



**JUNOS[™]e Software
for E Series[™] Broadband Services Routers**

Command Reference A to M

Release 11.1.x

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

Published: 2010-04-09

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.

JUNOSe™ Software for E Series™ Broadband Services Routers Command Reference Guide A to M
Release 11.1.x

Copyright © 2010, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Writing: Subash Babu Asokan, Krupa Chandrashekar, Megha Shaseendran, Pallavi Madhusudhan, Namrata Metha, Mark Barnard, Diane Florio, Bruce Gillham, Sarah Lesway-Ball, Brian Wesley Simmons, Fran Singer, Chander Aima, Poornima Goswami, Hema Priya J, Sairam Venugopalan

Editing: Benjamin Mann

Illustration: Nathaniel Woodward

Cover Design: Edmonds Design

Revision History

April 2010—FRS JUNOSe 11.1.x

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 the Documentation	xxxix
-------------------------	-------

Part 1

Commands, A to M

Chapter 1	Command Reference Topics	3
Chapter 2	A Commands	21
Chapter 3	B Commands	211
Chapter 4	C Commands	349
Chapter 5	D Commands	475
Chapter 6	E Commands	555
Chapter 7	F Commands	625
Chapter 8	G Commands	663
Chapter 9	H Commands	679
Chapter 10	I Commands	695
Chapter 11	K Commands	1145
Chapter 12	L Commands	1149
Chapter 13	M Commands	1261

Part 2

Index

Index	1445
-------	------

Table of Contents

	About the Documentation	xxxix
	E Series and JUNOS ^e Documentation and Release Notes	xxxix
	Audience	xxxix
	E Series and JUNOS ^e Text and Syntax Conventions	xxxix
	Obtaining Documentation	xli
	Documentation Feedback	xli
	Requesting Technical Support	xli
	Self-Help Online Tools and Resources	xl ii
	Opening a Case with JTAC	xl ii
Part 1	Commands, A to M	
Chapter 1	Command Reference Topics	3
	Using the no Version Versus the default Version of Commands	3
	Deprecated Commands	4
	Filtering show Commands	4
	Interface Types and Specifiers	5
Chapter 2	A Commands	21
	aaa accounting acct-stop on-aaa-failure	22
	aaa accounting acct-stop on-access-deny	23
	aaa accounting broadcast	24
	aaa accounting commands	25
	aaa accounting default	26
	aaa accounting duplication	27
	aaa accounting exec	28
	aaa accounting immediate-update	29
	aaa accounting interval	30
	aaa accounting statistics	31
	aaa accounting suppress null-username	32
	aaa accounting vr-group	33
	aaa authentication default	34
	aaa authentication enable default	35
	aaa authentication login	36
	aaa authorization	37
	aaa authorization config-commands	38

aaa delimiter	39
aaa dhcpv6-delegated-prefix delegated-ipv6-prefix	40
aaa dns	41
aaa domain-map	42
aaa duplicate-address-check	43
aaa intf-desc-format include	44
aaa ipv6-dns	45
aaa ipv6-nd-ra-prefix framed-ipv6-prefix	46
aaa local database	47
aaa local select database	48
aaa local username	49
aaa new-model	50
aaa parse-direction	51
aaa parse-order	52
aaa profile	53
aaa qos downstream-rate	54
aaa route-download	55
aaa route-download now	56
aaa route-download suspend	57
aaa service accounting interval	58
aaa subscriber limit per-port	59
aaa subscriber limit per-vr	60
aaa timeout	61
aaa tunnel assignment-id-format	62
aaa tunnel calling-number-format	63
aaa tunnel calling-number-format-fallback	66
aaa tunnel client-name	68
aaa tunnel-group	69
aaa tunnel ignore	70
aaa tunnel nas-port-method	71
aaa tunnel password	72
aaa tunnel switch-profile	73
aaa tunnel tx-connect-speed-method	74
aaa user accounting interval	75
aaa virtual-router	76
aaa wins	77
access-class in	78
access-list	79
accounting	80
adapter accept	81
adapter disable	82
adapter enable	83
adapter erase	84
address	85
address area	86
address authentication key	87
address authentication-key	88
address authentication message-digest	89
address authentication mode	90
address authentication-none	91
address bfd-liveness-detection	92

address cost	93
address dead-interval	94
address-family	95
address hello-interval	97
address message-digest-key md5	98
address network	99
address passive-interface	100
address-pool-name	101
address priority	102
address receive version	103
address retransmit-interval	104
address send version	105
address transmit-delay	106
adjustment-factor	107
agent context-name	108
aggregate-address	109
aggregation-node	110
aggressive-mode	111
allow	112
append-after	113
application	114
aps events	115
aps force	116
aps group	117
aps lockout	118
aps manual	119
aps protect	120
aps revert	121
aps unidirectional	122
aps working	123
area	124
area-authentication	125
area-authentication-key	126
area default-cost	127
area-message-digest-key	128
area nssa	130
area range	131
area stub	132
area virtual-link	133
area virtual-link authentication-key	134
area virtual-link authentication message-digest	135
area virtual-link authentication-none	136
area virtual-link dead-interval	137
area virtual-link hello-interval	138
area virtual-link message-digest-key md5	139
area virtual-link retransmit-interval	140
area virtual-link transmit-delay	141
arp	142
arp spoof-check	144
arp timeout	145
assured-rate	146

atm	147
atm aal5 description	148
atm aal5 shutdown	149
atm aal5 snmp trap link-status	150
atm atm1483 advisory-rx-speed	151
atm atm1483 auto-configure	152
atm atm1483 description	153
atm atm1483 export-subinterface-description	154
atm atm1483 mtu	155
atm atm1483 profile	156
atm atm1483 shutdown	157
atm atm1483 snmp trap link-status	158
atm atm1483 subscriber	159
atm auto-configuration	160
atm bulk-config	161
atm bulk-config modify	162
atm bulk-config shutdown	163
atm cac	164
atm cell-packing	165
atm-cell-mode	166
atm classifier-list	167
atm class-vc	168
atm clock internal	169
atm description	170
atm dos-protection-group	171
atm framing	172
atm ilmi-enable	173
atm ilmi-keepalive	174
atm lbo	175
atm mcpt-timers	176
atm oam	177
atm oam flush	178
atm oam loopback-location	179
atm policy	180
atm policy-list	181
atm pvc	182
atm shutdown	185
atm snmp trap link-status	186
atm sonet stm-1	187
atm uni-version	188
atm vc-per-vp	189
atm vp-description	190
atm-vp qos-parameter	191
atm-vp qos-profile	192
atm vp-tunnel	193
authentication	194
authentication key	195
authentication-key	196
authentication message-digest	197
authentication mode	198
authentication-none	199

authorization	200
authorization change	201
auth-router-name	202
auto-configure	203
auto-configure atm1483	204
auto-configure vlan	205
auto-cost reference-bandwidth	206
automatic-virtual-link	207
auto-summary	208
average-length-exponent	209
avp	210

Chapter 3

B Commands 211

backup-address-pool-name	212
bandwidth	213
bandwidth oversubscription	214
banner	215
baseline aaa	216
baseline aaa route-download	217
baseline atm vp interface	218
baseline bridge	219
baseline bridge interface	220
baseline bridge interface vpls	221
baseline clns	222
baseline cops	223
baseline dhcp	224
baseline frame-relay interface	225
baseline frame-relay multilinkinterface	226
baseline hdlc interface	227
baseline interface	228
baseline ip	229
baseline ip bgp	230
baseline ip dhcp-external	231
baseline ip dhcp-local	232
baseline ip dvmrp	233
baseline ip http	234
baseline ip igmp	235
baseline ip igmp-proxy interface	236
baseline ip interface	237
baseline ip mobile home-agent	238
baseline ip nat	239
baseline ip ospf	240
baseline ip rip	241
baseline ip tunnel-reassembly	242
baseline ip udp	243
baseline ip vrrp	244
baseline ipv6	245
baseline ipv6 dhcpv6-local	246
baseline ipv6 interface	247

baseline ipv6 local pool	248
baseline ipv6 mld	249
baseline ipv6 mld-proxy interface	250
baseline ipv6 ospf	251
baseline ipv6 tcp	252
baseline line interface sonet	253
baseline local pool	254
baseline log	255
baseline mpls interface	256
baseline mpls label	257
baseline mpls next-hop	258
baseline mpls tunnel	259
baseline path interface sonet	260
baseline ppp interface	261
baseline pppoe interface	262
baseline radius	263
baseline radius dynamic-request	264
baseline radius relay	265
baseline section interface sonet	266
baseline show-delta-counts	267
baseline snmp	268
baseline ssc	269
baseline suspicious-control-flow-detection counts	270
baseline tacacs	271
baseline tcp	272
bert	273
bfd adapt	274
bgp advertise-best-external-to-internal	275
bgp advertise-inactive	276
bgp always-compare-med	277
bgp bestpath med confed	278
bgp bestpath missing-as-worst	279
bgp client-to-client reflection	280
bgp cluster-id	281
bgp confederation identifier	282
bgp confederation peers	283
bgp dampening	284
bgp default ipv4-unicast	285
bgp default local-preference	286
bgp default route-target filter	287
bgp enforce-first-as	288
bgp fast-external-fallover	289
bgp graceful-restart	290
bgp graceful-restart path-selection-defer-time-limit	291
bgp graceful-restart restart-time	292
bgp graceful-restart stalepaths-time	293
bgp log-neighbor-changes	294
bgp maxas-limit	295
bgp redistribute-internal	296
bgp router-id	297
bgp shutdown	298

bgp wait-on-end-of-rib	299
boolean-test	300
boot backup	301
boot config	302
boot force-backup	303
boot hotfix	304
boot revert-tolerance	305
boot revert-tolerance never	306
boot subsystem	307
boot system	308
bridge1483 dos-protection-group	309
bridge1483 mtu	310
bridge1483 service-profile	311
bridge	312
bridge acquire	313
bridge address	314
bridge aging-time	316
bridge crb	317
bridge-group	318
bridge learn	319
bridge route	320
bridge snmp-trap link-status	321
bridge subscriber-policy	322
bridge vpls rd	323
bridge vpls route-target	325
bridge vpls site-name site-id	327
bridge vpls site-range	328
bridge vpls transport-virtual-router	329
broadcast	330
buffer-weight	331
bulkstats	332
bulkstats collector	333
bulkstats file-format endOfLine-LF	334
bulkstats interfaces description-format common	335
bulkstats interfaces rfc1213	336
bulkstats interface-type	337
bulkstats receiver remote-name	338
bulkstats schema	339
bulkstats schema subtree	340
bulkstats schema subtree policy	341
bulkstats schema subtree qos	342
bulkstats traps	344
bulkstats virtual-router-group	345
bundled-group-id	346
bundled-group-id-overrides-mlppp-ed	347

Chapter 4**C Commands****349**

cache entries	350
cache timeout	351

cablelength	352
cbr	353
channelized	354
check-disk	355
check-vpn-next-hops	356
classifier-group	357
class-int	359
class-vc	360
cleanup-timeout-factor	361
clear access-list	362
clear arp	363
clear bfd adapted-intervals	364
clear bfd session	365
clear bgp ipv6	366
clear bgp ipv6 dampening	367
clear bgp ipv6 dynamic-peers	369
clear bgp ipv6 redistribution	370
clear bgp ipv6 wait-end-of-rib	371
clear bridge	372
clear bridge address	373
clear bridge interface	374
clear bridge interface vpls	375
clear egress-queue	376
clear fabric-queue	377
clear ip bgp	378
clear ip bgp dampening	380
clear ip bgp dynamic-peers	382
clear ip bgp redistribution	383
clear ip bgp wait-end-of-rib	384
clear ip demux	385
clear ip dhcp-local binding	386
clear ip dvmrp routes	387
clear ip flow stats	388
clear ip interface	389
clear ip isis redistribution	390
clear ip mobile binding	391
clear ip mroute	392
clear ip nat translation	393
clear ip ospf database	395
clear ip ospf neighbor	396
clear ip ospf redistribution	397
clear ip pim auto-rp	398
clear ip pim interface count	399
clear ip pim remote-neighbor count	400
clear ip prefix-list	401
clear ip prefix-tree	402
clear ip rip dynamic-interfaces	403
clear ip rip redistribution	404
clear ip routes	405
clear ip routes download	406
clear ip tunnel-routes	407

clear ipv6 access-list	408
clear ipv6 bfd session	409
clear ipv6 interface	410
clear ipv6 mroute	411
clear ipv6 neighbors	412
clear ipv6 ospf counters	413
clear ipv6 ospf process	414
clear ipv6 ospf redistribution	415
clear ipv6 pim interface	416
clear ipv6 pim remote-neighbor	417
clear ipv6 prefix-list	418
clear ipv6 routes	419
clear ipv6 tunnel-routes	420
clear isis adjacency	421
clear isis database	422
clear isis ipv6 redistribution	423
clear l2c discovery-table	424
clear l2c neighbor	425
clear line	426
clear mirror log	427
clear mpls dynamic-interfaces on-major-interfaces	428
clear mpls ldp	429
clear redundancy history	430
clear rsvp authentication	431
clear suspicious-control-flow-detection	432
client-name	433
clns configuration-time	434
clns holding-time	435
clns host	436
clock set	437
clock source	438
clock summer-time date	439
clock summer-time recurring	440
clock timezone	441
color	442
color-aware	443
color-mark-profile	444
committed-action	445
committed-burst	446
committed-drop-threshold	447
committed-length	448
committed-rate	449
committed-threshold	450
common-name	451
configure	452
confirmations explicit	453
conformed-action	454
conformed-drop-threshold	455
conformed-fraction	456
conformed-length	457
conformed-threshold	458

control-plane	459
controlled-interface-type	460
controller e3	461
controller sonet	462
controller t3	463
convergence-factor	464
copy	465
copy running-configuration	467
copy running-configuration startup-configuration	468
copy startup-configuration	469
cost	470
country	471
crc	472
crl	473
crypto key dss	474

Chapter 5**D Commands 475**

data-character-bits	476
dead-interval	477
deadtime	478
debounce	479
debounce-interval	480
debounce-time	481
debug ip bgp	482
debug ip mbgp	484
debug ip ospf	486
debug ip pim	488
debug ip rip	490
debug ipv6 ospf	491
debug ipv6 pim	493
debug isis	495
default-fields peer	497
default-fields route	499
default-information originate	501
default-metric	503
default-router	504
default-upper-type mlppp	505
delete	506
delta-sampling	507
deny	508
description	509
dhcp delete-binding	510
dhcp-external delete-binding	513
dhcp-external duplicate-mac-address	514
dhcpv6 delete-binding	515
diag	516
diag-level	517
dir	518
disable	519

disable-autosync	520
disable-dynamic-redistribute	521
disable-incremental-external-spf	522
disable proxy lcp	523
disable-switch-on-error	524
disconnect-cause	525
disconnect ssh	526
discovery-mode	527
distance	528
distance bgp	529
distance ip	530
distribute-domain-wide	531
distribute-list	532
dns-domain-search	533
dns-server	534
dns-server (for IPv6)	535
do	536
domain	537
domain-authentication	538
domain-authentication-key	539
domain-id	540
domain-message-digest-key	541
domain-name	543
domain-suffix	544
domain-tag	545
dont-install-routes	546
dos-protection-group	547
drop-profile	548
ds3-scrumble	549
dsr-detect	550
dsu bandwidth	551
dsu mode	552
duplex	553
dvmrp destination profile	554

Chapter 6**E Commands 555**

e3-scrumble	556
enable	557
enabled	558
enable ipsec-transport	559
enable password	560
enable proxy authenticate	561
enable secret	562
encapsulation	563
encapsulation bridge1483	564
encapsulation frame-relay ietf	565
encapsulation hdlc	566
encapsulation mlframe-relay ietf	567
encapsulation mlppp	568

encapsulation ppp	569
encapsulation pppoe	570
encapsulation vlan	571
encryption	572
end	573
enrollment retry-limit	574
enrollment retry-period	575
enrollment url	576
equipment loopback	577
erase secrets	578
ethernet description	579
ethernet dos-protection-group	580
ethernet oam lfm	581
ethernet oam lfm high-threshold	582
ethernet oam lfm link-monitor frame-seconds	583
ethernet oam lfm link-monitor frame-seconds-summary	585
ethernet oam lfm link-monitor symbol-period	587
ethernet oam lfm mode	589
ethernet oam lfm pdu-lost-threshold	590
ethernet oam lfm pdu-transmit-interval	591
ethernet oam lfm remote-failure	592
ethernet oam lfm remote-loopback	594
ethernet oam lfm remote-loopback supported	595
event	596
exceeded-action	597
exceeded-drop-threshold	598
exceeded-fraction	599
exceeded-length	600
exceeded-threshold	601
exception dump	602
exception gateway	603
exception http-redirect	604
exception monitor	605
exception monitor interval	606
exception protocol ftp	607
exception source	608
excess-burst	609
exclude-prefix	610
exclude-subsystem	611
exec-banner	612
exec-timeout	613
existence-test	614
exit	615
exit-address-family	616
exit-remote-neighbor	617
exp-mask	618
export destination	619
export map	620
export source	621
extended-authentication	622
external-paths	623

Chapter 7**F Commands****625**

fabric-strict-priority	626
fabric-weight	627
fabric weights	628
failover-resync	629
filter	630
flash-disk compare	631
flash-disk duplicate	632
flash-disk initialize	633
flash-disk scan	634
forward	635
forward interface	636
forward next-hop	637
forwarding-rate-threshold	638
forwarding-table route-holddown	639
frame-relay class	640
frame-relay classifier-list	641
frame-relay description	642
frame-relay dos-protection-group	643
frame-relay fragment	644
frame-relay interface-dlci ietf	645
frame-relay intf-type	646
frame-relay keepalive	647
frame-relay lmi-n391dte	648
frame-relay lmi-n392dce	649
frame-relay lmi-n392dte	650
frame-relay lmi-n393dce	651
frame-relay lmi-n393dte	652
frame-relay lmi-t391dte	653
frame-relay lmi-t392dce	654
frame-relay lmi-type	655
frame-relay policy	656
frame-relay policy-list	657
framing	658
frequency	659
ftp-server enable	660
ftp-server flush	661
full-spf-always	662

Chapter 8**G Commands****663**

global export map	664
global import map	665
graceful-restart	666
graceful-restart helper	667
graceful-restart helper-abort-topology-change	668
graceful-restart notify-time	669
graceful-restart restart-time	670

grace-period	671
gre destination profile	672
green-mark	673
gre-tunnel classifier-list	674
gre-tunnel policy	675
gre-tunnel policy-list	676
group	677
gsmp-syn-timeout	678

Chapter 9**H Commands 679**

halt	680
hash	681
hdlc dos-protection-group	682
hdlc down-when-looped	683
hdlc keepalive	684
hdlc shutdown	685
hello hold-time	686
hello interval	687
hello-interval	688
help	689
hops-of-statistics-kept	690
host	691
hostname	692
hotfix activate	693

