocol Independent Multicast – Dense Mode (PIM-DM): Protocol Specification (Revised).....	35
RFC 4090, Fast Reroute Extensions to RSVP-TE for LSP Tunnels.....	39
RFC 4124, Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering.....	37
RFC 4125, Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering.....	37, 39
RFC 4127, Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering.....	37, 39
RFC 4203, OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS).....	32
RFC 4205, Intermediate System to Intermediate System (IS-IS) Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS).....	31
RFC 4206, Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE).....	36
RFC 4271, A Border Gateway Protocol 4 (BGP-4).....	33
RFC 4360, BGP Extended Communities Attribute.....	34
RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs).....	34, 42
RFC 4379, Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures.....	37, 42
RFC 4444, Management Information Base for Intermediate System to Intermediate System (IS-IS).....	13
RFC 4456, BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP).....	34

RFC 4552, Authentication/Confidentiality for OSPFv3.....	32
RFC 4576, Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs).....	32, 42
RFC 4577, OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs).....	32, 42
RFC 4601, Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification (Revised).....	35
RFC 4659, BGP/MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN.....	42
RFC 4684, Constrained Route Distribution for Border Gateway Protocol/MultiProtocol [sic] Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs).....	42
RFC 4724, Graceful Restart Mechanism for BGP.....	34
RFC 4741, NETCONF Configuration Protocol.....	8
RFC 4742, Using the NETCONF Configuration Protocol over Secure SHell (SSH).....	8
RFC 4761, Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling.....	43
RFC 4762, Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling.....	43
RFC 4781, Graceful Restart Mechanism for BGP with MPLS.....	34
RFC 4893, BGP Support for Four-octet AS Number Space.....	34
RFC 4915, Multi-Topology Routing (MT) in OSPF.....	32
RFC 5120, M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs).....	31
RFC 5130, A Policy Control Mechanism in IS-IS Using Administrative Tags.....	31