Chapter 10**I Commands 695**

id	696
identification	697
idle-character	698
igmp disable	699
igmp promiscuous	700
ignore-lsp-errors	701
ike cri	702
ike local-identity	703
ike peer-identity distinguished-name	704
ike peer-identity domain-name	705
ike peer-identity ip address	706
ike peer-identity username	707
import map	708
inarp	709
include circuit-identifier	710
include dhcp-option 82	711
include hostname	712
include ip-address	713
include mac-address	714
include virtual-router-name	715
index	716
instance-interface-type	717

interface	718
interface atm	719
interface-event-disable	720
interface fastEthernet	721
interface gigabitEthernet	722
interface ip	723
interface ipv6	724
interface lag	725
interface loopback	726
interface mlframe-relay	727
interface mlppp	728
interface null	729
interface pos	730
interface serial	731
interface tenGigabitEthernet	732
interface tunnel	733
invert data	734
ip	735
ip access-routes	736
ip access-route table-map	737
ip address	738
ip-address	739
ip address-pool	740
ip-address-pool	741
ip address virtual-router	742
ip alwaysup	743
ip analyzer	744
ip as-path access-list	745
ip atm-vc	747
ip auto-configure ip-subscriber	748
ip auto-detect ip-subscriber	749
ip bgp-community new-format	750
ip bgp-confed-as-set new-format	751
ip block-multicast-sources	752
ip broadcast-address	753
ip classifier-list	754
ip community-list	757
ip debounce-time	758
ip demux-type da-prefix	759
ip description	760
ip destination-prefix	761
ip dhcp-capture	762
ip dhcp-external auto-configure	763
ip dhcp-external disregard-giaddr-next-hop	764
ip dhcp-external recreate-subscriber-interface	765
ip dhcp-external server-address	766
ip dhcp-external server-sync	767
ip dhcp-local auth domain	768
ip dhcp-local auth include	769
ip dhcp-local auth password	770
ip dhcp-local auth user-prefix	771

ip dhcp-local auto-configure agent-circuit-identifier	772
ip dhcp-local cable-modem	773
ip dhcp-local excluded-address	774
ip dhcp-local limit	775
ip dhcp-local pool	776
ip dhcp-local snmpTraps	777
ip dhcp-local unique-client-ids	778
ip dhcp-server	779
ip directed-broadcast	780
ip disable-forwarding	781
ip domain-lookup	782
ip domain-name	783
ip dos-protection-group	784
ip dvmrp	785
ip dvmrp accept-filter	786
ip dvmrp announce-filter	787
ip dvmrp auto-summary	788
ip dvmrp disable	789
ip dvmrp metric-offset	790
ip dvmrp route-hog-notification	791
ip dvmrp route-limit	792
ip dvmrp summary-address	793
ip dvmrp unicast-routing	794
ip dynamic-interface-prefix	795
ip explicit-path	796
ip extcommunity-list	797
ip fallback global	798
ip filter-options all	799
ip flow-aggregation cache	800
ip flow-cache entries	801
ip flow-cache timeout	802
ip flow-export	803
ip flow-sampling-mode packet-interval	804
ip flow statistics	805
ip ftp source-address	806
ip ftp source-interface	807
ip-hint	808
ip http	809
ip http access-class	810
ip http max-connection-time	811
ip http port	812
ip http redirectUrl	813
ip http same-host-limit	814
ip http server	815
ip icmp update-source	816
ip igmp	817
ip igmp access-group	818
ip igmp access-source-group	819
ip igmp apply-oif-map	820
ip igmp explicit-tracking	821
ip igmp group limit	822

ip igmp immediate-leave	823
ip igmp last-member-query-interval	824
ip igmp oif-map	825
ip igmp promiscuous	826
ip igmp-proxy	827
ip igmp-proxy unsolicited-report-interval	828
ip igmp-proxy V1-router-present-time	829
ip igmp querier	830
ip igmp querier-timeout	831
ip igmp query-interval	832
ip igmp query-max-response-time	833
ip igmp robustness	834
ip igmp ssm-map enable	835
ip igmp ssm-map static	836
ip igmp static-exclude	837
ip igmp static-group	838
ip igmp static-include	839
ip igmp version	840
ip ignore-df-bit	841
ip inactivity-timer	842
ip initial-sequence-preference	843
ip interface	844
ip irdp	845
ip local alias	846
ip local pool	847
ip local pool snmpTrap	848
ip local pool warning	849
ip local shared-pool	850
ip mac-validate	851
ip mask-reply	852
ip match-policy-list	853
ip mirror	854
ip mobile home-agent	855
ip mobile host	856
ip mobile profile	857
ip mobile secure foreign-agent	858
ip mobile secure host	859
ip mpls forwarding-mode label-switched	861
ip mtu	862
ip multicast admission-bandwidth-limit	863
ip multicast ioa-packet-replication	864
ip multicast-routing	865
ip multicast-routing bandwidth-map	866
ip multicast-routing disable-rpf-check	867
ip multicast-routing permanent-mroute	868
ip multipath round-robin	869
ip name-server	870
ip nat	871
ip nat inside source list	872
ip nat inside source static	873
ip nat outside source list	874

ip nat outside source static	875
ip nat pool	876
ip nat translation	877
ip nat translation max-entries	878
ip nfs	879
ip nfs host	880
ip ospf authentication-key	881
ip ospf authentication message-digest	882
ip ospf authentication-none	883
ip ospf bfd-liveness-detection	884
ip ospf cost	885
ip ospf dead-interval	886
ip ospf hello-interval	887
ip ospf message-digest-key md5	888
ip ospf network	889
ip ospf priority	890
ip ospf retransmit-interval	891
ip ospf shutdown	892
ip ospf transmit-delay	893
ip pim	894
ip pim bfd-liveness-detection	895
ip pim bsr-candidate	896
ip pim data-mdt	897
ip pim dr-priority	898
ip pim group-address-pool	899
ip pim join-filter	900
ip pim join-prune-interval	901
ip pim query-interval	902
ip pim rp-address	903
ip pim rp-candidate	904
ip pim send-rp-announce	905
ip pim send-rp-discovery scope	906
ip pim sparse-mode graceful-restart-duration	907
ip pim spt-threshold	908
ip pim ssm	909
ip policy	910
ip policy-list	912
ip policy-parameter hierarchical	913
ip policy-parameter reference-rate	914
ip prefix-list	915
ip prefix-tree	916
ip profile	917
ip proxy-arp	918
ip re-authenticate-auto-detect ip-subscriber	919
ip redirects	920
ip refresh-route	921
ip rip	922
ip rip authentication key	923
ip rip authentication mode	924
ip rip bfd-liveness-detection	925
ip rip copy-to-dynamic	926

ip rip receive version	927
ip rip send version	928
ip route	929
ip route-cache flow sampled	931
ip route-map ip-subscriber	932
ip route-type	933
ip router-id	934
ip router isis	935
ip-router-name	936
ip rpf-route	937
ip rsvp authentication	938
ip rsvp authentication key	939
ip rsvp bandwidth	940
ip rsvp bfd-liveness-detection	941
ip rsvp signalling hello	942
ip sa-validate	943
ip sa-validate trap-enable	944
ip service-profile	945
ip share-interface	946
ip share-nexthop	947
ip shutdown	948
ip source-prefix	949
ip source-route	950
ip speed	951
ip split-horizon	952
ip ssh authentication-retries	953
ip ssh crypto	954
ip ssh disable-user-authentication	955
ip ssh mac	956
ip ssh sleep	957
ip ssh timeout	958
ip ssh user-authentication-protocol	959
ip static-route table-map	960
ip summary-address	961
ip tcp ack-rst-and-syn	962
ip tcp adjust-mss	963
ip ttl	964
ip tunnel reassembly	965
ip unnumbered	966
ip unreachable	967
ip use-framed-routes ip-subscriber	968
ip virtual-router	969
ip vrf	970
ip vrf forwarding	971
ip vrrp	972
ip vrrp accept-data	973
ip vrrp advertise-interval	974
ip vrrp authentication-key	975
ip vrrp authentication-type	976
ip vrrp enable	977
ip vrrp icr-partition	978

ip vrrp icr-partition group	979
ip vrrp icr-partition svlan-list	980
ip vrrp icr-partition svlan-list explicit	981
ip vrrp icr-partition svlan-range	982
ip vrrp icr-partition vlan-list	983
ip vrrp icr-partition vlan-range	984
ip vrrp preempt	986
ip vrrp priority	987
ip vrrp timers-learn	988
ip vrrp track	989
ip vrrp virtual-address	990
ipsec ca authenticate	991
ipsec ca enroll	992
ipsec ca identity	993
ipsec certificate-database refresh	994
ipsec certificate-request generate	995
ipsec clear sa	996
ipsec crl	997
ipsec identity	998
ipsec ike-policy-rule	999
ipsec isakmp-policy-rule	1000
ipsec key generate	1001
ipsec key manual pre-share	1002
ipsec key pubkey-chain rsa	1003
ipsec key zeroize	1004
ipsec lifetime	1005
ipsec local-endpoint	1006
ipsec option dpd	1007
ipsec option nat-t	1008
ipsec option tx-invalid-cookie	1009
ipsec transform-set	1010
ipsec transport profile	1011
ipsec tunnel profile	1012
ipv6	1013
ipv6 access-list	1014
ipv6 access-route table-map	1015
ipv6 address	1016
ipv6 address-pool local	1017
ipv6 block-multicast-sources	1018
ipv6 classifier-list	1019
ipv6 description	1021
ipv6 dhcpv6-local delegated-prefix	1022
ipv6 dhcpv6-local dns-domain-search	1023
ipv6 dhcpv6-local dns-server	1024
ipv6 dhcpv6-local prefix-lifetime	1025
ipv6 dos-protection-group	1026
ipv6 enable	1027
ipv6 hop-limit	1028
ipv6 http	1029
ipv6 http port	1030
ipv6 http redirectUrl	1031

ipv6 http server	1032
ipv6 initial-sequence-preference	1033
ipv6-local-interface	1034
ipv6 local pool	1035
ipv6 mld	1036
ipv6 mld access-group	1037
ipv6 mld access-source-group	1038
ipv6 mld apply-oif-map	1039
ipv6 mld explicit-tracking	1040
ipv6 mld group limit	1041
ipv6 mld immediate-leave	1042
ipv6 mld last-member-query-interval	1043
ipv6 mld oif-map	1044
ipv6 mld-proxy	1045
ipv6 mld-proxy unsolicited-report-interval	1046
ipv6 mld-proxy version	1047
ipv6 mld querier-timeout	1048
ipv6 mld query-interval	1049
ipv6 mld query-max-response-time	1050
ipv6 mld robustness	1051
ipv6 mld ssm-map enable	1052
ipv6 mld ssm-map static	1053
ipv6 mld static-exclude	1054
ipv6 mld static-group	1055
ipv6 mld static-include	1056
ipv6 mld version	1057
ipv6 mtu	1058
ipv6 multicast admission-bandwidth-limit	1059
ipv6 multicast ioa-packet-replication	1060
ipv6 multicast-routing	1061
ipv6 multicast-routing bandwidth-map	1062
ipv6 multicast-routing disable-rpf-check	1063
ipv6 multicast-routing permanent-mroute	1064
ipv6 nd	1065
ipv6 nd active-solicitations	1066
ipv6 nd dad attempts	1067
ipv6 nd managed-config-flag	1068
ipv6 nd ns-interval	1069
ipv6 nd other-config-flag	1070
ipv6 nd prefix-advertisement	1071
ipv6 nd proxy	1072
ipv6 nd ra-interval	1073
ipv6 nd ra-lifetime	1074
ipv6 nd reachable-time	1075
ipv6 nd suppress-ra	1076
ipv6 nd suppress-ra-source-link-layer	1077
ipv6 neighbor	1078
ipv6 ospf area	1079
ipv6 ospf bfd-liveness-detection	1080
ipv6 ospf cost	1081
ipv6 ospf dead-interval	1082

ipv6 ospf hello-interval	1083
ipv6 ospf mtu-ignore	1084
ipv6 ospf network	1085
ipv6 ospf priority	1086
ipv6 ospf retransmit-interval	1087
ipv6 ospf shutdown	1088
ipv6 ospf transmit-delay	1089
ipv6 pim bfd-liveness-detection	1090
ipv6 pim bsr-candidate	1091
ipv6 pim dr-priority	1092
ipv6 pim join-filter	1093
ipv6 pim join-prune-interval	1094
ipv6 pim query-interval	1095
ipv6 pim rp-address	1096
ipv6 pim rp-candidate	1097
ipv6 pim sparse-mode	1098
ipv6 pim sparse-mode graceful-restart-duration	1099
ipv6 pim spt-threshold	1100
ipv6 pim ssm	1101
ipv6 policy	1102
ipv6 policy-list	1104
ipv6 policy-parameter hierarchical	1105
ipv6 policy-parameter reference-rate	1106
ipv6 prefix-list	1107
ipv6-prefix-pool-name	1108
ipv6 route	1109
ipv6 router isis	1110
ipv6 router mld	1111
ipv6-router-name	1112
ipv6 router ospf	1113
ipv6 router pim	1114
ipv6 route-type	1115
ipv6 rpf-route	1116
ipv6 sa-validate	1117
ipv6 share-interface	1118
ipv6 static-route table-map	1119
ipv6 unnumbered	1120
ipv6 virtual-router	1121
isis authentication-key	1122
isis bfd-liveness-detection	1123
isis circuit-type	1124
isis csnp-interval	1125
isis hello-interval	1126
isis hello-multiplier	1127
isis hello padding	1128
isis lsp-interval	1129
isis mesh-group	1130
isis message-digest-key	1131
isis metric	1133
isis network point-to-point	1134
isis priority	1135

isis retransmit-interval	1136
isis retransmit-throttle-interval	1137
isis tag	1138
issuer-identifier	1139
issu initialize	1140
issu start	1141
issu stop	1142
is-type	1143

Chapter 11**K Commands****1145**

key	1146
key-string	1148

Chapter 12**L Commands****1149**

l2c	1150
l2c end-user-id	1151
l2c ip listen	1152
l2c ip oif	1153
l2c line-configuration	1154
l2c max-branches	1155
l2c oam	1156
l2c peer-attachment-id	1157
l2tp checksum	1158
l2tp classifier-list	1159
l2tp destination lockout-test	1160
l2tp destination lockout-timeout	1161
l2tp destination profile	1162
l2tp destruct-timeout	1163
l2tp dial-out connecting-timer-value	1164
l2tp dial-out dormant-timer-value	1165
l2tp dial-out max-buffered-triggers	1166
l2tp dial-out session delete	1167
l2tp dial-out session reset	1168
l2tp dial-out target	1169
l2tp disable calling-number-avp	1170
l2tp disable challenge	1171
l2tp disconnect-cause	1172
l2tp drain	1173
l2tp drain destination	1174
l2tp drain tunnel	1175
l2tp failover-resync	1176
l2tp fail-over-within-preference	1177
l2tp ignore-receive-data-sequencing	1178
l2tp ignore-transmit-address-change	1179
l2tp policy	1180
l2tp policy-list	1181
l2tp policy-parameter hierarchical	1182
l2tp policy-parameter reference-rate	1183

l2tp reject-transmit-address-change	1184
l2tp retransmission	1185
l2tp rx-connect-speed-when-equal	1186
l2tp shutdown	1187
l2tp shutdown destination	1188
l2tp shutdown session	1189
l2tp shutdown tunnel	1190
l2tp switch-profile	1191
l2tp tunnel default-receive-window	1192
l2tp tunnel idle-timeout	1193
l2tp tunnel short-drain-timeout	1194
l2tp tunnel-switching	1195
l2tp tunnel test	1196
l2tp unlock destination	1197
l2tp unlock-test destination	1198
l2tp weighted-load-balancing	1199
l2vpn control-word	1200
l2vpn encapsulation-type	1201
l2vpn local-site-id remote-site-id	1202
l2vpn rd	1203
l2vpn route-target	1204
l2vpn sequencing	1205
l2vpn site-name site-id	1206
l2vpn site-range	1207
lACP	1208
lACP port-priority	1209
lag dos-protection-group	1210
lease	1211
license bfd	1212
license b-ras	1213
license ipsec-tunnels	1214
license ipv6	1215
license issu	1216
license l2tp-session	1217
license mobile-ip home-agent	1218
license nat	1219
license service-management	1220
lifetime	1221
line	1223
link	1224
link failover arp-flush	1225
link failover force	1226
link failover timeout	1227
link selection	1228
list	1229
load-interval	1230
load-rebalance	1231
local host	1232
local-interface	1233
local ip address	1234
local ip identity	1236

local ip network	1237
log	1238
log-adjacency-changes	1239
log destination	1241
log destination syslog source	1243
log engineering	1244
log fields	1245
log filters	1246
log here	1247
log severity	1248
log unlimit	1250
log verbosity	1251
login	1252
login authentication	1253
logout subscribers	1254
loopback	1255
lsp-gen-interval	1257
lsp-mtu	1258
lsp-refresh-interval	1259

Chapter 13**M Commands****1261**

macro	1262
map-class frame-relay	1263
map-group	1264
map-list	1265
mark	1266
mark-clp	1268
mark-de	1269
mark-exp	1270
mark-user-priority	1271
mask destination	1272
masked-key	1273
mask source	1274
mask-val	1275
match as-path	1276
match community	1277
match distance	1278
match extcommunity	1279
match ip address	1280
match ip next-hop	1281
match ipv6 address	1282
match ipv6 next-hop	1283
match ipv6 route-source	1284
match level	1285
match metric	1286
match metric-type	1287
match mpls-label	1288
match policy-list	1289
match route-type	1290

match-set summary prefix-tree	1291
match tag	1292
max-branches	1293
max-discovery-table-entries	1294
maximum-paths	1295
maximum routes	1296
maximum-voql	1297
max-interfaces	1298
max-lsp-lifetime	1299
max-response-failure	1300
max-sessions	1301
mdl carrier	1303
mdl string	1304
mdl transmit	1305
mdt-data-delay	1306
mdt-data-holddown	1307
mdt-data-timeout	1308
mdt-interval	1309
medium ipv4	1310
member interface	1311
member-interface	1312
member-interface-type	1313
memory	1314
message-digest-key md5	1315
metric	1316
metric-style narrow	1317
metric-style transition	1318
metric-style wide	1319
minimum-dynamic-rate-percent	1320
minimum-links	1321
mirror	1322
mirror analyzer-ip-address	1324
mirror disable	1325
mirror-enable	1327
mirror trap-enable	1328
mld disable	1329
mode	1330
monitor atm vc	1331
monitor atm vp	1332
monitor vlan interface	1333
more	1334
motd-banner	1335
mount	1336
mpls	1337
mpls atm vci range	1339
mpls atm vpi range	1340
mpls backup-path	1341
mpls bandwidth	1342
mpls classifier-list	1343
mpls copy-upc-to-exp	1344
mpls create-dynamic-interfaces	1345

mpls diff-serv phb-id traffic-class	1346
mpls disable	1347
mpls explicit-path	1348
mpls ip propagate-ttl	1349
mpls l2transport load-balancing-group	1350
mpls ldp	1352
mpls ldp advertise-labels	1353
mpls ldp autoconfig	1354
mpls ldp deaggregate	1355
mpls ldp disable	1356
mpls ldp discovery transport-address	1357
mpls ldp egress-label	1358
mpls ldp graceful-restart	1359
mpls ldp graceful-restart reconnect-time	1360
mpls ldp graceful-restart recovery-time	1361
mpls ldp graceful-restart timers max-recovery	1362
mpls ldp graceful-restart timers neighbor-liveness	1363
mpls ldp igp sync holddown	1364
mpls ldp independent-control	1365
mpls ldp ip-forwarding	1366
mpls ldp link-hello disable	1367
mpls ldp neighbor password	1368
mpls ldp profile	1369
mpls ldp redistribute	1370
mpls ldp session holdtime	1371
mpls ldp session keepalive interval	1372
mpls ldp session retries	1373
mpls ldp session retry-time	1374
mpls ldp strict-security	1375
mpls ldp sync	1376
mpls ldp targeted-hello holdtime	1377
mpls ldp targeted-hello interval	1378
mpls ldp targeted-hello receive list	1379
mpls ldp targeted-hello send list	1380
mpls ldp vpls neighbor	1381
mpls ldp vpls vpls-id	1382
mpls lsp no-route retries	1383
mpls lsp no-route retry-time	1384
mpls lsp retries	1385
mpls lsp retry-time	1386
mpls match exp-bits	1387
mpls match traffic-class	1388
mpls policy	1389
mpls policy-list	1390
mpls policy-parameter hierarchical	1391
mpls policy-parameter reference-rate	1392
mpls policy-statistics	1393
mpls preserve-vpn-exp	1394
mpls-relay	1395
mpls-relay atm cell-packing mcpt-timer	1398
mpls-relay atm vpi-range vci-range	1399

mpls-relay disable	1400
mpls reoptimize	1401
mpls reoptimize timers frequency	1402
mpls rsvp	1403
mpls rsvp authentication	1404
mpls rsvp authentication key	1405
mpls rsvp bfd-liveness-detection	1406
mpls rsvp disable	1407
mpls rsvp egress-label	1408
mpls rsvp message-bundling	1409
mpls rsvp profile	1410
mpls rsvp refresh-reduction	1411
mpls rsvp signalling hello	1412
mpls rsvp signalling hello graceful-restart	1413
mpls rsvp signalling hello graceful-restart recovery-time	1414
mpls rsvp signalling hello graceful-restart restart-time	1415
mpls rsvp signalling node-hello	1416
mpls signaling-interface	1417
mpls spf-use-any-best-path	1418
mpls statistics label	1419
mpls statistics next-hop	1420
mpls statistics policy	1421
mpls topology-driven-lsp	1422
mpls topology-driven-lsp ip-interfaces	1423
mpls traffic-class	1424
mpls traffic-eng	1425
mpls traffic-eng administrative-weight	1426
mpls traffic-eng area	1427
mpls traffic-eng attribute-flags	1428
mpls traffic-eng egress-label	1429
mpls traffic-eng flood thresholds	1430
mpls traffic-eng link-management timers periodic-flooding	1431
mpls traffic-eng multicast-intact	1432
mpls traffic-eng router-id	1433
mpls tunnel-model	1434
mpls tunnels profile	1435
mroute port admission-bandwidth-limit	1436
mroute port limit	1437
mru	1438
mtrace	1439
mtu	1440
multicast	1441
multicast group port limit	1442

Part 2

Index

Index	1445
-------------	------

List of Tables

About the Documentation	xxxix
Table 1: Notice Icons	xl
Table 2: Text and Syntax Conventions	xl

Part 1

Commands, A to M

Chapter 1	Command Reference Topics	3
	Table 3: Interface Types and Specifiers for ERX7xx Models, ERX14xx Models, and ERX310 Router	5
	Table 4: Interface Types and Specifiers for E120 Router and E320 Router	13

About the Documentation

- E Series and JUNOS^e Documentation and Release Notes on page xxxix
- Audience on page xxxix
- E Series and JUNOS^e Text and Syntax Conventions on page xxxix
- Obtaining Documentation on page xli
- Documentation Feedback on page xli
- Requesting Technical Support on page xli

E Series and JUNOS^e Documentation and Release Notes

For a list of related JUNOS^e documentation, see <http://www.juniper.net/techpubs/software/index.html> .

If the information in the latest release notes differs from the information in the documentation, follow the *JUNOS^e Release Notes*.

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

Audience

This guide is intended for experienced system and network specialists working with Juniper Networks E Series Broadband Services Routers in an Internet access environment.

E Series and JUNOS^e Text and Syntax Conventions

Table 1 on page xl defines notice icons used in this documentation.

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 xl defines text and syntax conventions that we use throughout the E Series and JUNOS documentation.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents commands and keywords in text.	<ul style="list-style-type: none"> Issue the clock source command. Specify the keyword exp-msg.
Bold text like this	Represents text that the user must type.	host1(config)# traffic class low-loss1
Fixed-width text like this	Represents information as displayed on your terminal's screen.	<pre>host1#show ip ospf 2 Routing Process OSPF 2 with Router ID 5.5.0.250 Router is an Area Border Router (ABR)</pre>
<i>Italic text like this</i>	<ul style="list-style-type: none"> Emphasizes words. Identifies variables. Identifies chapter, appendix, and book names. 	<ul style="list-style-type: none"> There are two levels of access: <i>user</i> and <i>privileged</i>. <i>clusterId</i>, <i>ipAddress</i>. <i>Appendix A, System Specifications</i>
Plus sign (+) linking key names	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Syntax Conventions in the Command Reference Guide		
Plain text like this	Represents keywords.	terminal length
<i>Italic text like this</i>	Represents variables.	<i>mask</i> , <i>accessListName</i>
(pipe symbol)	Represents a choice to select one keyword or variable to the left or to the right of this symbol. (The keyword or variable can be either optional or required.)	diagnostic line

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

Convention	Description	Examples
[] (brackets)	Represent optional keywords or variables.	[internal external]
[]* (brackets and asterisk)	Represent optional keywords or variables that can be entered more than once.	[level1 level2 l1]*
{ } (braces)	Represent required keywords or variables.	{ permit deny } { in out } { <i>clusterId</i> <i>ipAddress</i> }

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the Technical Documentation page on the Juniper Networks Web site at <http://www.juniper.net/>.

To download complete sets of technical documentation to create your own documentation CD-ROMs or DVD-ROMs, see the Offline Documentation page at

<http://www.juniper.net/techpubs/resources/cdrom.html>

Copies of the Management Information Bases (MIBs) for a particular software release are available for download in the software image bundle from the Juniper Networks Web site at <http://www.juniper.net/>.

Documentation Feedback

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

- Document or topic name
- URL or page number
- Software release version

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 post-sales 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/7100059-EN.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: <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, see http://www.juniper.net/support/requesting_support.html .

Part 1

Commands, A to M

- Command Reference Topics on page 3
- A Commands on page 21
- B Commands on page 211
- C Commands on page 349
- D Commands on page 475
- E Commands on page 555
- F Commands on page 625
- G Commands on page 663
- H Commands on page 679
- I Commands on page 695
- K Commands on page 1145
- L Commands on page 1149
- M Commands on page 1261

Chapter 1

Command Reference Topics

- Using the no Version Versus the default Version of Commands on page 3
- Deprecated Commands on page 4
- Filtering show Commands on page 4
- Interface Types and Specifiers on page 5

Using the no Version Versus the default Version of Commands

Most router configuration commands have a **no** version, which you can use to negate a command (or a portion of it specified by an optional keyword) or restore its default setting. When you use a command *without* the keyword **no**, you can reenable a disabled feature or override a default setting. You have the option of using the **default** keyword whenever the **no** keyword is also a choice; simply enter the keyword **default** instead of **no**.

In most cases, when you execute the **default** version of a command, it produces the exact results as the **no** version. There are some commands for which the **default** version yields a different result than the **no** version.

Commands for which the **default** behavior differs from the **no** behavior are clearly identified in this guide. Unless otherwise specified, therefore, the **default** command is identical to the **no** command and is neither documented nor discussed.

The syntax for each **no** command is described in this guide. Some commands do not have a **no** version; this is indicated in the individual command descriptions except for the **show** commands, none of which has a **no** version.

The CLI can act on **no** versions of commands when you have entered sufficient information to distinguish the command syntactically, and ignores all subsequent input on that line.

To be compatible with some non-E Series implementations, the **no** versions of commands accept the same options as the affirmative version of the commands. The CLI ignores the optional input if it has no effect on the command behavior. If using the option changes the behavior of the **no** version, the individual command entry in this guide describes the difference in behavior.

Deprecated Commands

A command that has been deprecated in a release or in a particular configuration mode returns a notice when you issue the command manually:

NOTICE: This command is obsolete. It may be completely removed from a subsequent software release.

A preferred alternate command is provided in the notice. If you have a script that uses the deprecated command, the deprecated command is automatically mapped to the preferred command when you run the script. If the deprecated command no longer has a function, then that command has no effect when you run a script containing the command.

We recommend that you use the preferred command when writing new scripts.

Filtering show Commands

You have access to a variety of **show** commands that display router and protocol information. You can filter the output of a **show** command by specifying **|** (the UNIX pipe symbol), one of the following keywords, and either a case-sensitive text string or a regular expression.

- **begin**—Displays output beginning with the first line that contains the text string or regular expression
- **include**—Displays output lines that contain the text string or regular expression and excludes lines that do not contain the text string or regular expression
- **exclude**—Displays output lines that do not contain the text string or regular expression and excludes lines that do contain the text string or regular expression

You can press Ctrl + c to interrupt the **show** command output.



NOTE: The router does not recognize beginning spaces of the text string. For example, if you enter the **include** option with IP as the text string on which to filter, the router ignores the space and displays lines that include words such as RIP.

Example In the following example, the output display consists only of lines that contain the string *ip*. The router omits all other lines of the output from the display because none of them contain the string *ip*.

```
host1#show config include-defaults | include ip
! Configuration script generated on FRI NOV 12 1999 16:56:41 UTC
ip address 192.168.1.229 255.255.255.0
ip rip receive version 2 1
ip rip send version 1
ip rip authentication mode md5 17
ip rip authentication key
ip route 10.6.0.0 255.255.0.0 192.168.1.1
ip route 10.10.0.0 255.255.0.0 192.168.1.1
```

```
ip route 10.10.0.166 255.255.255.255 192.168.1.1
ip debounce-time 0
router rip
```

- Related Topics** ■ For a list of regular expressions, see *Using Regular Expressions* in the *JUNOS IP Services Configuration Guide*

Interface Types and Specifiers

Many commands take the variables *interfaceType* and *interfaceSpecifier*. Some commands support all types of interfaces, whereas other commands support only certain types of interfaces. Similarly, some commands support all interface specifier formats for a particular interface type, whereas other commands support only certain interface specifier formats.

Table 3 on page 5 lists the interface specifiers for each type of interface on ERX7xx models, ERX14xx models, and the Juniper Networks ERX310 Broadband Services Router.



NOTE: On ERX7xx models, ERX14xx models, and the ERX310 router, you can use the **atm slot/port/vpi/vci** interface specifier format as an alternative to the **atm slot/port.subinterface** format with the specific **show interface** and **show subinterface** commands to monitor all ATM 1483 subinterfaces (except NBMA interfaces) as well as the upper-layer interfaces configured over an ATM 1483 subinterface. You cannot, however, use the **atm slot/port/vpi/vci** format to create or modify an ATM 1483 subinterface.

Table 4 on page 13 lists the interface specifiers for each type of interface on the Juniper Networks E120 and E320 Broadband Services Routers.



NOTE: On the E120 router and the E320 router you can use the **atm slot/adapter/port/vpi/vci** interface specifier format as an alternative to the **atm slot/adapter/port.subinterface** format with the specific **show interface** and **show subinterface** commands to monitor all ATM 1483 subinterfaces (except NBMA interfaces) as well as the upper-layer interfaces configured over an ATM 1483 subinterface. You cannot, however, use the **atm slot/adapter/port/vpi/vci** format to create or modify an ATM 1483 subinterface.

Table 3: Interface Types and Specifiers for ERX7xx Models, ERX14xx Models, and ERX310 Router

Interface Type	Description	Interface Specifier	Example
atm	ATM interface or ATM 1483 subinterface	Refer to the individual formats listed below.	

Table 3: Interface Types and Specifiers for ERX7xx Models, ERX14xx Models, and ERX310 Router *(continued)*

Interface Type	Description	Interface Specifier	Example
■ ATM interface or subinterface		<p>To configure an ATM interface or subinterface:</p> <p><i>slot/port[.subinterface]</i></p> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–6 (ERX7xx models), 0–13 (ERX14xx models), and 0–2 (ERX310 router) ■ <i>port</i>—Port number on the I/O module ■ <i>subinterface</i>—Number of the subinterface in the range 1–2147483647 	atm 3/2.6
■ ATM 1483 subinterface		<p>To display information about an ATM 1483 subinterface by using show commands:</p> <p><i>slot/port/vpil/vci</i></p> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–6 (ERX7xx models), 0–13 (ERX14xx models), and 0–2 (ERX310 router) ■ <i>port</i>—Port number on the I/O module ■ <i>vpi</i>—Virtual path identifier of the PVC on this ATM 1483 subinterface; allowable numeric range depends on the module capabilities and current configuration ■ <i>vci</i>—Virtual circuit identifier of the PVC on this ATM 1483 subinterface; allowable numeric range depends on the module capabilities and current configuration 	atm 3/2/1/2

Table 3: Interface Types and Specifiers for ERX7xx Models, ERX14xx Models, and ERX310 Router (continued)

Interface Type	Description	Interface Specifier	Example
fastEthernet	IEEE 802.3 Fast Ethernet (FE) interface	<code>slot/port[.subinterface1[.subinterface2]]</code> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–6 (ERX7xx models), 0–13 (ERX14xx models), and 0–2 (ERX310 router) ■ <i>port</i>—Port number on the I/O module or port 0 for the Fast Ethernet management port on the SRP I/O module <p>The meaning of the <i>subinterface</i> variables depends on the configuration context. You can configure Fast Ethernet interfaces with or without VLANs.</p> <ul style="list-style-type: none"> ■ VLANs: <ul style="list-style-type: none"> ■ <i>subinterface1</i>—Number of the VLAN subinterface in the range 1–2147483647; no more than 4096 VLAN subinterfaces per Fast Ethernet physical port ■ <i>subinterface2</i>—When using PPPoE, the number of the PPPoE subinterface in the range 1–2147483647; no more than 8000 PPPoE subinterfaces per Fast Ethernet line module ■ No VLANs: <ul style="list-style-type: none"> ■ <i>subinterface1</i>—When using PPPoE, the number of the PPPoE subinterface in the range 1–2147483647; no more than 8000 PPPoE subinterfaces per Fast Ethernet line module ■ <i>subinterface2</i>—Not used 	fastEthernet 3/2.6.20

Table 3: Interface Types and Specifiers for ERX7xx Models, ERX14xx Models, and ERX310 Router (continued)

Interface Type	Description	Interface Specifier	Example
gigabitEthernet	IEEE 802.3 Gigabit Ethernet (GE) interface	<i>slot</i> / <i>port</i> [. <i>subinterface1</i> [. <i>subinterface2</i>]] <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–6 (ERX7xx models), 0–13 (ERX14xx models), and 0–2 (ERX310 router) ■ <i>port</i>—Port number on the I/O module <p>The meaning of the <i>subinterface</i> variables depends on the configuration context. You can configure Gigabit Ethernet interfaces with or without VLANs.</p> <ul style="list-style-type: none"> ■ VLANs: <ul style="list-style-type: none"> ■ <i>subinterface1</i>—Number of the VLAN subinterface in the range 1–2147483647; no more than 4096 VLAN subinterfaces per Gigabit Ethernet physical port ■ <i>subinterface2</i>—When using PPPoE, the number of the PPPoE subinterface in the range 1–2147483647; no more than 8000 PPPoE subinterfaces per Gigabit Ethernet line module ■ No VLANs: <ul style="list-style-type: none"> ■ <i>subinterface1</i>—When using PPPoE, the number of the PPPoE subinterface in the range 1–2147483647; no more than 8000 PPPoE subinterfaces per Gigabit Ethernet line module ■ <i>subinterface2</i>—Not used 	gigabitEthernet 3/0.6.20
lag	IEEE 802.3ad link aggregation group (LAG) interface	<i>bundle-name</i> [. <i>subinterface</i>] <ul style="list-style-type: none"> ■ <i>bundle-name</i>—Name of the bundle ■ <i>subinterface</i>—Number of the LAG subinterface in the range 1–2147483647 	lag paris.2
loopback	Loopback interface	<i>integer</i> <ul style="list-style-type: none"> ■ <i>integer</i>—Integer in the range 1–4294967293 	loopback 20
mlframe-relay	Multilink frame relay interface	<i>bundle-name</i> [. <i>subinterface</i>] <ul style="list-style-type: none"> ■ <i>bundle-name</i>—Name of the bundle ■ <i>subinterface</i>—Number of the MLFR subinterface in the range 1–4294967293 	mlframe-relay boston.1

Table 3: Interface Types and Specifiers for ERX7xx Models, ERX14xx Models, and ERX310 Router (continued)

Interface Type	Description	Interface Specifier	Example
mlppp	Multilink PPP interface	<i>bundle-name</i> ■ <i>bundle-name</i> —Name of the bundle	mlppp chicago
mplsL2shim	MPLS shim interface	<i>slot/port[.subinterface]</i> ■ <i>slot</i> —Number of the chassis slot in the range 0–6 (ERX7xx models), 0–13 (ERX14xx models), and 0–2 (ERX310 router) ■ <i>port</i> —Port number on the I/O module ■ <i>subinterface</i> —Number of the subinterface in the range 1–2147483647	mplsL2shim 3/2.1
mplsMajor	MPLS major interface	<i>slot/port[.subinterface]</i> ■ <i>slot</i> —Number of the chassis slot in the range 0–6 (ERX7xx models), 0–13 (ERX14xx models), and 0–2 (ERX310 router) ■ <i>port</i> —Port number on the I/O module ■ <i>subinterface</i> —Number of the subinterface in the range 1–2147483647	mplsMajor 3/2.1
mplsMinor	MPLS minor interface	<i>[vr:]tunnel-name</i> ■ <i>vr</i> —Name of a virtual router ■ <i>tunnel-name</i> —Name of the tunnel	mplsMinor lsp-02020202-1-4
null	Null interface, which acts as a data sink and cannot forward or receive traffic. You cannot configure values on the null interface.	0	null 0

Table 3: Interface Types and Specifiers for ERX7xx Models, ERX14xx Models, and ERX310 Router *(continued)*

Interface Type	Description	Interface Specifier	Example
pos	Packet over SONET (POS) interface	<code>slot/port[.subinterface]</code> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–6 (ERX7xx models), 0–13 (ERX14xx models), and 0–2 (ERX310 router) ■ <i>port</i>—Port number on the I/O module ■ <i>subinterface</i>—Number of the subinterface in the range 1–2147483647 	pos 3/2
serial	CT3, E3 Frame, T3 Frame, or cOCx/STMx interface	Refer to the individual formats listed below.	
■ CT3		<code>slot/port:channel/subchannel[.subinterface]</code> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–6 (ERX7xx models) and 0–13 (ERX14xx models) ■ <i>port</i>—Port number on the I/O module ■ <i>channel</i>—Number of a T1 channel on a CT3 module; in the range 1–28 ■ <i>subchannel</i>—Number of the channel group associated with a range of DS0 timeslots on a CT3 module; in the range 1–28 ■ <i>subinterface</i>—Number of the subinterface in the range 1–2147483647 	serial 3/2:20/15
■ E3/T3 Frame		<code>slot/port[.subinterface]</code> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–6 (ERX7xx models) and 0–13 (ERX14xx models) ■ <i>port</i>—Port number on the I/O module ■ <i>subinterface</i>—Number of the subinterface in the range 1–2147483647 	serial 3/2

Table 3: Interface Types and Specifiers for ERX7xx Models, ERX14xx Models, and ERX310 Router (continued)

Interface Type	Description	Interface Specifier	Example
■ cOCx/STMx: unframed E1		<i>slot/port/path-channel/path-payload/ tributary-group/tributary-number/ channelNumber[.subinterface]</i> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–6 (ERX7xx models), 0–13 (ERX14xx models), and 0–2 (ERX310 router) ■ <i>port</i>—Port number on the I/O module ■ <i>path-channel</i>—Number of the STS-1 or STM-0 line in the range 1–2147483648 ■ <i>path-payload</i>—Number of the payload within the path ■ <i>tributary-group</i>—Number of the tributary group within the path ■ <i>tributary-number</i>—Number of the tributary within the group ■ <i>channelNumber</i>—1 (the router assigns the number one to an unframed E1 channel) ■ <i>subinterface</i>—Number of the subinterface in the range 1–2147483647 	serial 3/0:10/1/2/2/1
■ cOCx/STMx: fractional E1/T1		<i>slot/port/path-channel/path-payload/ tributary-group/tributary-number/ channel-group[.subinterface]</i> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–6 (ERX7xx models), 0–13 (ERX14xx models), and 0–2 (ERX310 router) ■ <i>port</i>—Port number on the I/O module ■ <i>path-channel</i>—Number of the STS-1 or STM-0 line in the range 1–2147483648 ■ <i>path-payload</i>—Number of the payload within the path ■ <i>tributary-group</i>—Number of the tributary group within the path ■ <i>tributary-number</i>—Number of the tributary within the group ■ <i>channel-group</i>—Number of a fractional T1 or E1 line ■ <i>subinterface</i>—Number of the subinterface in the range 1–2147483647 	serial 3/0:10/1/2/2/1

Table 3: Interface Types and Specifiers for ERX7xx Models, ERX14xx Models, and ERX310 Router (continued)

Interface Type	Description	Interface Specifier	Example
■ cOCx/STMx: unchannelized DS3		<i>slot/port:path-channel/ds3-channel-number</i> [.subinterface] <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–6 (ERX7xx models), 0–13 (ERX14xx models), and 0–2 (ERX310 router) ■ <i>port</i>—Port number on the I/O module ■ <i>path-channel</i>—Number of the STS-1 or STM-0 line in the range 1–2147483648 ■ <i>ds3-channel-number</i>—Number of a T3 channel ■ <i>subinterface</i>—Number of the subinterface in the range 1–2147483647 	serial 3/0:1/1
■ cOCx/STMx: DS3 channelized to DS0		<i>slot/port:path-channel/ds3-channel-number/ ds1-channel-number/subchannel-number</i> [.subinterface] <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–6 (ERX7xx models), 0–13 (ERX14xx models), and 0–2 (ERX310 router) ■ <i>port</i>—Port number on the I/O module ■ <i>path-channel</i>—Number of the STS-1 or STM-0 line in the range 1–2147483648 ■ <i>ds3-channel-number</i>—Number of a T3 channel ■ <i>ds1-channel-number</i>—Number of a T1 channel ■ <i>subchannel-number</i>—Number of a fractional T1 channel ■ <i>subinterface</i>—Number of the subinterface in the range 1–2147483647 	serial 3/0:1/1/10/15
sonet – line layer	Line layer of a SONET/SDH interface	<i>slot/port</i> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–6 (ERX7xx models), 0–13 (ERX14xx models), and 0–2 (ERX310 router) ■ <i>port</i>—Port number on the I/O module 	sonet 3/0

Table 3: Interface Types and Specifiers for ERX7xx Models, ERX14xx Models, and ERX310 Router (continued)

Interface Type	Description	Interface Specifier	Example
sonet – path layer	Path layer of a SONET/SDH interface	<i>slot/port:path-channel</i> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–6 (ERX7xx models), 0–13 (ERX14xx models), and 0–2 (ERX310 router) ■ <i>port</i>—Port number on the I/O module ■ <i>path-channel</i>—Number of the STS-1 or STM-0 line in the range 1–2147483648 	sonet 3/0:2
sonet – section layer	Section layer of a SONET/SDH interface	<i>slot/port</i> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–6 (ERX7xx models), 0–13 (ERX14xx models), and 0–2 (ERX310 router) ■ <i>port</i>—Port number on the I/O module 	sonet 3/0
tunnel	Tunnel interface	<i>tunnel-type:tunnel-name[.subinterface]</i> <ul style="list-style-type: none"> ■ <i>tunnel-type</i>—Type of the tunnel: dvmrp, gre, ipsec, l2tp, or mpls ■ <i>tunnel-name</i>—Name of the tunnel ■ <i>subinterface</i>—For GRE tunnels, number of the subinterface in the range 1–2147483647 	tunnel gre:boston

Table 4: Interface Types and Specifiers for E120 Router and E320 Router

Interface Type	Description	Interface Specifier	Example
atm	ATM interface or ATM 1483 subinterface	Refer to the individual formats listed below.	

Table 4: Interface Types and Specifiers for E120 Router and E320 Router (*continued*)

Interface Type	Description	Interface Specifier	Example
■ ATM interface or subinterface	To configure an ATM interface or subinterface:	<code>slot/adapter/port[.subinterface]</code> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–5 (E120 router) and 0–5 or 11–16 (E320 router) ■ <i>adapter</i>—Identifier for the IOA within the chassis slot, either 0 or 1, where: <ul style="list-style-type: none"> ■ 0 indicates that the IOA is installed in the right IOA bay (E120 router) or the upper IOA bay (E320 router). ■ 1 indicates that the IOA is installed in the left IOA bay (E120 router) or the lower IOA bay (E320 router). ■ <i>port</i>—Port number on the IOA ■ <i>subinterface</i>—Number of the subinterface in the range 1–2147483647 	atm 3/1/7.6
■ ATM 1483 subinterface	To display information about an ATM 1483 subinterface by using show commands:	<code>slot/adapter/port/vpi/vci</code> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–5 (E120 router) and 0–5 or 11–16 (E320 router) ■ <i>adapter</i>—Identifier for the IOA within the chassis slot, either 0 or 1, where: <ul style="list-style-type: none"> ■ 0 indicates that the IOA is installed in the right IOA bay (E120 router) or the upper IOA bay (E320 router). ■ 1 indicates that the IOA is installed in the left IOA bay (E120 router) or the lower IOA bay (E320 router). ■ <i>port</i>—Port number on the IOA ■ <i>vpi</i>—Virtual path identifier of the PVC on this ATM 1483 subinterface; numeric range for the E120 and E320 routers is 0–255 ■ <i>vci</i>—Virtual circuit identifier of the PVC on this ATM 1483 subinterface; numeric range for the E120 and E320 routers is 1–65535 	atm 3/1/7/1/2

Table 4: Interface Types and Specifiers for E120 Router and E320 Router (continued)

Interface Type	Description	Interface Specifier	Example
fastEthernet (for Fast Ethernet management port on SRP IOA)	IEEE 802.3 Fast Ethernet (FE) interface	<i>slot/adapter/port</i> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot, either 6 or 7 ■ <i>adapter</i>—Identifier for the SRP I/O adapter (IOA) within the chassis slot; always 0 ■ <i>port</i>—Port number on the SRP IOA; always 0 	fastEthernet 6/0/0
gigabitEthernet	IEEE 802.3 Gigabit Ethernet (GE) interface	<i>slot/adapter/port[.subinterface1[.subinterface2]]</i> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–5 (E120 router) and 0–5 or 11–16 (E320 router) ■ <i>adapter</i>—Identifier for the IOA within the chassis slot, either 0 or 1, where: <ul style="list-style-type: none"> ■ 0 indicates that the IOA is installed in the right IOA bay (E120 router) or the upper IOA bay (E320 router). ■ 1 indicates that the IOA is installed in the left IOA bay (E120 router) or the lower IOA bay (E320 router). ■ <i>port</i>—Port number on the IOA The meaning of the <i>subinterface</i> variables depends on the configuration context. You can configure Gigabit Ethernet interfaces with or without VLANs. ■ VLANs: <ul style="list-style-type: none"> ■ <i>subinterface1</i>—Number of the VLAN subinterface in the range 1–2147483647; no more than 4096 VLAN subinterfaces per Gigabit Ethernet physical port ■ <i>subinterface2</i>—When using PPPoE, the number of the PPPoE subinterface in the range 1–2147483647; no more than 16,000 PPPoE subinterfaces per Gigabit Ethernet line module ■ No VLANs: <ul style="list-style-type: none"> ■ <i>subinterface1</i>—When using PPPoE, the number of the PPPoE subinterface in the range 1–2147483647; no more than 16,000 PPPoE subinterfaces per Gigabit Ethernet line module ■ <i>subinterface2</i>—Not used 	gigabitEthernet 4/0/1.20

Table 4: Interface Types and Specifiers for E120 Router and E320 Router (continued)

Interface Type	Description	Interface Specifier	Example
lag	IEEE 802.3ad link aggregation group (LAG) interface	<i>bundle-name[.subinterface]</i> ■ <i>bundle-name</i> —Name of the bundle ■ <i>subinterface</i> —Number of the LAG subinterface in the range 1–2147483647	lag paris.2
mplsL2shim	MPLS shim interface	<i>slot/adapter/port[.subinterface]</i> ■ <i>slot</i> —Number of the chassis slot in the range 0–5 (E120 router) and 0–5 or 11–16 (E320 router) ■ <i>adapter</i> —Identifier for the IOA within the chassis slot, either 0 or 1, where: ■ 0 indicates that the IOA is installed in the right IOA bay (E120 router) or the upper IOA bay (E320 router). ■ 1 indicates that the IOA is installed in the left IOA bay (E120 router) or the lower IOA bay (E320 router). ■ <i>port</i> —Port number on the IOA ■ <i>subinterface</i> —Number of the subinterface in the range 1–2147483647	mplsL2shim 3/0/2.1
mplsMajor	MPLS major interface	<i>slot/adapter/port[.subinterface]</i> ■ <i>slot</i> —Number of the chassis slot in the range 0–5 (E120 router) and 0–5 or 11–16 (E320 router) ■ <i>adapter</i> —Identifier for the IOA within the chassis slot, either 0 or 1, where: ■ 0 indicates that the IOA is installed in the right IOA bay (E120 router) or the upper IOA bay (E320 router). ■ 1 indicates that the IOA is installed in the left IOA bay (E120 router) or the lower IOA bay (E320 router). ■ <i>port</i> —Port number on the IOA ■ <i>subinterface</i> —Number of the subinterface in the range 1–2147483647	mplsMajor 3/0/2.1
mplsMinor	MPLS minor interface	<i>[vr:]tunnel-name</i> ■ <i>vr</i> —Name of a virtual router ■ <i>tunnel-name</i> —Name of the tunnel	mplsMinor lsp-02020202-1-4

Table 4: Interface Types and Specifiers for E120 Router and E320 Router (continued)

Interface Type	Description	Interface Specifier	Example
pos	Packet over SONET (POS) interface	<i>slot/adapter/port</i> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–5 (E120 router) and 0–5 or 11–16 (E320 router) ■ <i>adapter</i>—Identifier for the IOA within the chassis slot, either 0 or 1, where: <ul style="list-style-type: none"> ■ 0 indicates that the IOA is installed in the right IOA bay (E120 router) or the upper IOA bay (E320 router). ■ 1 indicates that the IOA is installed in the left IOA bay (E120 router) or the lower IOA bay (E320 router). ■ <i>port</i>—Port number on the IOA 	pos 5/0/0
sonet – line layer	Line layer of a SONET/SDH interface	<i>slot/adapter/port</i> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–5 (E120 router) and 0–5 or 11–16 (E320 router) ■ <i>adapter</i>—Identifier for the IOA within the chassis slot, either 0 or 1, where: <ul style="list-style-type: none"> ■ 0 indicates that the IOA is installed in the right IOA bay (E120 router) or the upper IOA bay (E320 router). ■ 1 indicates that the IOA is installed in the left IOA bay (E120 router) or the lower IOA bay (E320 router). ■ <i>port</i>—Port number on the IOA 	sonet 3/0/0
sonet – path layer	Path layer of a SONET/SDH interface	<i>slot/adapter/port</i> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–5 (E120 router) and 0–5 or 11–16 (E320 router) ■ <i>adapter</i>—Identifier for the IOA within the chassis slot, either 0 or 1, where: <ul style="list-style-type: none"> ■ 0 indicates that the IOA is installed in the right IOA bay (E120 router) or the upper IOA bay (E320 router). ■ 1 indicates that the IOA is installed in the left IOA bay (E120 router) or the lower IOA bay (E320 router). ■ <i>port</i>—Port number on the IOA 	sonet 3/0/0

Table 4: Interface Types and Specifiers for E120 Router and E320 Router (continued)

Interface Type	Description	Interface Specifier	Example
sonet – section layer	Section layer of a SONET/SDH interface	<code>slot/adapter/port</code> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–5 (E120 router) and 0–5 or 11–16 (E320 router) ■ <i>adapter</i>—Identifier for the IOA within the chassis slot, either 0 or 1, where: <ul style="list-style-type: none"> ■ 0 indicates that the IOA is installed in the right IOA bay (E120 router) or the upper IOA bay (E320 router). ■ 1 indicates that the IOA is installed in the left IOA bay (E120 router) or the lower IOA bay (E320 router). ■ <i>port</i>—Port number on the IOA 	sonet 3/0/0
tenGigabitEthernet	IEEE 802.3ae 10-Gigabit Ethernet (GE) interface	<code>slot/adapter/port[.subinterface1[.subinterface2]]</code> <ul style="list-style-type: none"> ■ <i>slot</i>—Number of the chassis slot in the range 0–5 (E120 router) and 0–5 or 11–16 (E320 router) ■ <i>adapter</i>—Identifier for the IOA within the chassis slot. 0 indicates that this is a full-height IOA. ■ <i>port</i>—Port number on the IOA <p>The meaning of the <i>subinterface</i> variables depends on the configuration context. You can configure 10-Gigabit Ethernet interfaces with or without VLANs.</p> <ul style="list-style-type: none"> ■ VLANs: <ul style="list-style-type: none"> ■ <i>subinterface1</i>—Number of the VLAN subinterface in the range 1–2147483647; no more than 4096 VLAN subinterfaces per 10-Gigabit Ethernet physical port ■ <i>subinterface2</i>—When using PPPoE, the number of the PPPoE subinterface in the range 1–2147483647; no more than 16,000 PPPoE subinterfaces per 10-Gigabit Ethernet line module ■ No VLANs: <ul style="list-style-type: none"> ■ <i>subinterface1</i>—When using PPPoE, the number of the PPPoE subinterface in the range 1–2147483647; no more than 16,000 PPPoE subinterfaces per 10-Gigabit Ethernet line module ■ <i>subinterface2</i>—Not used 	tenGigabitEthernet 4/0/1.20

Table 4: Interface Types and Specifiers for E120 Router and E320 Router *(continued)*

Interface Type	Description	Interface Specifier	Example
tunnel	Tunnel interface	<i>tunnel-type:tunnel-name[.subinterface]</i> <ul style="list-style-type: none"> ■ <i>tunnel-type</i>—Type of the tunnel: dvmrp, gre, l2tp, or mpls ■ <i>tunnel-name</i>—Name of the tunnel ■ <i>subinterface</i>—For GRE tunnels, number of the subinterface in the range 1–2147483647 	tunnel gre:boston

Chapter 2

A Commands

aaa accounting acct-stop on-aaa-failure

Syntax aaa accounting acct-stop on-aaa-failure { enable | disable }
no aaa accounting acct-stop on-aaa-failure

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures AAA to send an Acct-Stop message if a user fails AAA, but RADIUS grants access. The **no** version returns the parameter to the default of enable.

- Options**
- enable—Specifies the feature; this is the default setting
 - disable—Disables the feature

Mode Global Configuration

aaa accounting acct-stop on-access-deny

Syntax aaa accounting acct-stop on-access-deny { enable | disable }
no aaa accounting acct-stop on-access-deny

Release Information Command introduced before JUNOS Release 7.1.0.

Description Issues an Acct-Stop message if RADIUS denies access. The **no** version returns the parameter to the default of disable.

- Options**
- enable—Specifies the feature
 - disable—Disables the feature; this is the default setting

Mode Global Configuration

aaa accounting broadcast

Syntax `aaa accounting broadcast vrGroupName`
 `no aaa accounting broadcast`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Broadcasts accounting records for a virtual router to accounting servers of the virtual routers in the specified virtual router group. The **no** version disables the feature.

Options ■ *vrGroupName*—Name of the virtual router group; a string of up to 32 characters

Mode Global Configuration

aaa accounting commands

Syntax `aaa accounting commands level { default | listName } stop-only tacacs +`
 `no aaa accounting commands level listName`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables AAA accounting for TACACS+ to be captured for a specific user privilege level and creates accounting method lists. The **no** version deletes the accounting method list.

- Options**
- *level*—Privilege level of user commands for which accounting information is captured; in the range 0–15
 - *default*—Specifies that the default method list is used to specify how accounting is performed
 - *listName*—Named method list used to specify how accounting is performed
 - *stop-only*—Sends a stop accounting notice at the end of a process

Mode Global Configuration

aaa accounting default

Syntax `aaa accounting { subscriberType } default accountor [accountor]*`
 `no aaa accounting { subscriberType } default`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the accounting method used for a particular type of subscriber. The **no** version produces the same result as specifying the **radius** value.

- Options**
- *subscriberType*—Type of subscriber:
 - atm1483—Specifies ATM 1483 subscribers; not supported
 - ip—Specifies IP subscriber management interfaces
 - ipsec—Specifies IPSec subscribers
 - ppp—Specifies PPP subscribers
 - radius-relay—Specifies RADIUS relay server subscribers
 - tunnel—Specifies tunnel subscribers
 - *accountor*—Accounting method:
 - none—Disables accounting
 - radius—Enables RADIUS accounting
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

aaa accounting duplication

Syntax `aaa accounting duplication routerName`
 `no aaa accounting duplication`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sends duplicate accounting records to the accounting server of a different virtual router. The **no** version disables the feature.

Options ■ *routerName*—Virtual router name

Mode Global Configuration

aaa accounting exec

Syntax `aaa accounting exec { default | listName } start-stop tacacs +`
`no aaa accounting exec listName`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables AAA accounting for TACACS+ to be captured for User Exec terminal sessions, and creates accounting method lists. The **no** version deletes the accounting method list.

- Options**
- `exec`—Specifies that accounting information is captured for User Exec terminal sessions
 - `default`—Specifies that the default method list is used to specify how accounting is performed
 - `listName`—Named method list used to specify how accounting is performed
 - `start-stop`—Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a successful process

Mode Global Configuration

aaa accounting immediate-update

Syntax aaa accounting immediate-update { enable | disable }
no aaa accounting immediate-update

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the router to send an Acct-Update message to the accounting server on receipt of a response (ACK or timeout) for the Acct-Start message. The **no** version restores the default condition, disabling immediate updates.

- Options**
- enable—Specifies the feature
 - disable—Disables the feature; this is the default setting

Mode Global Configuration

aaa accounting interval

Syntax `aaa accounting interval period`
`no aaa accounting interval`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the default accounting interval used for all users and services. The **no** version sets the value to 0, which turns off interim accounting.



NOTE: This command is deprecated and might be removed completely in a future release. Use the **aaa service accounting interval** and **aaa user accounting interval** commands to configure default accounting intervals for services and users.

Options ■ *period*—Accounting interval in minutes in the range 10–1440, which sets the time period between accounting updates

Mode Global Configuration

aaa accounting statistics

Syntax aaa accounting statistics { volume-time | time }

 no aaa accounting statistics

Release Information Command introduced in JUNOS Release 7.2.0.

Description Configures the router to collect either a full set of statistics or only uptime status for the sessions AAA is managing. Collecting only the uptime status is a more efficient use of system resources. The **no** version restores the default setting in which the router collects full statistics.

- Options**
- volume-time—Collects a full complement of statistics from each connection; the default setting
 - time—Collects only uptime status for each connection

Mode Global Configuration

aaa accounting suppress null-username

Syntax [no] aaa accounting suppress null-username

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that accounting records are not generated for users whose username string is null; accounting records will be generated only for users with explicit usernames. The **no** version enables accounting records to be generated for all users, including those who do not have usernames.

Mode Global Configuration

aaa accounting vr-group

Syntax [no] aaa accounting vr-group *vrGroupName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates an accounting virtual router group and enters VR Group Configuration mode. A virtual router group can have up to four virtual routers, whose accounting servers can receive broadcast accounting records. A group must contain at least one virtual router. The **no** version deletes the accounting virtual router group.

Options ■ *vrGroupName*—Name of the virtual router group; a string of up to 32 characters

Mode Global Configuration

aaa authentication default

Syntax `aaa authentication subscriberType default authenticator [authenticator]*`
 `no aaa authentication subscriberType default`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the authentication method used for a particular type of subscriber. The **no** version produces the same result as specifying the **radius** value.

- Options**
- *subscriberType*—Type of subscriber:
 - atm1483—Specifies ATM 1483 subscribers
 - ip—Specifies IP subscriber management interfaces
 - ipsec—Specifies IPSec subscribers
 - ppp—Specifies PPP subscribers
 - radius-relay—Specifies RADIUS relay server subscribers
 - tunnel—Specifies tunnel subscribers
 - *authenticator*—Authentication method:
 - none—Disables authentication, allowing all users access
 - local—Enables local authentication; supported for PPP subscribers only
 - radius—Enables RADIUS for authentication
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

aaa authentication enable default

Syntax aaa authentication enable default *authenticator* [*authenticator*]*
no aaa authentication enable default

Release Information Command introduced before JUNOS Release 7.1.0.

Description Allows privilege determination to be authenticated through the authenticator(s) you specify. This authentication is applied to vty users. The **no** version removes the authentication settings.

- Options** ■ *authenticator*—Authentication method:
- enable—Use the enable password
 - line—Use the line password
 - none—Use no authentication
 - radius—Use RADIUS authentication
 - tacacs + —Use TACACS+ authentication
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

aaa authentication login

Syntax `aaa authentication login { default | authListName } authenticator [authenticator]*`
 `no aaa authentication login authListName`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates an authentication list and the criteria for login. This authentication is applied to vty users. The **no** version disables AAA authentication.

- Options**
- *default*—Specifies the use of the default login for authentication
 - *authListName*—Existing authentication list name (created using the **login authentication** command); a string of 1–32 characters
 - *authenticator*—Authentication method:
 - *line*—Use the line password for authentication
 - *none*—Use no authentication
 - *radius*—Use RADIUS authentication
 - *tacacs +* —Use TACACS+ authentication
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

aaa authorization

Syntax `aaa authorization { exec | commands level } authorListName authMethod [authMethod]*`

`no aaa authorization { exec | commands level } authorListName`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets parameters that restrict a user's access to a network. The **no** version disables authorization for a function.

- Options**
- *exec*—Runs authorization to determine if the user is allowed to run Exec mode commands
 - *level*—Privilege level of commands for which authorization is run; in the range 0–15
 - *authorListName*—Name of the authorization methods list of up to 32 characters
 - *authMethod*—Authorization method:
 - *if-authenticated*—Allows the user to access the requested function if the user is authenticated
 - *none*—NAS does not request authorization information; authorization is not performed over this line
 - *tacacs +* —NAS exchanges authorization information with the TACACS + security daemon
 - ***—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

aaa authorization config-commands

Syntax [no] aaa authorization config-commands

Release Information Command introduced before JUNOS Release 7.1.0.

Description Reauthorizes the use of Global Configuration commands. This command is enabled by default when the **aaa authorization commands** command is executed. The **no** version disables AAA configuration command authorization.



NOTE: Using the **no** version can potentially reduce the amount of administrative control on configuration commands.

Mode Global Configuration

aaa delimiter

Syntax `aaa delimiter { domainName | realmName } delimiters`
 `no aaa delimiter { domainName | realmName }`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies delimiters for the domain and realm names. You can specify up to eight delimiters each for domain and realm names. The **no** version restores the default value.

- Options**
- `domainName`—Allows you to set delimiters for the domain name
 - `realmName`—Allows you to set delimiters for the realm name
 - `delimiters`—Either the domain or realm delimiter(s). You can specify up to eight characters.
 - The default domain name delimiter is `@`.
 - The default realm name delimiter is NULL (no character). In this case, realm parsing is disabled (having no delimiter disables realm parsing).

Mode Global Configuration

aaa dhcpv6-delegated-prefix delegated-ipv6-prefix

Syntax [no] aaa dhcpv6-delegated-prefix delegated-ipv6-prefix

Release Information Command introduced in JUNOS Release 10.1.0.

Description Sets the Delegated-IPv6-Prefix RADIUS attribute to be used for DHCPv6 Prefix Delegation. The **no** version restores the default behavior, which causes the Framed-IPv6-Prefix RADIUS attribute to be used for Prefix Delegation.



NOTE: If you configured the Framed-IPv6-Prefix attribute to be used for IPv6 Neighbor Discovery router advertisements by using the **aaa ipv6-nd-ra-prefix framed-ipv6-prefix** command, you must also issue the **aaa dhcpv6-delegated-prefix delegated-ipv6-prefix** command after you issue the **aaa ipv6-nd-ra-prefix framed-ipv6-prefix** command to enable the use of the Delegated-IPv6-Prefix attribute for DHCPv6 Prefix Delegation. Otherwise, the Framed-IPv6-Prefix attribute will be used for both IPv6 Neighbor Discovery router advertisements and DHCPv6 Prefix Delegation.

Mode Global Configuration

aaa dns

Syntax `aaa dns { primary | secondary } ipAddress`
`no aaa dns { primary | secondary }`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the IP address of the primary DNS name server. The **no** version sets the corresponding address to 0.

- Options**
- `primary`—Specifies the primary DNS name server
 - `secondary`—Specifies the secondary DNS name server
 - `ipAddress`—IP address of the name server

Mode Global Configuration

aaa domain-map

Syntax `aaa domain-map domainName`
 `[routerName [loopback interfaceNumber | ipAddress ipMask]]`

 `no aaa domain-map domainName`

Release Information Command introduced before JUNOS Release 7.1.0.
 ipAddress and *ipMask* variables added in JUNOS Release 9.0.0.

Description Maps a user domain name to a virtual router. When you specify only the domain name, the command sets the mode to Domain Map Configuration. The **no** version deletes the map entry.

- Options**
- *domainName*—User domain name; specify the domain name *none* to assign users without domains to a specific virtual router.
 - *routerName*—Router name associated with the domain name
 - *loopback*—Specifies the loopback interface
 - *interfaceNumber*—Interface number in the range 0–32000
 - *ipAddress*—IP address of the local interface
 - *ipMask*—IPv4 address mask of the local interface

Mode Global Configuration

aaa duplicate-address-check

Syntax aaa duplicate-address-check { enable | disable }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Allows you to enable or disable routing table address lookup or duplicate address check. There is no **no** version.



NOTE: To use this command, you must have a B-RAS license. Run the **license b-ras** command and enter your password.

- Options**
- enable—Specifies the feature; this is the default
 - disable—Disables the feature

Mode Global Configuration

aaa intf-desc-format include

Syntax aaa intf-desc-format include { sub-intf | adapter } { enable | disable }
 no aaa intf-desc-format include { sub-intf | adapter }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies whether the subinterface or adapter is included in or omitted from the interface description that the router passes to RADIUS for inclusion in the NAS-Port-Id attribute. Also affects the Interface field displayed by the **show subscribers** command. The **no** version restores the default, in which the subinterface and adapter are included.

- Options**
- sub-intf—Specifies that the subinterface is included in or omitted from the interface description
 - adapter—Specifies that the adapter is included in or omitted from the interface description
 - enable—Includes the subinterface or adapter in the interface description; this is the default
 - disable—Omits the subinterface or adapter from the interface description

Mode Global Configuration

aaa ipv6-dns

Syntax `aaa ipv6-dns { primary | secondary } ipv6Address`
`no aaa ipv6-dns { primary | secondary }`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the IPv6 address of the primary DNS name server. The **no** version sets the corresponding address to 0 (or ::).

- Options**
- `primary`—Specifies the primary DNS name server
 - `secondary`—Specifies the secondary DNS name server
 - `ipv6Address`—IPv6 address of the name server

Mode Global Configuration

aaa ipv6-nd-ra-prefix framed-ipv6-prefix

Syntax [no] aaa ipv6-nd-ra-prefix framed-ipv6-prefix

Release Information Command introduced in JUNOS Release 10.1.0.

Description Sets the Framed-IPv6-Prefix RADIUS attribute to be used for IPv6 Neighbor Discovery router advertisements. The **no** version restores the default behavior, which causes the IPv6-NdRa-Prefix VSA to be used for router advertisements.



NOTE: If you issue this command before issuing the **aaa dhcpv6-delegated-prefix delegated-ipv6-prefix** command, a warning message is displayed prompting you to configure the Delegated-IPv6-Prefix attribute for DHCPv6 Prefix Delegation. The message also states that the Framed-IPv6-Prefix RADIUS attribute will be used for both IPv6 Neighbor Discovery router advertisements and DHCPv6 Prefix Delegation if you do not configure the Delegated-IPv6-Prefix attribute for Prefix Delegation.

This warning message is displayed only if you configured the logging severity level as warning for the aaaServerGeneral logging event category.

Mode Global Configuration

aaa local database

Syntax [no] aaa local database *databaseName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates a local user database for use by a local authentication server. The **no** version deletes the local user database and all entries in the database.

Options ■ *databaseName*—Name of the user database; up to 32 characters; the name **default** is recognized as the default user database

Mode Global Configuration

aaa local select database

Syntax aaa local select database *databaseName*
 no aaa local select

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns the local user database that the virtual router uses for local authentication. The **no** version restores the default setting, which uses the default local user database for local authentication.

Options ■ *databaseName*—Name of the local user database

Mode Global Configuration

aaa local username

Syntax [no] aaa local username *userName* database *databaseName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures a user entry in the specified local user database and enters Local User Configuration mode. The **no** version deletes the user entry from the specified local user database.

- Options**
- *userName*—User name of the subscriber
 - *databaseName*—Name of the local user database; database name **default** configures the username in the default local user database

Mode Global Configuration

aaa new-model

Syntax [no] aaa new-model

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies AAA authentication for Telnet sessions. The **no** version restores simple authentication (login and password).

Mode Global Configuration

aaa parse-direction

Syntax `aaa parse-direction { domainName | realmName } { left-to-right | right-to-left }`
 `no aaa parse-direction { domainName | realmName }`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the direction the router uses for domain and realm parsing. The router either searches from right-to-left, or from left-to-right. If searching for the realm, the router uses the realm delimiter valued in its search. If searching for the domain, it uses the domain delimiter values in its search. The **no** version returns the parse direction to the default setting.

- Options**
- `domainName`—Specifies that the domain name is parsed. The router performs domain searches from right-to-left by default.
 - `realmName`—Specifies that the realm name is parsed. The router performs realm searches from left-to-right by default.
 - `left-to-right`—Causes the router to search from the left-most character. When the router reaches a realm delimiter, it uses anything to the left of the delimiter as the domain. When the router reaches a domain delimiter, it uses anything to the right of the delimiter as the domain.
 - `right-to-left`—Causes the router to search from the right-most character. When the router reaches a realm delimiter, it uses anything to the left of the delimiter as the domain. When the router reaches a domain delimiter, it uses anything to the right of the delimiter as the domain.

Mode Global Configuration

aaa parse-order

Syntax aaa parse-order { domain-first | realm-first }

 no aaa parse-order

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the order in which the router searches for a domain name. It either searches for realm and then domain, or it searches for domain and then realm. The **no** version returns the parse order to the default of searching for realm first.

- Options**
- domain-first—Causes the router to search for a domain name first. When the router reaches a domain delimiter, it uses anything to the right of the delimiter as the domain name.
 - realm-first—Causes the router to search for a realm name first. When the router reaches a realm delimiter, it uses anything to the left of the delimiter as the domain name.

Mode Global Configuration

aaa profile

Syntax [no] aaa profile *profileName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates a new AAA profile to allow mapping to AAA services. The **no** version removes the profile.

Options ■ *profileName*—Profile name of up to 32 characters

Mode AAA Profile Configuration

aaa qos downstream-rate

Syntax [no] aaa qos downstream-rate

Release Information Command introduced in JUNOS Release 8.1.0.

Description Enables the QoS downstream rate application to shape VLANs or ATM VCs based on downstream rates obtained from the Actual-Data-Rate-Downstream [26-130] DSL Forum VSA. The **no** version returns the parameter to the default of disabled.

Mode Global Configuration

aaa route-download

Syntax `aaa route-download [downloadInterval] [retry-interval retryInterval]`
 `[cost cost] [tag tagValue] [base-user-name name] [password password]`
 `[synchronization time]`

`no aaa route-download`

Release Information Command introduced in JUNOS Release 8.1.0.

Description Enables the RADIUS route-download server and configures parameters for the server. The **no** version disables the route-download server.

- Options**
- *downloadInterval*—Interval between download operations, in the range 1–1440 minutes; default is 720 minutes
 - *retryInterval*—Interval between retries after a failed download, in the range 1–60 minutes; default is 10 minutes
 - *cost*—Default cost of a downloaded route, in the range 1–254; default is 2
 - *tagValue*—Default tag of a downloaded route, in the range 1–4294967295; default is 0
 - *name*—Name of router used for route-download requests; default is the router hostname
 - *password*—Password used for route-download requests
 - *time*—Time the download operation is restarted each day, in 24-hour format (hh:mm:ss)

Mode Global Configuration

aaa route-download now

Syntax aaa route-download now [force] [adjust-scheduler]

Release Information Command introduced in JUNOS Release 8.1.0.

Description Specifies that the RADIUS route-download server immediately perform the route download operation. If a download is currently in progress when you issue this command without the **force** keyword, the in-progress download continues until complete and no additional download is started. There is no **no** version.

- Options**
- force—Interrupts any in-progress route-download operation and immediately starts a new download.
 - adjust-scheduler—Resets the download scheduler to use this download as the start time for synchronizing download counts

Mode Privileged Exec

aaa route-download suspend

Syntax [no] aaa route-download suspend

Release Information Command introduced in JUNOS Release 8.1.0.

Description Temporarily suspends the RADIUS route-download server operation. The **no** version stops the suspend specification and restores the route download operation.

Mode Privileged Exec

aaa service accounting interval

Syntax `aaa service accounting interval period`
`no aaa service accounting interval`

Release Information Command introduced in JUNOS Release 9.0.0.

Description Specifies the default accounting interval used for services on the virtual router—the Service Manager application uses this setting for RADIUS-initiated services when no value is specified in the Service-Interim-Acct-Interval VSA (Juniper VSA 26-140). The **no** version restores the default setting of 0, which turns off interim accounting for services associated with users attached to this virtual router.



NOTE: This command and the **aaa user accounting interval** command replace the deprecated **aaa accounting interval** command, which may be removed completely in a future release.

Options ■ *period*—Accounting interval in minutes in the range 10–1440, which sets the time period between accounting updates for services associated with users on this virtual router; 0 is the default

Mode Global Configuration

aaa subscriber limit per-port

Syntax `aaa subscriber limit per-port interfaceSpecifier limitValue`
 `no aaa subscriber limit per-port interfaceSpecifier`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the maximum number of active subscribers permitted on the specified port. The **no** version returns the limit to the default, 0 (zero).

- Options** ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
- *limitValue*—Maximum number of subscribers; default value is 0 (zero), which means there is no limit on the number of subscribers

Mode Global Configuration

aaa subscriber limit per-vr

Syntax aaa subscriber limit per-vr *limitValue*
 no aaa subscriber limit per-vr

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the maximum number of active subscribers permitted on the virtual router. The **no** version returns the limit to the default, 0 (zero).

Options ■ *limitValue*—Maximum number of subscribers; default value is 0 (zero), which means there is no limit on the number of subscribers

Mode Global Configuration

aaa timeout

Syntax To set the default idle timeout:

aaa timeout idle *idleTimeout*

no aaa timeout idle

To set the default session timeout:

aaa timeout session *sessionTimeout*

no aaa timeout session

To enable monitoring of only ingress traffic for the configured idle timeout period:

aaa timeout idle ingress-only

no aaa timeout idle [ingress-only]

Release Information Command introduced before JUNOS Release 7.1.0.
ingress-only keyword added in JUNOS Release 9.3.0.

Description Sets the default idle timeout or session timeout for B-RAS PPP users, and optionally enables the PPP application to monitor only ingress traffic for the configured idle timeout period to determine whether to disconnect an inactive PPP session. The **no** version restores the idle timeout or session timeout to its default value, 0 seconds, and disables ingress-only traffic monitoring for idle timeout if configured. .



NOTE: To enable ingress-only traffic monitoring for the idle timeout period by issuing the **aaa timeout idle ingress-only** command, you must also set the idle timeout value by issuing the **aaa timeout idle** command.

- Options**
- *idleTimeout*—In seconds, 300–86400
 - *sessionTimeout*—Time in the range 60–31 622 400 seconds (that is, a minimum of 1 minute to a maximum of 366 days); the router terminates the user session once the maximum session timeout is reached, which means that the duration of a PPP or an L2TP user session cannot exceed 366 days
 - **ingress-only**—Enables PPP to monitor only ingress traffic for the configured idle timeout period to determine whether to disconnect an inactive PPP session; if you do not specify the **ingress-only** keyword, PPP monitors both ingress traffic and egress traffic for the idle timeout period to determine inactivity and subsequent disconnection of an inactive PPP session

Mode Global Configuration

aaa tunnel assignment-id-format

Syntax aaa tunnel assignment-id-format { assignmentId | client-server-id }
no aaa tunnel assignment-id-format

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the format for the tunnel assignment ID. The **no** version sets the tunnel assignment ID to the default, assignmentID.

- Options**
- assignmentId—Configures the format to be assignmentId only
 - client-server-id—Configures the format to be a combination of clientAuthId + serverAuthId + assignmentId

Mode Global Configuration

aaa tunnel calling-number-format

Syntax aaa tunnel calling-number-format
 { descriptive [include-agent-circuit-id] [include-agent-remote-id] |
 fixed [stacked] |
 fixed-adapter-embedded [stacked] |
 fixed-adapter-new-field [stacked] |
 include-agent-circuit-id [include-agent-remote-id] |
 include-agent-remote-id }

no aaa tunnel calling-number-format

Release Information Command introduced before JUNOS Release 7.1.0.
 include-agent-circuit-id and **include-agent-remote-id** keywords added in JUNOS Release 8.1.0.
 stacked keyword added in JUNOS Release 9.3.0.
 fixed-adapter-embedded and **fixed-adapter-new-field** keywords added in JUNOS Release 10.0.0.

Description Configures the format used by the E Series L2TP access concentrator (LAC) to generate the L2TP Calling Number attribute value pair (AVP) 22 that it passes to the L2TP network server (LNS). Available formats include different fixed formats and several formats that include either or both of the agent-circuit-id (suboption 1) and agent-remote-id (suboption 2) suboptions of the PPPoE intermediate agent tags. The **no** version restores the default calling number format, descriptive.

- Options**
- descriptive—Formats calling number AVP in descriptive format that includes only interface information
 - descriptive include-agent-circuit-id—Formats calling number AVP in descriptive format to include interface information and the agent-circuit-id suboption
 - descriptive include-agent-circuit-id include-agent-remote-id—Formats calling number AVP in descriptive format to include interface information and both the agent-circuit-id and agent-remote-id suboptions
 - descriptive include-agent-remote-id—Formats calling number AVP in descriptive format to include interface information and the agent-remote-id
 - fixed—Formats calling number AVP to use a fixed format of up to 15 characters consisting of all ASCII fields, similar to the fixed format of RADIUS attribute 31 (Calling-Station-Id):
 - Format for ATM interfaces:
 systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) *VPI* (3 bytes) *VCI* (5 bytes)
 - Format for Ethernet interfaces:
 systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) *VLAN* (8 bytes)
 - Format for serial interfaces:

systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) 0 (8 bytes)

- In the case of PPP terminated from LNS, the Calling-Station-Id attribute is the value passed as the calling-station AVP.
- fixed-adapter-embedded—Formats calling number AVP to use a fixed format of up to 15 characters consisting of all ASCII fields with a 1-byte *slot* field, 1-byte *adapter* field, and 1-byte *port* field:
 - Format for ATM interfaces:
systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte)
VPI (3 bytes) *VCI* (5 bytes)
 - Format for Ethernet interfaces:
systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte)
VLAN (8 bytes)
 - Format for serial interfaces:
systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte)
0 (8 bytes)
 - For E120 and E320 routers, *adapter* is the number of the bay in which the I/O adapter (IOA) resides, either 0 (representing the right IOA bay on the E120 router and the upper IOA bay on the E320 router) or 1 (representing the left IOA bay on the E120 router or the lower IOA bay on the E320 router). For ERX7xx models, ERX14xx models, and ERX310 routers, which do not use IOAs, *adapter* is always shown as 0.
 - Slot numbers 0 through 16 are shown as ASCII characters in the 1-byte *slot* field.
- fixed-adapter-new-field—Formats calling number AVP to use a fixed format of up to 17 characters consisting of all ASCII fields with a 2-byte *slot* field, 1-byte *adapter* field, and 2-byte *port* field:
 - Format for ATM interfaces:
systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes)
VPI (3 bytes) *VCI* (5 bytes)
 - Format for Ethernet interfaces:
systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes) *VLAN*
(8 bytes)
 - Format for serial interfaces:
systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes)
0 (8 bytes)
 - For E120 routers and E320 routers, *adapter* is the number of the bay in which the IOA resides, either 0 or 1. For ERX7xx models, ERX14xx models, and ERX310 routers, which do not use IOAs, *adapter* is always shown as 0.
 - Slot numbers 0 through 16 are shown as integers in the 2-byte *slot* field.
- include-agent-circuit-id—Formats calling number AVP to include only the agent-circuit-id suboption
- include-agent-circuit-id include-agent-remote-id—Formats calling number AVP to include both the agent-circuit-id and agent-remote-id suboptions

- **include-agent-remote-id**—Formats calling number AVP to include only the agent-remote-id suboption
- **stacked**—Includes a 4-byte stacked VLAN (S-VLAN) ID in the fixed, fixed-adapter-embedded, and fixed-adapter-new-field calling number AVP formats for Ethernet interfaces; by default, these formats do not include the S-VLAN ID unless you specify the optional **stacked** keyword:
 - Format for Ethernet interfaces that use **fixed**:
systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) *S-VLAN* (4 bytes) *VLAN* (4 bytes)
 - Format for Ethernet interfaces that use **fixed-adapter-embedded**:
systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte) *S-VLAN* (4 bytes) *VLAN* (4 bytes)
 - Format for Ethernet interfaces that use **fixed-adapter-new-field**:
systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes) *S-VLAN* (4 bytes) *VLAN* (4 bytes)

Mode Global Configuration

aaa tunnel calling-number-format-fallback

Syntax aaa tunnel calling-number-format-fallback
 { descriptive |
 fixed [stacked] |
 fixed-adapter-embedded [stacked] |
 fixed-adapter-new-field [stacked] }

 no aaa tunnel calling-number-format-fallback

Release Information Command introduced in JUNOS Release 8.1.0.
fixed-adapter-embedded, **fixed-adapter-new-field**, and **stacked** keywords added in JUNOS Release 10.0.0.

Description Configures the fallback format for the tunnel calling number to be passed by the E Series L2TP access concentrator (LAC) to the L2TP network server (LNS) in the L2TP Calling Number attribute value pair (AVP) 22 when the PPPoE agent circuit ID is null or unavailable. The fallback format is used only when the configured calling number format includes either or both of the agent-circuit-id and agent-remote-id suboptions. The **no** version restores the default fallback format, descriptive.

- Options**
- **descriptive**—Configures the fallback format in descriptive format that includes only interface information
 - **fixed**—Configures the fallback format in a fixed format of up to 15 characters consisting of all ASCII fields, similar to the fixed format of RADIUS attribute 31 (Calling-Station-Id):
 - Fallback format for ATM interfaces:
 systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) *VPI* (3 bytes) *VCI* (5 bytes)
 - Fallback format for Ethernet interfaces:
 systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) *VLAN* (8 bytes)
 - Fallback format for serial interfaces:
 systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) 0 (8 bytes)
 - In the case of PPP terminated from LNS, the Calling-Station-Id attribute is the value passed as the calling-station AVP.
 - **fixed-adapter-embedded**—Configures the fallback format in a fixed format of up to 15 characters consisting of all ASCII fields with a 1-byte *slot* field, 1-byte *adapter* field, and 1-byte *port* field:
 - Fallback format for ATM interfaces:
 systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte) *VPI* (3 bytes) *VCI* (5 bytes)
 - Fallback format for Ethernet interfaces:
 systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte) *VLAN* (8 bytes)

- Fallback format for serial interfaces:
systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte)
0 (8 bytes)
- For E120 routers and E320 routers, *adapter* is the number of the bay in which the I/O adapter (IOA) resides, either 0 (representing the right IOA bay on the E120 router and the upper IOA bay on the E320 router) or 1 (representing the left IOA bay on the E120 router or the lower IOA bay on the E320 router). For ERX7xx models, ERX14xx models, and ERX310 routers, which do not use IOAs, *adapter* is always shown as 0.
- Slot numbers 0 through 16 are shown as ASCII characters in the 1-byte slot field.
- **fixed-adapter-new-field**—Configures the fallback format in a fixed format of up to 17 characters consisting of all ASCII fields with a 2-byte *slot* field, 1-byte *adapter* field, and 2-byte *port* field:
 - Fallback format for ATM interfaces:
systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes)
VPI (3 bytes) *VCI* (5 bytes)
 - Fallback format for Ethernet interfaces:
systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes) *VLAN*
(8 bytes)
 - Fallback format for serial interfaces:
systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes)
0 (8 bytes)
 - For E120 routers and E320 routers, *adapter* is the number of the bay in which the IOA resides, either 0 or 1. For ERX7xx models, ERX14xx models, and ERX310 routers, which do not use IOAs, *adapter* is always shown as 0.
 - Slot numbers 0 through 16 are shown as integers in the 2-byte *slot* field.
- **stacked**—Includes a 4-byte stacked VLAN (S-VLAN) ID in the fixed, fixed-adapter-embedded, and fixed-adapter-new-field fallback formats for Ethernet interfaces; by default, these formats do not include the S-VLAN ID unless you specify the optional **stacked** keyword:
 - Fallback format for Ethernet interfaces that use **fixed**:
systemName (up to 4 bytes) *slot* (2 bytes) *port* (1 byte) *S-VLAN* (4 bytes) *VLAN*
(4 bytes)
 - Fallback format for Ethernet interfaces that use **fixed-adapter-embedded**:
systemName (up to 4 bytes) *slot* (1 byte) *adapter* (1 byte) *port* (1 byte) *S-VLAN*
(4 bytes) *VLAN* (4 bytes)
 - Fallback format for Ethernet interfaces that use **fixed-adapter-new-field**:
systemName (up to 4 bytes) *slot* (2 bytes) *adapter* (1 byte) *port* (2 bytes)
S-VLAN (4 bytes) *VLAN* (4 bytes)

Mode Global Configuration

aaa tunnel client-name

Syntax aaa tunnel client-name *name*
 no aaa tunnel client-name

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the default tunnel client name. If the tunnel client name is not included in the tunnel attributes that are returned from the domain map or authentication server, the router uses the default name. The **no** version deletes the client name.

Options ■ *name*—Default tunnel client name; a string of up to 32 characters

Mode Global Configuration

aaa tunnel-group

Syntax [no] aaa tunnel-group *groupName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies an AAA tunnel group and changes the mode to Tunnel Group Configuration mode. In Tunnel Group Configuration mode, you can add up to 31 tunnel definitions. The **no** version deletes the AAA group tunnel configuration from the router.

Options ■ *groupName*—String of up to 64 characters (no spaces)

Mode Global Configuration

aaa tunnel ignore

Syntax aaa tunnel ignore { nas-port | nas-port-type } { enable | disable }
no aaa tunnel ignore { nas-port | nas-port-type }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies whether to use the tunnel peer's NAS-Port [5] and NAS-Port-Type [61] attributes. The **no** version negates the command or restores the default of enable.

- Options**
- nas-port—Configures the tunnel peer's supplied nas-port value
 - nas-port-type—Configures the tunnel peer's supplied nas-port-type value
 - enable—Implements the feature; this is the default setting
 - disable—Disables the feature

Mode Global Configuration

aaa tunnel nas-port-method

Syntax aaa tunnel nas-port-method cisco-avp
 no aaa tunnel nas-port-method

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the tunnel's default NAS port type to provide limited support for a Cisco proprietary vendor-specific method when configuring the LAC to LNS NAS port identification transfer mechanism. The **no** version disables the command.



NOTE: Use of this feature is not recommended and continued compatibility cannot be guaranteed.

Mode Global Configuration

aaa tunnel password

Syntax aaa tunnel password *name*
 no aaa tunnel password

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the default tunnel password. If the tunnel password is not included in the tunnel attributes that are returned from the domain map or authentication server, the router uses the default password. The **no** version deletes the password.

Options ■ *name*—Default tunnel password; a string of up to 32 characters

Mode Global Configuration

aaa tunnel switch-profile

Syntax `aaa tunnel switch-profile profileName`
`no aaa tunnel switch-profile`

Release Information Command introduced in JUNOS Release 7.2.0.

Description Applies a default L2TP tunnel switch profile to a virtual router. The default tunnel switch profile defines the L2TP tunnel switching behavior for the interfaces to which this profile is assigned. The router uses the default tunnel switch profile if the tunnel attributes returned from an AAA domain map or tunnel group or from a RADIUS authentication server do not include a named tunnel switch profile. The **no** version removes the default tunnel switch profile assignment from the virtual router.

Options ■ *profileName*—Name of the default tunnel switch profile; a string of up to 64 alphanumeric characters

Mode Global Configuration

aaa tunnel tx-connect-speed-method

Syntax aaa tunnel tx-connect-speed-method { static-layer2 | dynamic-layer2 | qos | actual }

```
no aaa tunnel tx-connect-speed-method
```

Release Information Command introduced in JUNOS Release 8.0.0.

Description	Configures the method used to calculate the transmit connect speed of the subscriber's access interface for establishing a tunneled L2TP session associated with a virtual router. This speed is reported in L2TP Transmit (TX) Speed AVP 24. The router uses the calculation method specified with the aaa tunnel tx-connect-speed-method command if the tunnel attributes returned from an AAA domain map, an AAA tunnel group, or a RADIUS authentication server do not include the transmit connect speed calculation method. The no version removes configuration of the transmit connect speed calculation method from the tunneled L2TP sessions associated with the virtual router.
--------------------	---

- Options**
- **static-layer2**—Calculates the transmit connect speed of the subscriber's access interface based on statically configured settings for the underlying layer 2 interface
 - **dynamic-layer2**—Calculates the transmit connect speed of the subscriber's access interface based on dynamically configured settings for the underlying layer 2 interface
 - **qos**—Calculates the transmit connect speed of the subscriber's access interface based on settings determined by QoS
 - **actual**—Calculates the transmit connect speed of the subscriber's access interface as the lesser of the **dynamic-layer2** value or the **qos** value

Mode Global Configuration

aaa user accounting interval

Syntax `aaa user accounting interval period`
 `no aaa user accounting interval`

Release Information Command introduced in JUNOS Release 9.0.0.

Description Specifies the default user accounting interval used on the virtual router. This router uses this value for users when no value is specified in the RADIUS Acct-Interim-Interval attribute (RADIUS attribute 85). The **no** version restores the default setting of 0, which turns off interim accounting for users attached to this virtual router.



NOTE: This command and the **aaa service accounting interval** command replace the deprecated **aaa accounting interval** command, which may be removed completely in a future release.

Options ■ *period*—Accounting interval in minutes in the range 10–1440, which sets the time period between accounting updates for users on this virtual router; 0 is the default

Mode Global Configuration

aaa virtual-router

Syntax `aaa virtual-router indexInteger vrName`
`no aaa virtual-router indexInteger`

Release Information Command introduced before JUNOS Release 7.1.0.

Description For AAA broadcast accounting, adds a virtual router to a virtual router group. The **no** version with the *indexInteger* parameter removes a specific virtual router from the virtual router group.

- Options**
- *indexInteger*—Number in the range 1–4 that indicates the virtual router's listing in the virtual router group; the *indexInteger* is used in the **no** version of the command to delete a particular virtual router from the group
 - *vrName*—Name of virtual router that can receive AAA broadcast accounting packets.

Mode VR Group Configuration

aaa wins

Syntax `aaa wins { primary | secondary } ipAddress`
`no aaa wins { primary | secondary }`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the IP address of the WINS name server. The **no** version sets the corresponding address to 0.

- Options**
- `primary`—Specifies the primary WINS name server
 - `secondary`—Specifies the secondary WINS name server
 - `ipAddress`—IP address of the name server

Mode Global Configuration

access-class in

Syntax access-class *listName* in
 no access-class [*listName*] in

Release Information Command introduced before JUNOS Release 7.1.0.

Description Restricts incoming connections between a particular virtual terminal line and the addresses in an access list. The no version removes access restrictions.

Options ■ *listName*—Name of the access list

Mode Line Configuration

access-list

Syntax Standard IP access list:

```
access-list accessListName { permit | deny }
{ srcIP srcWildcard | [ host ] srcIPHost | any } [ log ]
```

```
no access-list accessListName [ { permit | deny }
{ srcIP srcWildcard | [ host ] srcIPHost | any } [ log ] ]
```

Extended IP access list:

```
access-list accessListName { permit | deny } ip { srcIP srcWildcard |
host srcIPHost | any } { dstIP dstWildcard | host dstIPHost | any } [ log ]
```

```
no access-list accessListName [ { permit | deny } ip { srcIP srcWildcard |
host srcIPHost | any } { dstIP dstWildcard | host dstIPHost | any } [ log ] ]
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a standard or extended IP access list. The extended access list enables you to specify a destination address or host, precedence, and type of service. This command imposes an implicit last rule of “deny ip any any” to deny all routes that do not match previous rules in the access list. The **no** version removes the IP access list, the specified entry in an access list, or the log for a specified entry.

- Options**
- *accessListName*—String of up to 32 alphanumeric characters
 - permit—Permits access if the conditions are matched
 - deny—Denies access if the conditions are matched
 - *srcIP*—Source IP address from which the packet is being sent
 - *srcWildcard*—Wildcard mask IP address
 - host—Identifies the address as a host
 - *srcIPHost*—Source host IP address; assumes a wildcard mask of 0
 - any—Creates an address of 0.0.0.0 with a wildcard mask of 255.255.255.255
 - *dstIP*—Destination IP address
 - *dstWildcard*—Wildcard mask IP address for destination
 - *dstIPHost*—Destination host IP address to which the packet is being sent
 - log—Logs an Info event into the ipAccessList log whenever the access-list rule is matched

Mode Global Configuration

accounting

Syntax accounting { exec | commands *level* } *listName*
 no accounting { exec | commands *level* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables AAA accounting services on a console line, a virtual terminal line, or a group of lines and applies the specified accounting method list. The **no** version restores the default method list.



NOTE: To disable accounting for a console line or virtual terminal line, specify a nonexistent accounting method list name (for example, noAccounting).

- Options**
- *exec*—Specifies that accounting information is captured for User Exec terminal sessions on the line
 - *level*—Privilege level of User Exec mode commands for which accounting information is captured; in the range 0–15
 - *listName*—Named method list used to specify how accounting is performed

Mode Line Configuration

adapter accept

Syntax adapter accept *adapterSpecifier*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Erases from NVS the type and configuration of the previous I/O adapter (IOA) in the specified IOA bay, and allows you to configure a new IOA. Issue this command after you have installed a different type of IOA in an IOA bay. You can use this command only when the state of the IOA is not present or disabled (mismatch). There is no **no** version.



NOTE: Issuing this command reboots the line module associated with the IOA, but it does not accept its configuration.

To accept the configuration of the line module and its associated IOAs, issue the slot accept command.

- Options**
- *adapterSpecifier*—Particular IOA in the format *slot/adapter*:
 - *slot*—Number of the chassis slot; for E120 routers, in the range 0–5; for E320 routers, in the range 0–5 or 11–16
 - *adapter*—Identifier for the IOA within the chassis slot, either 0 or 1, where:
 - 0 indicates that the IOA is installed in the right IOA bay (E120 router) or the upper IOA bay (E320 router).
 - 1 indicates that the IOA is installed in the left IOA bay (E120 router) or the lower IOA bay (E320 router).

Mode Global Configuration

adapter disable

Syntax adapter disable *adapterSpecifier*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Disables the IOA installed in the specified IOA bay. There is no **no** version.



NOTE: For IOAs that support hot-swapping, issuing this command does not reboot the line module. For IOAs that do not support hot-swapping, issuing this command reboots the line module associated with the IOA, but it does not disable it.

To disable the line module and its associated IOAs, issue the slot disable command.

- Options** ■ *adapterSpecifier*—Particular IOA in the format *slot/adapter*:
- *slot*—Number of the chassis slot; for E120 routers, in the range 0–5; for E320 routers, in the range 0–5 or 11–16
 - *adapter*—Identifier for the IOA within the chassis slot, either 0 or 1, where:
 - 0 indicates that the IOA is installed in the right IOA bay (E120 router) or the upper IOA bay (E320 router).
 - 1 indicates that the IOA is installed in the left IOA bay (E120 router) or the lower IOA bay (E320 router).

Mode Global Configuration

adapter enable

Syntax adapter enable *adapterSpecifier*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Enables the IOA installed in the specified IOA bay. There is no **no** version.



NOTE: For IOAs that support hot-swapping, issuing this command does not reboot the line module. For IOAs that do not support hot-swapping, issuing this command reboots the line module associated with the IOA, but it does not enable it.

To enable the line module and its associated IOAs, issue the slot enable command.

- Options**
- *adapterSpecifier*—Particular IOA in the format *slot/adapter*:
 - *slot*—Number of the chassis slot; for E120 routers, in the range 0–5; for E320 routers, in the range 0–5 or 11–16
 - *adapter*—Identifier for the IOA within the chassis slot, either 0 or 1, where:
 - 0 indicates that the IOA is installed in the right IOA bay (E120 router) or the upper IOA bay (E320 router).
 - 1 indicates that the IOA is installed in the left IOA bay (E120 router) or the lower IOA bay (E320 router).

Mode Global Configuration

adapter erase

Syntax adapter erase *adapterSpecifier*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Erases from NVS the type and configuration of the previous IOA in the specified IOA bay, and allows you to configure a new IOA. Issue this command before you install a different type of IOA in an IOA bay. There is no **no** version.



NOTE: Issuing this command reboots the line module associated with the IOA, but it does not erase its configuration.

To erase the configuration of the line module and its associated IOAs, issue the slot erase command.

- Options**
- *adapterSpecifier*—Particular IOA in the format *slot/adapter*:
 - *slot*—Number of the chassis slot; for E120 routers, in the range 0–5; for E320 routers, in the range 0–5 or 11–16
 - *adapter*—Identifier for the IOA within the chassis slot, either 0 or 1, where:
 - 0 indicates that the IOA is installed in the right IOA bay (E120 router) or the upper IOA bay (E320 router).
 - 1 indicates that the IOA is installed in the left IOA bay (E120 router) or the lower IOA bay (E320 router).

Mode Global Configuration

address

Syntax To set the tunnel endpoint address:

`address serverAddress`

`no address`

To configure RIP:

`[no] address { ipAddress | unnumbered interfaceType interfaceSpecifier }`

To configure NAT address pool ranges:

`[no] address startIpAddress endIpAddress`

Release Information Command introduced before JUNOS Release 7.1.0.

Description From Domain Map Tunnel Configuration mode, sets the tunnel endpoint address of an L2TP tunnel. The **no** version removes the address of the tunnel.

From Tunnel Group Tunnel Configuration mode, sets the tunnel endpoint address of an L2TP tunnel. The **no** version removes the address of the tunnel.

From Interface Configuration or Subinterface Configuration mode, configures RIP to run on the interface specified by the IP address or on an unnumbered interface. Uses the default values: send version is RIP version 1, receive version is RIP version 1 and version 2, authentication is not enabled. The **no** version deletes the RIP interface. Use the **address** commands to configure RIP attributes on the network.

From IP NAT Pool Configuration mode, configures NAT IP address pool ranges. The **no** version removes the range from the current NAT address pool.

- Options**
- *serverAddress*—IP address of the LNS endpoint
 - *ipAddress*—Address of IP interface where RIP will be run
 - *unnumbered*—Specifies that RIP will be run on an unnumbered interface
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *startIpAddress*—Starting IP address (inclusive) of the NAT pool range you are creating
 - *endIpAddress*—Ending IP address (inclusive) of the NAT pool range you are creating

Mode Address Family Configuration (RIP), Domain Map Tunnel Configuration, IP NAT Pool Configuration, Router Configuration (RIP), Tunnel Group Tunnel Configuration

address area

Syntax [no] address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
 area { *areaId* | *areaIdInt* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates an interface on which OSPF runs in the specified area, on top of the IP interface at the specified IP address. Uses the default values. The **no** version deletes OSPF interfaces. If the OSPF network was previously specified with the **network area** command, the OSPF interface already exists, and you do not need to use this command, unless you want to change the area of the OSPF interface to an area different from the one specified by the **network area** command.



NOTE: Before you issue this command, you must first configure an interface with the IP address specified by *ipAddress* or an interface configured as unnumbered.

You must issue this command before issuing any other OSPF **address** command.

- Options**
- *ipAddress*—IP address of the interface on which OSPF will be run
 - unnumbered—Configures OSPF on an unnumbered interface
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *areaId*—OSPF area ID in IP address format
 - *areaIdInt*—OSPF area ID as a decimal value in the range 1–4294967295

Mode Router Configuration

address authentication key

Syntax address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
 authentication key [0 | 8] *authkey*

no address [*ipAddress* | unnumbered *interfaceType* *interfaceSpecifier*]
 authentication key

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the password for text authentication and the key for MD5 authentication. The **no** version clears the key for the interface. Supported only in RIP version 2. Authentication is disabled by default.

- Options**
- *ipAddress*—Address of IP interface where RIP will be run
 - unnumbered—Specifies that RIP will be run on an unnumbered interface
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - 0—Indicates the *authKey* is entered in unencrypted form (plaintext); this is the default option
 - 8—Indicates the *authKey* is entered in encrypted form (ciphertext)
 - *authkey*—Password sent with RIP messages or the key used to encrypt/decrypt RIP messages, depending on the authentication mode set for this interface

Mode Address Family Configuration, Router Configuration

address authentication-key

Syntax [no] address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
authentication-key [0 | 8] *authKey*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns a password used by neighboring routers that are using OSPF simple password authentication. The no version deletes the password.



NOTE: You must issue the **address area** command before issuing this command.

- Options**
- *ipAddress*—OSPF interface address previously specified with the **address** command
 - unnumbered—Indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - 0—Indicates the *authKey* is entered in unencrypted form (plaintext); this is the default option
 - 8—Indicates the *authKey* is entered in encrypted form (ciphertext)
 - *authKey*—Password, string of up to 8 characters

Mode Router Configuration

address authentication message-digest

Syntax [no] address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
authentication message-digest

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that MD5 authentication is used for the OSPF interface. The **no** version sets authentication for the interface to none, but leaves any configured MD5 key intact.



NOTE: You must issue the **address area** command before issuing this command.

- Options**
- *ipAddress*—OSPF interface address previously specified with the **address** command
 - unnumbered—Indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Router Configuration

address authentication mode

Syntax address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
 authentication mode { text | md5 *keyID* }

no address [*ipAddress* | unnumbered *interfaceType* *interfaceSpecifier*]
 authentication mode

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the type of authentication used on this interface. The **no** version removes authentication from the interface. Supported only in RIP version 2. Authentication is disabled by default.

- Options**
- *ipAddress*—Address of IP interface where RIP will be run
 - unnumbered—Specifies RIP will be run on an unnumbered interface
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - text—Simple text password is sent with each RIP message. If the password is not possessed by neighbors, the message is rejected.
 - md5—MD5 message-digest algorithms are used to encrypt and compress the RIP message.
 - *keyID*—Number identifying the MD5 key. Neighbors must share the MD5 key to decrypt the message and encrypt the response.

Mode Address Family Configuration, Router Configuration

address authentication-none

Syntax [no] address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
authentication-none

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that no authentication is to be used for the OSPF interface. The **no** version has no effect.



NOTE: You must issue the **address area** command before issuing this command.

- Options**
- *ipAddress*—OSPF interface address previously specified with the **address** command
 - unnumbered—Indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Router Configuration

address bfd-liveness-detection

Syntax address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
 bfd-liveness-detection [minimum-interval *minInterval* |
 [minimum-receive-interval *minRecInterval*]
 [minimum-transmit-interval *minTransInterval*]] [multiplier *multValue*]

no address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
 bfd-liveness-detection

Release Information Command introduced in JUNOS Release 8.0.0.

Description Enables BFD (bidirectional forwarding detection) on an interface running RIP and defines BFD values to be negotiated between peers for detection of IP data path failures. The **no** version disables BFD on the RIP interface.

- Options**
- *ipAddress*—Address of IP interface where RIP will be run
 - unnumbered—Specifies that RIP will be run on an unnumbered interface
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *minInterval* —Minimum proposed transmit interval and required receive interval for BFD control packets; has the same effect as configuring the minimum receive interval and the minimum transmit interval to the same value; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *minRecInterval*—Minimum interval at which the local peer must receive BFD control packets sent by the remote peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *minTransInterval*—Minimum proposed interval between BFD control packets sent by the local peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *multValue*—Detection multiplier value that the remote peer router multiplies by the local peer's negotiated transmit interval to determine the remote peer's BFD liveness detection interval; equal to the number of BFD packets that can be missed before the BFD session is declared down; number in the range 1–255; default value is 3

Mode Address Family Configuration, Router Configuration

address cost

Syntax [no] address { *ipAddress* | unnumbered *interfaceType interfaceSpecifier* } cost *intfCost*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a cost metric for an OSPF interface. Used in the calculation of the SPF routing table. The **no** version resets the path cost to the default.



NOTE: You must issue the **address area** command before issuing this command.

- Options**
- *ipAddress*—OSPF interface address previously specified with the **address** command
 - unnumbered—Indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *intfCost*—Link-state metric cost; a number in the range 0–65535; default value is 10

Mode Router Configuration

address dead-interval

Syntax [no] address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
dead-interval *deadInterval*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the time period that the router's neighbors should wait without seeing hello packets from the router before they declare the router to be down. The **no** version resets the dead interval to its default.



NOTE: You must issue the **address area** command before issuing this command.

- Options**
- *ipAddress*—OSPF interface address previously specified with the **address** command
 - unnumbered—Indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *deadInterval*—Number in the range 0–2147483647 seconds; default value is 40 seconds

Mode Router Configuration

address-family

Syntax For BGP:

```
[ no ] address-family { { ipv4 | ipv6 } [ unicast | multicast
| [ unicast ] vrf vrfName ] |
{ vpnv4 | vpnv6 } [ unicast ] | l2vpn [ signaling ] | route-target [ signaling ] |
vpls vplsName | vpws vpwsName }
```

For IS-IS:

```
[ no ] address-family ipv6 [ unicast | multicast | unicast multicast ]
```

For RIP:

```
[ no ] address-family ipv4 [ unicast ] vrf vrfName
```

Release Information Command introduced before JUNOS Release 7.1.0.
l2vpn and **signaling** keywords added in JUNOS Release 7.1.0.
vpls keyword and *vplsName* variable added in JUNOS Release 7.1.0.
vpws keyword and *vpwsName* variable added in JUNOS Release 8.1.0.
route-target signaling keywords and IS-IS IPv6 version added in JUNOS Release 8.2.0.

Description For BGP, configures the router to exchange addresses for the specified address family. This command takes effect immediately.

- For the IPv4 address family, configures the router or a specific VRF to exchange IPv4 addresses in unicast, multicast, or VPN mode.
- For the IPv6 address family, configures the router or a specific VRF to exchange IPv6 addresses in unicast, multicast, or VPN mode.
- For the L2VPN address family, configures a router to exchange layer 2 NLRI for all VPLS instances and all L2VPN (VPWS) instances.
- For the VPLS address family, configures the router to exchange layer 2 NLRI for the VPLS address family for a specified VPLS instance.
- For the VPWS address family, configures the router to exchange layer 2 NLRI for the VPWS address family for a specified L2VPN (VPWS) instance.
- For the route-target address family, configures the router to exchange route-target membership NLRI (RT-MEM-NLRI) that includes information about membership in VPN route-target extended communities.

For IS-IS, configures IS-IS to exchange IPv6 addresses.

For RIP, configures RIP in a specific VRF to exchange IPv4 addresses.

For all routing protocols, the **no** version removes the address family.

- Options**
- **ipv4**—Specifies sessions that carry standard IPv4 address prefixes (default)
 - **ipv6**—Specifies sessions that carry IPv6 address prefixes
 - **multicast**—Specifies multicast prefixes
 - **unicast**—Specifies unicast prefixes (default)
 - **vrfName**—Name of the VRF; string of 1–32 alphanumeric characters
 - **vpnv4**—Specifies sessions that carry customer VPN-IPv4 prefixes, each of which has been made globally unique by adding an 8-byte route distinguisher
 - **vpnv6**—Specifies sessions that carry customer VPN-IPv6 prefixes, each of which has been made globally unique by adding an 8-byte route distinguisher
 - **l2vpn**—Specifies sessions that carry L2VPN reachability information
 - **l2vpn signaling**—Specifies BGP signaling of L2VPN reachability information; currently, you can omit the **signaling** keyword with no adverse effects
 - **route-target**—Specifies sessions that carry route-target membership information
 - **route-target signaling**—Specifies BGP signaling of route-target membership information; currently, this can be omitted with no adverse effects
 - **vplsName**—Name of a VPLS instance for which you are specifying the L2VPN address family; must be issued for each separate VPLS instance
 - **vpwsName**—Name of a layer 2 VPN (VPWS) instance for which you are specifying the L2VPN address family; must be issued for each separate L2VPN instance

Mode Router Configuration

- Related Topics**
- *Configuring BGP Signaling for L2VPNS and Configuring BGP Signaling for VPLS in the JUNOS BGP and MPLS Configuration Guide*

address hello-interval

Syntax [no] address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
hello-interval *helloInterval*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the interval between hello packets that the router sends on the interface. The **no** version resets the hello interval to its default.



NOTE: You must issue the **address area** command before issuing this command.

- Options**
- *ipAddress*—OSPF interface address previously specified with the **address** command
 - unnumbered—Indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *helloInterval*—Number in the range 1–65535 seconds; default value is 10 seconds

Mode Router Configuration

address message-digest-key md5

Syntax address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
 message-digest-key *keyID* md5 [0 | 8] *msgDigestKey*

no address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
 message-digest-key *keyID*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables OSPF MD5 authentication and configures the MD5 key. The **no** version deletes an MD5 key.



NOTE: If all the MD5 keys have been deleted, the authentication type is still MD5, but you need to configure MD5 keys.

To disable MD5 authentication for the interface, use the **address authentication-none** command.

You must issue the **address area** command before issuing this command.

- Options**
- *ipAddress*—OSPF interface address previously specified with the **address** command
 - unnumbered—Indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *keyID*—Key identifier in the range 1–255
 - md5—Specifies use of the MD5 algorithm
 - 0—Indicates the *msgDigestKey* is entered in unencrypted form (plaintext); this is the default option
 - 8—Indicates the *msgDigestKey* is entered in encrypted form (ciphertext)
 - *msgDigestKey*—OSPF password; string of up to 16 alphanumeric characters

Mode Router Configuration

address network

Syntax address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
 network { broadcast | non-broadcast | point-to-point }
 no address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* } network

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the OSPF network type for the specified interface to something other than the default for the network medium. The **no** version restores the default value for the medium.



NOTE: You must issue the **address area** command before issuing this command.

- Options**
- *ipAddress*—OSPF interface address previously specified with the **address** command
 - unnumbered—Indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - broadcast—Sets network type to broadcast
 - non-broadcast—Sets network type to NBMA
 - point-to-point—Sets network type to point-to-point

Mode Router Configuration

address passive-interface

Syntax [no] address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
passive-interface

Release Information Command introduced before JUNOS Release 7.1.0.

Description Disables the transmission of routing updates on an interface. OSPF routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF domain. The **no** version reenables the transmission of routing updates.



NOTE: You must issue the **address area** command before issuing this command.

- Options**
- *ipAddress*—OSPF interface address previously specified with the **address** command
 - unnumbered—Indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Router Configuration

address-pool-name

Syntax address-pool-name *poolName*
no address-pool-name

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies an address pool name to associate with the domain name being configured. The **no** version removes the pool name.

Options ■ *poolName*—Name of the pool to associate with the domain name

Mode Domain Map Configuration

address priority

Syntax [no] address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
priority *intfPriority*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the router priority. Used in determining the designated router for the particular network. This designation only applies to multi-access networks. Every broadcast and nonbroadcast multiaccess network has a designated router. The **no** version restores the default value.



NOTE: You must issue the **address area** command before issuing this command.

- Options**
- *ipAddress*—OSPF interface address previously specified with the **address** command
 - unnumbered—Indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *intfPriority*—Priority value, an 8-bit number in the range 1–255; default value is 1

Mode Router Configuration

address receive version

Syntax address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
 receive version { 1 | 2 | 1 2 | 2 1 | off }
 no address [*ipAddress* | unnumbered *interfaceType* *interfaceSpecifier*] receive version

Release Information Command introduced before JUNOS Release 7.1.0.

Description Restricts the RIP version that the router can receive on an interface. The **no** version sets the interface back to the default value, receiving both RIP version 1 and version 2.

- Options**
- *ipAddress*—Address of IP interface where RIP will be run
 - unnumbered—Specifies that RIP will be run on an unnumbered interface
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - 1—Specifies RIP version 1 only
 - 2—Specifies RIP version 2 only
 - 1 2—Specifies RIP version 1 and version 2; the default value
 - 2 1—Specifies RIP version 2 and version 1
 - off—Turns reception off

Mode Address Family Configuration, Router Configuration

address retransmit-interval

Syntax [no] address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
 retransmit-interval *retransInterval*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the time between LSA retransmissions for the interface when an acknowledgment for the LSA is not received. The **no** version restores the default value.



NOTE: You must issue the **address area** command before issuing this command.

- Options**
- *ipAddress*—OSPF interface address previously specified with the **address** command
 - unnumbered—Indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *retransInterval*—Number in the range 0–3600 seconds; default value is 5 seconds

Mode Router Configuration

address send version

Syntax address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
 send version { 1 | 2 | 1 2 | 2 1 | off }
 no address [*ipAddress* | unnumbered *interfaceType* *interfaceSpecifier*] send version

Release Information Command introduced before JUNOS Release 7.1.0.

Description Restricts the RIP version that the router can send on an interface. The **no** version sets the interface back to the default value, sending only RIP version 1.

- Options**
- *ipAddress*—Address of IP interface where RIP will be run
 - unnumbered—Specifies that RIP will be run on an unnumbered interface
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - 1—Specifies RIP version 1 only
 - 2—Specifies RIP version 2 only
 - 1 2—Specifies RIP version 1 and version 2
 - 2 1—Specifies RIP version 2 and version 1
 - off—Turns reception off

Mode Address Family Configuration, Router Configuration

address transmit-delay

Syntax [no] address { *ipAddress* | unnumbered *interfaceType* *interfaceSpecifier* }
transmit-delay *transmDelay*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the estimated time it takes to transmit a link-state update packet on the interface. The **no** version restores the default value.



NOTE: You must issue the **address area** command before issuing this command.

- Options**
- *ipAddress*—OSPF interface address previously specified with the **address** command
 - unnumbered—Indicates that OSPF is running on an unnumbered interface previously specified with the **address** command
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *transmDelay*—Link-state transmit delay, a number in the range 0–3600 seconds; default value is 1 second

Mode Router Configuration

adjustment-factor

Syntax adjustment-factor *dslType value*
 no adjustment-factor *dslType*

Release Information Command introduced in JUNOS Release 9.1.0.

Description Configures an adjustment factor that is applied globally to the ANCP-reported downstream and upstream data rate for all subscribers of a particular DSL line type. The adjusted data rate results in an accurate QoS shaping rate. The **no** version restores the default, wherein the rate is not adjusted.

- Options**
- *dslType*—Type of DSL subscriber line for which the data rate is adjusted by the specified QoS adjustment factor: **adsl1**, **adsl2**, **adsl2 +**, **vdsl**, **vdsl2**, or **sds**
 - *value*—QoS adjustment factor applied to upstream or down stream data rates for the DSL type; a percentage in the range 1–100

Mode L2C Configuration

agent context-name

Syntax agent context-name *contextName* [wildcard] [limit *contextNameLimit*]
 no agent

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the virtual router SNMP agent on which you want to poll MIB objects. The **no** version returns the context name to the default context (virtual router).

Options ■ *contextName*—Context name of the agent



NOTE: The *contextName* value is the virtual router number in the order the virtual router was created (for example, router1, router2, and so on). Use the **show snmp agent** command to obtain the context name for the virtual router.

- wildcard—Specifies that the context name is a wildcard value
- *contextNameLimit*—Maximum number of agents to be polled

Mode SNMP Trigger Configuration

aggregate-address

Syntax [no] aggregate-address { *address mask* | *ipv6Prefix* }
 [as-set | summary-only | attribute-map *attributeMapTag* |
 advertise-map *advertiseMapTag* | suppress-map *suppressMapName*]*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates an aggregate entry in a BGP routing table. The **no** version removes the aggregate.

- Options**
- *address*—Aggregate IPv4 address
 - *mask*—Aggregate IPv4 mask
 - *ipv6Prefix*—Aggregate IPv6 prefix
 - **as-set**—If the **as-set** option is not specified, the path attributes of the aggregate route are set in the same way as locally originated routes, except that the **atomic_aggregate** and **agggregator** attributes are added. If the **as-set** option is used, the path attributes of the aggregate route are determined by combining the path attributes of the aggregated routes as described in *RFC 4271—A Border Gateway Protocol 4 (BGP-4)*. If the **as-set** option is used, the path attributes of the aggregate route may change whenever one of the aggregated routes changes, causing the aggregate route to be readvertised.
 - **summary-only**—Filters all more specific routes from updates. **summary-only** not only creates the aggregate route but also suppresses advertisements of more-specific routes to all neighbors. If you only want to suppress advertisements to certain neighbors, you may use the **neighbor distribute-list** command, with caution. If a more-specific route leaks out, all BGP speakers will prefer that route over the less-specific aggregate you are generating (using longest-match routing). Alternatively, you can use the **suppress-map** keyword to suppress specific routes.
 - *attributeMapTag*—String of up to 32 characters that identifies the route map used to set the attributes of the aggregate route
 - *advertiseMapTag*—String of up to 32 characters that identifies the route map used to set the routes to create AS-SET origin communities in the range
 - *suppressMapName*—String of up to 32 characters that identifies a route map that filters routes to be suppressed
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Address Family Configuration, Router Configuration

aggregation-node

Syntax aggregation-node { *nodeValue* | atm | atm-vc | atm-vp *vpValue* | ethernet | fr-vc | forwarding | ppp-interface | svlan *svlanValue* | vlan }

no aggregation-node

Release Information Command introduced in JUNOS Release 8.0.0.
ppp-interface keyword added in JUNOS Release 10.3.0.

Description Configures the aggregation node value. The **no** version restores the default value, where the forwarding interface becomes the aggregation node.

- Options**
- *nodeValue*— Aggregation node number in the range 1–65535
 - *vpValue*—ATM VPI number in the range 0–255
 - *svlanValue*—S-VLAN ID number in the range 0–4095

Mode Policy Parameter Configuration

Related Topics

- Creating a Classifier Group for a Policy List

aggressive-mode

Syntax aggressive-mode { accepted | requested | required }
no aggressive-mode

Release Information Command introduced before JUNOS Release 7.1.0.
accepted, **requested**, and **required** keywords added in JUNOS Release 7.3.0.

Description Enables aggressive mode negotiation for the tunnel. The **no** version restores the default, no aggressive mode.

- Options**
- accepted—Accepts aggressive mode when proposed by peers
 - requested—Requests aggressive mode when negotiating with peers
 - required—Only requests and accepts aggressive mode when negotiating with peers

Mode IKE Policy Configuration

allow

Syntax [no] allow *domainName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the domain names that are to be allowed access to AAA authentication. The **no** version negates the command.

Options ■ *domainName*—Name of the domain; maximum of 64 characters

Mode AAA Profile Configuration

append-after

Syntax append-after *indexNumber* next-address *ipAddress* [[mask] *ipMask*] [loose]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Adds a next hop after a particular index in the MPLS explicit path. The sequence numbers for existing hops after the index adjust automatically. There is no **no** version.

- Options**
- *indexNumber*—Number of a node in an ordered set of abstract nodes
 - *ipAddress*—Address of the next hop
 - *ipMask*—[not currently used] mask for the next adjacent address
 - loose—Indicates the node is not necessarily directly connected (adjacent) to the previous node in the path. If loose is not configured, the configuration defaults to strict. Strict indicates that the node is directly connected to the previous node.

Mode Explicit Path Configuration

application

Syntax application *applicationType1* [*applicationType2* [*applicationType3*]]
 no application

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the type of application that is secured by connections created with this IPSec transport profile. You can specify multiple application types. The **no** version restores the default application, L2TP.

- Options** ■ *applicationType*—One of the following application types:
- dvmrp—Secures DVMRP traffic.
 - gre—Secures GRE traffic.
 - l2tp—Secures L2TP traffic; this is the default application
 - l2tp-nat-passthrough—Secures L2TP traffic and also allows clients to connect from behind NAT devices that support IPSec passthrough

Mode IPSec Transport Profile Configuration

aps events

Syntax `aps events list [list]*`

`no aps events`

Release Information Command introduced in JUNOS Release 7.2.0.

Description Enables line modules to deliver APS events to the necessary SNMP traps. You can configure notification for specific events. The **no** version disables the delivery of APS events from line modules to SNMP traps.

- Options** ■ *list*—One of the following APS events:
- *all*—Configures notification of all APS events
 - *channel-mismatch*—Configures notification of APS channel mismatches
 - *feplf*—Configures notification of APS far-end protection line failures
 - *mode-mismatch*—Configures notification of APS mode mismatches
 - *psbf*—Configures notification of APS protection signal byte failures
 - *switchover*—Configures notification of APS switchovers
 - ***—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

aps force

Syntax `aps force channelNumber`
`no aps force`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Forces the specified interface to be replaced by the inactive interface in an APS/MSP group. The **no** version allows the specified interface to resume operation.

- Options** ■ *channelNumber*—One of the following channel numbers:
- 0—Switches from the protect interface back to the working interface
 - 1—Switches from the working interface to the protect interface

Mode Controller Configuration

aps group

Syntax `aps group groupName`

`no aps group`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns an interface to an APS/MSP group. The **no** version removes a group of APS/MSP interfaces.

Options ■ *groupName*—Name of the APS/MSP group to which the active and standby interfaces belong; string of up to 32 characters

Mode Controller Configuration

aps lockdown

Syntax aps lockdown [0]
 no aps lockdown

Release Information Command introduced before JUNOS Release 7.1.0.

Description Prevents the working interface from switching to the protect interface. The **no** version restores the default situation, in which the working interface can switch to the protect interface.

Options ■ 0—Specifies the channel number that identifies the protect interface; because the protect interface is always assigned channel number 0, this is the only valid option

Mode Controller Configuration

aps manual

Syntax `aps manual channelNumber`
`no aps manual`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Forces the working interface to switch to the protect interface, unless a request of equal or higher priority exists. The **no** version allows the specified working interface to resume the active role.

- Options** ■ *channelNumber*—One of the following channel numbers:
- 0—Switches from the protect interface back to the working interface
 - 1—Switches from the working interface to the protect interface

Mode Controller Configuration

aps protect

Syntax aps protect [0]
 no aps protect

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures an interface as a protect interface. The **no** version removes the relationship between the protect interface and the active interface.

Options ■ 0—Specifies the channel number that identifies the protect interface; because the protect interface is always assigned channel number 0, this is the only valid option

Mode Controller Configuration

aps revert

Syntax `aps revert minutes`
`no aps revert`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the APS/MSP group to operate in revertive mode. The **no** version restores the default setting, nonrevertive mode.

Options ■ *minutes*—Number of minutes in the range 5–12 at which the interface resumes the active role after that interface becomes available

Mode Controller Configuration

aps unidirectional

Syntax [no] aps unidirectional

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the APS/MSP group to operate in unidirectional mode, the default setting. The **no** version configures the APS/MSP group to operate in bidirectional mode.

Mode Controller Configuration

aps working

Syntax aps working [1]
 no aps working

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures an interface as a working interface. The **no** version removes the configuration.

Options ■ 1 —Channel number that identifies the working interface; because the working interface is always assigned channel number 1, this is the only valid option

Mode Controller Configuration

area

Syntax no area { *areaId* | *areaIdInt* }

Description This command has only a **no** version. See the no area command for a complete description.

area-authentication

Syntax [no] area-authentication { csnp | psnp }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables or disables (suppresses) simple text authentication or HMAC MD5 authentication of IS-IS level 1 CSNP packets or PSNP packets. The **no** version restores the default behavior, in which authentication of IS-IS level 1 CSNPs and PSNPs is disabled.

- Options**
- csnp—Enables authentication of IS-IS level 1 complete sequence number PDUs (CSNPs)
 - psnp—Enables authentication of IS-IS level 1 partial sequence number PDUs (PSNPs)

Mode Router Configuration

area-authentication-key

Syntax `area-authentication-key [0 | 8] authKey`
 `no area-authentication-key`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns a password used by neighboring routers for authentication of IS-IS level 1 LSPs, CSNPs, and PSNPs. The **no** version deletes the password.



NOTE: Issuing this command enables simple authentication of level 1 LSPs only. To enable authentication of level 1 CSNPs or PSNPs, use the **area-authentication** command.

- Options**
- 0—Indicates the *authKey* is entered in unencrypted form (plaintext); this is the default option
 - 8—Indicates the *authKey* is entered in encrypted form (ciphertext)
 - *authKey*—Password, string of up to 8 characters

Mode Router Configuration

area default-cost

Syntax `area { areaId | areaIdInt } default-cost defaultCost`
 `no area { areaId | areaIdInt } default-cost`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a cost for the default summary route sent into a stub area. A stub area is an OSPF area that carries a default route, intra-area routes, and interarea routes, but does not carry external routes. You cannot configure virtual links across a stub area. Stub areas cannot contain an AS boundary router. The **no** version removes the configured default route cost.

- Options**
- *areaId*—OSPF area ID in IP address format
 - *areaIdInt*—OSPF area ID as a decimal value 0–4294967295
 - *defaultCost*—Stub area's advertised external route cost (cost metric); an integer in the range 0–16777215

Mode Router Configuration

area-message-digest-key

Syntax `area-message-digest-key keyId hmac-md5 [0 | 8] key`
`[start-accept startAcceptTime [{ startAcceptMonth startAcceptDay | startAcceptDay startAcceptMonth } startAcceptYear]]`
`[start-generate startGenTime [{ startGenMonth startGenDay | startGenDay startGenMonth } startGenYear]]`
`[stop-accept { never | stopAcceptTime [{ stopAcceptMonth stopAcceptDay | stopAcceptDay stopAcceptMonth } stopAcceptYear] }]`
`[stop-generate { never | stopGenTime [{ stopGenMonth stopGenDay | stopGenDay stopGenMonth } stopGenYear] }]`

`no area-message-digest-key keyId`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies an HMAC MD5 key that the router uses to create a secure, encrypted message digest of each IS-IS level 1 packet (LSPs, CSNPs, and PSNPs). The digest is inserted into the packet from which it is created. Using this algorithm for area routers protects against unauthorized routers injecting false routing information into your network.

You can specify when the router will start (default is the current time) and stop (default is never) accepting packets that include a digest made with this key. You can specify when the router will start (default is the current time plus 2 minutes) and stop (default is never) generating packets that include a digest made with this key. The **no** version deletes the key specified by the *keyId*.



NOTE: Issuing this command enables MD5 authentication of level 1 LSPs only. To enable authentication of level 1 CSNPs or PSNPs, use the **area-authentication** command.

- Options**
- *keyId*—Integer from 1 to 255 that is a unique identifier for the secret key, sent with the message digest in the packet.
 - 0—Indicates the *key* is entered in unencrypted form (plaintext); default option
 - 8—Indicates the *key* is entered in encrypted form (ciphertext)
 - *key*—String of up to 20 alphanumeric characters; secret key used by the HMAC MD5 algorithm to generate the message digest
 - *startAcceptTime*, *startAcceptMonth*, *startAcceptDay*, *startAcceptYear*—Time, month, day, year that the router will start accepting packets created with this password. Use military time format *HH : MM[: SS]*.
 - *startGenTime*, *startGenMonth*, *startGenDay*, *startGenYear*—Time, month, day, year that the router will start inserting this password into packets. Use military time format *HH : MM[: SS]*.

- *never*—Indicates the router never stops accepting or generating packets; overrides previously specified stop times and keeps using the authentication key in sending and receiving PDUs with the corresponding authentication indefinitely
- *stopAcceptTime, stopAcceptMonth, stopAcceptDay, stopAcceptYear*—Time, month, day, year that the router will stop accepting packets created with this password. Use military time format *HH : MM[: SS]*.
- *stopGenTime, stopGenMonth, stopGenDay, stopGenYear*—Time, month, day, year that the router will stop inserting this password into packets. Use military time format *HH : MM[: SS]*.

Mode Router Configuration

area nssa

Syntax [no] area { *areaId* | *areaIdInt* } nssa [default-information-originate [always | metric *absoluteValue* | metric-type 1 | metric-type 2 | route-map *mapTag*]*] [no-summary]

Release Information Command introduced before JUNOS Release 7.1.0.
no-summary keyword added in JUNOS Release 7.2.0.

Description Configures an area as an NSSA and controls generation of type 7 default LSAs. NSSAs are similar to stub areas but have the additional capability of importing AS external routes in a limited fashion. The **no** version removes the specified option for default-information-originate, removes default-information-originate, or removes the NSSA designation from the area.

- Options**
- *areaId*—OSPF area ID in IP address format
 - *areaIdInt*—OSPF area ID as a decimal value in the range 0–4294967295
 - default-information-originate—Causes the generation of a type 7 default LSA if a default route exists in the routing table.
 - always—Creates the default route if it does not exist
 - *absoluteValue*—Metric applied to the generated type 7 default LSAs; ranges from 0–4294967295
 - metric-type 1—Cost of the external routes is equal to the sum of all internal costs and the external cost
 - metric-type 2—Cost of the external routes is equal to the external cost alone; this is the OSPF default
 - *mapTag*—String of up to 32 alphanumeric characters that specifies a route map applied to the generated type 7 default LSAs
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line
 - no-summary—Restricts T3 summary LSAs from flowing into the NSSA area (T7 external LSAs and T3 default route LSAs are still injected into the area)

Mode Router Configuration

area range

Syntax For OSPFv2:

```
[ no ] area { areaId | areaIdInt } range ipAddress mask [ do-not-advertise ]
[ cost costValue ]
```

For OSPFv3:

```
[ no ] area { areaId | areaIdInt } range ipv6Prefix/ipv6PrefixLength
[ do-not-advertise | advertise | cost costValue ]
```

Release Information Command introduced before JUNOS Release 7.1.0.
cost keyword and *costValue* variable for OSPFv2 added in JUNOS Release 8.1.0.

Description Aggregates routes at an area boundary. By default, the range of configured networks is advertised in type 3 (summary) LSAs. The **no** version disables this function.

- Options**
- *areaId*—OSPF area ID in IP address format
 - *areaIdInt*—OSPF area ID as a decimal value in the range 0–4294967295
 - *ipAddress*—IP address to match
 - *mask*—IP address mask
 - *ipv6Prefix*—IPv6 network number to match
 - *ipv6PrefixLength*—Length of the IPv6 prefix; a decimal value that indicates how many of the higher-order contiguous bits of the IPv6 address make up the prefix (the network portion of the IPv6 address). A slash (/) must precede this value.
 - do-not-advertise—Specifies that the range of configured networks is not advertised
 - advertise—Specifies that the range of configured networks is advertised (IPv6 only)
 - *costValue*—Cost value for the specified range of networks in the range 0–65535

Mode Router Configuration

area stub

Syntax [no] area { *areaId* | *areaIdInt* } stub [no-summary]

Release Information Command introduced before JUNOS Release 7.1.0.
no-summary keyword for OSPFv2 added in JUNOS Release 7.2.0.

Description Defines an area as a stub area. A stub area is an OSPF area that carries a default route, intra-area routes, and interarea routes, but does not carry AS external routes. This reduces the size of the area's OSPF database and decreases memory usage for external routers in the stub area. The **no** version disables this function.

- Options**
- *areaId*—OSPF area ID in IP address format
 - *areaIdInt*—OSPF area ID as a decimal value in the range 0–4294967295
 - no-summary—Specifies that the summary LSA not be sent into the stub area

Mode Router Configuration

area virtual-link

Syntax [no] area { *areaId* | *areaIdInt* } virtual-link *ipAddress*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines an OSPF virtual link. The **no** version removes the virtual link.

- Options**
- *areaId*—OSPF area ID in IP address format
 - *areaIdInt*—OSPF area ID as a decimal value in the range 0–4294967295
 - *ipAddress*—IP address associated with the virtual link neighbor

Mode Router Configuration

area virtual-link authentication-key

Syntax [no] area { *areaID* | *areaIdInt* } virtual-link *ipAddress* authentication-key [0 | 8] *key*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures simple password (type 1) authentication for OSPF virtual links. The **no** version removes the password.

- Options**
- *areaId*—OSPF area ID in IP address format
 - *areaIdInt*—OSPF area ID as a decimal value in the range 0–4294967295
 - *ipAddress*—IP address of the virtual link neighbor
 - 0—Indicates the *key* is entered in unencrypted form (plaintext); this is the default option
 - 8—Indicates the *key* is entered in encrypted form (ciphertext)
 - *key*—Password to be used by neighbors; string of up to 16 alphanumeric characters. All neighboring routers on the same network must have the same password.

Mode Router Configuration

area virtual-link authentication message-digest

Syntax [no] area { *areaID* | *areaIdInt* } virtual-link *ipAddress* authentication message-digest

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that MD5 authentication is used for the virtual link. The **no** version sets the authentication for the virtual link to none, but leaves any configured MD5 key intact.

- Options**
- *areaId*—OSPF area ID in IP address format
 - *areaIdInt*—OSPF area ID as a decimal value in the range 0–4294967295
 - *ipAddress*—IP address of the virtual link neighbor

Mode Router Configuration

area virtual-link authentication-none

Syntax [no] area { *areaId* | *areaIdInt* } virtual-link *ipAddress* authentication-none

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that no authentication is to be used for the virtual link. The **no** version has no effect.

- Options**
- *areaId*—OSPF area ID in IP address format
 - *areaIdInt*—OSPF area ID as a decimal value in the range 0–4294967295
 - *ipAddress*—IP address of the virtual link neighbor

Mode Router Configuration

area virtual-link dead-interval

Syntax [no] area { *areaId* | *areaIdInt* } virtual-link *ipAddress* dead-interval *deadInterval*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines an OSPF virtual link and the time interval allowed for detecting a dead router. The **no** version removes the virtual link's dead interval.

- Options**
- *areaId*—OSPF area ID in IP address format
 - *areaIdInt*—OSPF area ID as a decimal value in the range 0–4294967295
 - *ipAddress*—IP address of the virtual link neighbor
 - *deadInterval*—Integer in the range 0–2147483647 seconds; default value is 40 seconds

Mode Router Configuration

area virtual-link hello-interval

Syntax [no] area { *areaId* | *areaIdInt* } virtual-link *ipAddress* hello-interval *helloInterval*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines an OSPF virtual link and the time between the hello packets. The hello interval value must be the same for both ends of the virtual link. The **no** version removes the virtual link's hello interval.

- Options**
- *areaId*—OSPF area ID in IP address format.
 - *areaIdInt*—OSPF area ID as a decimal value in the range 0–4294967295
 - *ipAddress*—IP address associated with the virtual link neighbor
 - *helloInterval*—Integer in the range 1–65535 seconds; default value is 10 seconds

Mode Router Configuration

area virtual-link message-digest-key md5

Syntax `area { areaId | areaIdInt } virtual-link ipAddress
 message-digest-key md5KeyId md5 [0 | 8] msgDigestKey
 no area { areaId | areaIdInt } virtual-link ipAddress message-digest-key md5KeyId`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables MD5 authentication and configures MD5 keys for virtual links. The `no` version deletes MD5 keys.



NOTE: If you delete all the MD5 keys, the authentication type for the virtual link is still MD5, but you need to configure MD5 keys.

To disable MD5 authentication for the virtual link, use the `area virtual-link authentication-none` command.

- Options**
- *areaId*—OSPF area ID in IP address format
 - *areaIdInt*—OSPF area ID as a decimal value in the range 0–4294967295
 - *ipAddress*—IP address of the virtual link neighbor
 - *md5KeyId*—Key identifier in the range 1–255
 - 0—Indicates the *msgDigestKey* is entered in unencrypted form (plaintext); this is the default option
 - 8—Indicates the *msgDigestKey* is entered in encrypted form (ciphertext)
 - *msgDigestKey*—Password to be used by neighbors; string of up to 16 alphanumeric characters. All neighboring routers on the same network must have the same password.

Mode Router Configuration

area virtual-link retransmit-interval

Syntax [no] area { *areaId* | *areaIdInt* } virtual-link *ipAddress* retransmit-interval *retransmInterval*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines an OSPF virtual link and the time between link-state advertisement retransmissions for the adjacency belonging to the virtual link. The **no** version removes the virtual link's retransmit interval.

- Options**
- *areaId*—OSPF area ID in IP address format.
 - *areaIdInt*—OSPF area ID as a decimal value in the range 0–4294967295
 - *ipAddress*—IP address of the virtual link neighbor
 - *retransmInterval*—LSA retransmit interval; an integer in the range 0–3600 seconds; default value is 5 seconds

Mode Router Configuration

area virtual-link transmit-delay

Syntax [no] area { *areaId* | *areaIdInt* } virtual-link *ipAddress* transmit-delay *transmDelay*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines an OSPF virtual link and the estimated time it takes to transmit a link-state update packet on the virtual link. The **no** version removes the virtual link's transmit delay.

- Options**
- *areaId*—OSPF area ID in IP address format
 - *areaIdInt*—OSPF area ID as a decimal value in the range 0–4294967295
 - *ipAddress*—IP address associated with the virtual link neighbor
 - *transmDelay*—LSA transmit delay; an integer in the range 0–3600 seconds; default value is 1 second

Mode Router Configuration

arp

Syntax To add a permanent ARP cache entry in Global Configuration mode:

```
[ no ] arp [ vrf vrfName ] ipAddress interfaceType interfaceSpecifier
[ macAddress [ validate ] ]
```

To modify the subscriber policy for ARP packets in Subscriber Policy Configuration mode:

```
arp { permit | deny }
```

```
no arp
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description In Global Configuration mode, adds a permanent entry in the ARP cache. This command applies only to Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet interfaces, and bridged Ethernet interfaces configured over ATM 1483. The **no** version removes an entry from the ARP cache.

In Subscriber Policy Configuration mode, modifies the subscriber policy for ARP to define whether the subscriber (client) interfaces belonging to a bridge group or VPLS instance forward (permit) or filter (deny) ARP packets. The **no** version restores the default value, permit ARP packets.

In Subscriber Policy Configuration mode, you cannot change the default subscriber policy values for trunk (server) interfaces belonging to a bridge group or VPLS interface. You also cannot change the default subscriber policy values for a VPLS virtual core interface, which acts as a trunk interface. The VPLS virtual core interface represents all of the MPLS tunnels from the router to the remote VPLS edge (VE) device.

- Options**
- *vrfName*—Name of the VRF to which the command applies; string of 1–32 alphanumeric characters
 - *ipAddress*—IP address in 32-bit dotted-decimal format corresponding to the local data link address
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *macAddress*—MAC address of the interface
 - *validate*—Allows the inclusion of MAC validation entries
 - *permit*—Specifies that the subscriber interface associated with the bridge group or VPLS instance forwards ARP packets
 - *deny*—Specifies that the subscriber interface associated with the bridge group or VPLS instance filters ARP packets

Mode Global Configuration, Subscriber Policy Configuration

arp spoof-check

Syntax [no] arp spoof-check

Release Information Command introduced in JUNOS Release 9.3.0.

Description Configures the router to check for spoofed ARP packets received on an IP interface. By default, the router checks all ARP packets received on a major IP interface or a subinterface to identify and discard spoofed ARP packets. The no version disables checking for spoofed ARP packets received on the interface.

Mode Interface Configuration

arp timeout

Syntax `arp timeout timeoutVal`

`no arp timeout`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies how long an entry remains in the ARP cache. You can set the ARP timeout on Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces, and bridged Ethernet interfaces configured over ATM 1483. The default value is 21600 seconds (6 hours). Use the **show configuration** command to display the current value. The **no** version restores the default value.

Options ■ *timeoutVal*—Time in seconds that an entry remains in the ARP cache

Mode Interface Configuration

assured-rate

Syntax `assured-rate { assuredRate | hierarchical | [operator operandValue]* }`
 `no assured-rate`

Release Information Command introduced before JUNOS Release 7.1.0.
 operator and *operandValue* variables added in JUNOS Release 7.1.0.

Description Sets the assured rate for the scheduler profile. The assured rate overrides the HRR weight of the scheduler node or queue. The **no** version deletes the assured rate.

- Options**
- *assuredRate*—Constant assured rate in bits per second; in the range 25000–1000000000 (25 Kbps to 1 Gbps)
 - *hierarchical*—Specifies that the node use the hierarchical assured rate (HAR) feature, in which the scheduler node's assured rate is dynamically adjusted based on the sum of the assured rates of all its child nodes and queues
 - *operator*—Mathematical function
 - *operandValue*—Input for the operator; can be a QoS parameter definition name or an integer
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Scheduler Profile Configuration

- Related Topics**
- Configuring an Assured Rate for a Scheduler Node or Queue
 - Configuring a Basic Parameter Definition for QoS Administrators

atm

Syntax atm { ubr | ubrpcr *pcr* | nrtvbr *pcr scr mbs* | rtvbr *pcr scr mbs* | cbr *pcr* }
 no atm

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures traffic-shaping parameters for PPPoA via domain-based parameters. The **no** version removes the ATM traffic-shaping configuration.

- Options**
- ubr—Sets the traffic category to unspecified bit rate
 - ubrpcr—Sets the traffic category to unspecified bit rate with peak cell rate
 - nrtvbr—Sets the traffic category to non-real time variable bit rate
 - rtvbr—Set the traffic category to real time variable bit rate
 - cbr—Sets the traffic category to constant bit rate
 - *pcr*—Peak cell rate in the range 0–4294967295 Kbps
 - *scr*—Sustained cell rate in the range 0–4294967295 Kbps
 - *mbs*—Maximum burst size in the range 0–4294967295 Kbps

Mode Domain Map Configuration

atm aal5 description

Syntax atm aal5 description *name*
 no atm aal5 description

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns a text description or alias to an ATM AAL5 interface. The **no** version removes the text description or alias. Use the show atm aal5 interface command to display the text description.

Options ■ *name*—Alias for the AAL5 interface; up to 32 characters

Mode Interface Configuration

atm aal5 shutdown

Syntax [no] atm aal5 shutdown

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the administrative state of an ATM AAL5 interface to disabled. The **no** version enables a disabled interface.

Mode Interface Configuration

atm aal5 snmp trap link-status

Syntax [no] atm aal5 snmp trap link-status

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables SNMP link status traps on the AAL5 layer on a per-interface basis. The **no** version disables the traps.

Mode Interface Configuration

atm atm1483 advisory-rx-speed

Syntax atm atm1483 advisory-rx-speed *speed*
 no atm atm1483 advisory-rx-speed

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets an advisory receive (RX) speed that the LAC sends in the RX Connect-Speed AVP [38] to the LNS. The **no** version restores the default behavior, in which the RX speed is not sent to the LNS.

Options ■ *speed*—Speed in the range 0–2147483647 kbps

Mode Profile Configuration, Subinterface Configuration

atm atm1483 auto-configure

Syntax atm atm1483 auto-configure *upperInterfaceType*
 [lockout-time { *minValue* *maxValue* | none }]

no atm atm1483 auto-configure *upperInterfaceType* [lockout-time]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies one or more types of dynamic upper interface encapsulations that are accepted or detected by a dynamic ATM 1483 subinterface. Optionally, specifies the lockout time range for the encapsulation type. You can issue this command repeatedly in Profile Configuration mode to include autodetection of multiple upper interface encapsulation types within the base profile for a dynamic ATM 1483 subinterface. The **no** version terminates detection of the specified encapsulation type.



NOTE: Encapsulation type lockout is available for bridged Ethernet, IP, PPP, and PPPoE encapsulation types.

- Options**
- *upperInterfaceType*—One of the following dynamic encapsulation types:
 - bridgedEthernet
 - ip
 - ppp
 - pppoe
 - *minValue*—Minimum lockout time in the range 1–86400 seconds (24 hours); default value is 1 second
 - *maxValue*—Maximum lockout time in the range 1–86400 seconds (24 hours); default value is 300 seconds (5 minutes)
 - none—Disables lockout for the specified dynamic encapsulation type

Mode Profile Configuration

atm atm1483 description

Syntax atm atm1483 description *name*
 no atm atm1483 description

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns a text description or alias to an ATM 1483 interface. The **no** version removes the text description or alias. Use the show atm subinterface command to display the text description.

Options ■ *name*—Text string or alias for the ATM 1483 interface; up to 255 characters

Mode Profile Configuration, Subinterface Configuration

atm atm1483 export-subinterface-description

Syntax [no] atm atm1483 export-subinterface-description

Release Information Command introduced before JUNOS Release 7.1.0.

Description Exports ATM 1483 subinterface descriptions to the line module. The **no** version restores the default behavior, where ATM 1483 subinterface descriptions are not sent to the line module.

Mode Global Configuration

atm atm1483 mtu

Syntax atm atm1483 mtu *size*

no atm atm1483 mtu

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the MTU size for an ATM 1483 subinterface. The **no** version restores the default MTU size of 9180.

Options ■ *size*—Maximum number of packet transmissions permitted on an ATM 1483 subinterface; in the range 256–9180; default value is 9180

Mode Subinterface Configuration

atm atm1483 profile

Syntax atm atm1483 profile *upperInterfaceType* *profileName*
 no atm atm1483 profile *upperInterfaceType*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Adds a nested profile assignment to a base profile for a dynamic ATM 1483 subinterface. A nested profile assignment references another profile that dynamically configures upper interface encapsulation types over the ATM 1483 subinterface. The **no** version removes the profile assignment for the upper interface type.

- Options** ■ *upperInterfaceType*—One of the following dynamic encapsulation types:
- bridgedEthernet
 - ip
 - ppp
 - pppoe
- *profileName*—Profile name of up to 80 characters

Mode Profile Configuration

atm atm1483 shutdown

Syntax [no] atm atm1483 shutdown

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the administrative state of an ATM 1483 subinterface to disabled. The **no** version enables a disabled subinterface.

Mode Subinterface Configuration

atm atm1483 snmp trap link-status

Syntax [no] atm atm1483 snmp trap link-status

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables SNMP link status traps on the ATM1483 layer. The **no** version disables the traps.

Mode Subinterface Configuration

atm atm1483 subscriber

Syntax atm atm1483 subscriber *upperInterfaceType* { user | user-prefix } *userName*
 domain *domainName* [{ password | password-prefix }
password] [no-authenticate]

no atm atm1483 subscriber *upperInterfaceType*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures a local subscriber (when one cannot be obtained externally, as in PPP) for a dynamic upper interface encapsulation type configured over a dynamic ATM 1483 subinterface. A subscriber supports authentication and configuration from the RADIUS server. The **no** version removes the subscriber.

- Options**
- *upperInterfaceType*—One of the following dynamic encapsulation types:
 - bridgedEthernet
 - ip
 - user—Employs the username as specified
 - user-prefix—Appends the interface physical location to the username
 - *userName*—RADIUS username
 - *domainName*—Domain name
 - password—Employs the password as specified
 - password-prefix—Appends the interface physical location to the password
 - *password*—RADIUS password
 - no-authenticate—Disables authentication

Mode Profile Configuration

atm auto-configuration

Syntax [no] atm auto-configuration

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables autoconfiguration of ILMI. Autoconfiguration is enabled by default. This command overrides any previous configuration of the **atm uni-version** command. The **no** version disables auto configuration and sets the ILMI parameters to the UNI version configured using the **atm uni-version** command, which has a default value of UNI 4.0.

Mode Interface Configuration

atm bulk-config

Syntax atm bulk-config *bulkConfigName* [vc-range *vpiStart vpiEnd vciStart vciEnd*]*
 no atm bulk-config *bulkConfigName* [vc-range *vpiStart vpiEnd vciStart vciEnd*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures a range of ATM PVCs for use by a dynamic ATM 1483 subinterface, and assigns a name to the virtual circuit (VC) range. Each VC range consists of one or more nonoverlapping VC subranges. A VC subrange is a group of VCs that resides within the specified VPI and VCI ranges. You can configure multiple VC ranges on an ATM AAL5 interface. The **no** version removes the specified VC range (including all subranges in the range) from the ATM AAL5 interface or the specified subrange from the VC range. The **no** version also removes any overriding profile assignments for ATM PVCs within the deleted VC range or VC subrange.



NOTE: The total number of VCs configured with the **atm bulk-config** command cannot exceed the maximum ATM VC capacity of the line module you are using. For details about the ATM VC capacity of supported line modules, see *JUNOS Release Notes, Appendix A, System Maximums*.

- Options**
- *bulkConfigName*—Name of the VC range; string of up to 80 characters
 - *vpiStart*—Starting virtual path identifier (inclusive) of the VC subrange you are configuring
 - *vpiEnd*—Ending virtual path identifier (inclusive) of the VC subrange you are configuring
 - *vciStart*—Starting virtual circuit identifier (inclusive) of the VC subrange you are configuring
 - *vciEnd*—Ending virtual circuit identifier (inclusive) of the VC subrange you are configuring
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Interface Configuration

atm bulk-config modify

Syntax atm bulk-config *bulkConfigName* modify vc-range *vpiStart vpiEnd vciStart vciEnd*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Modifies the VC subrange values for the specified bulk configuration VC range. If the new subrange encompasses previously configured subranges within that range, those subranges are merged into the new one, freeing subrange resources. There is no **no** version.

- Options**
- *bulkConfigName*—Name of the VC range; string of up to 80 characters
 - *vpiStart*—Starting virtual path identifier (inclusive) of the VC subrange you are configuring
 - *vpiEnd*—Ending virtual path identifier (inclusive) of the VC subrange you are configuring
 - *vciStart*—Starting virtual circuit identifier (inclusive) of the VC subrange you are configuring
 - *vciEnd*—Ending virtual circuit identifier (inclusive) of the VC subrange you are configuring

Mode Interface Configuration

atm bulk-config shutdown

Syntax [no] atm bulk-config *bulkConfigName* shutdown
[vc-range *vpiStart vpiEnd vciStart vciEnd*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Administratively disables (shuts down) the specified VC range or subrange. The **no** version reenables the specified VC range or the specified subranges; this is the default condition.

- Options**
- *bulkConfigName*—Name of the VC range; string of up to 80 characters
 - *vpiStart*—Starting virtual path identifier (inclusive) of the VC subrange you are configuring
 - *vpiEnd*—Ending virtual path identifier (inclusive) of the VC subrange you are configuring
 - *vciStart*—Starting virtual circuit identifier (inclusive) of the VC subrange you are configuring
 - *vciEnd*—Ending virtual circuit identifier (inclusive) of the VC subrange you are configuring

Mode Interface Configuration

atm cac

Syntax [no] atm cac [*subscriptionBandwidth*] [*ubr ubrWeight*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables CAC on the ATM interface. If the subscription limit or UBR weight parameters are set to zero, the router uses the effective port bandwidth as the subscription bandwidth. The effective bandwidth varies according to line module. The **no** version disables CAC on the interface.



NOTE: If you modify one of these parameters after CAC is enabled, you must modify both parameters. Otherwise, the parameter not specified reverts to its default value.

- Options**
- *subscriptionBandwidth*—Maximum allowable bandwidth on this port in the range 0–2147482647 Kbps; default value is 0
 - *ubrWeight*—Bandwidth associated with UBR and UBR-PCR connections in the range 0–2147482647 Kbps; default value is 0

Mode Interface Configuration

atm cell-packing

Syntax atm cell-packing *maxCellsPerPacket* mcpt-timer *timerIdentifier*
no atm cell-packing

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures cell concatenation parameters for an ATM 1483 subinterface that provides ATM layer 2 services over MPLS with virtual channel connection (VCC) cell relay encapsulation. The **no** version restores the default cell concatenation parameters for the subinterface.



NOTE: See the **atm mcpt-timers** command for information about configuring systemwide values for the three ATM Martini cell packing timers to define the cell collection time threshold.

- Options**
- *maxCellsPerPacket*—Maximum number of ATM cells in the range 1–190 that the router can concatenate in a single VCC cell relay–encapsulated packet and transmit on an MPLS pseudowire connection; default value is 1 cell per packet
 - *timerIdentifier*—Integer in the range 1–3 that identifies which of the three ATM Martini cell packing timers (timer 1, timer 2, or timer 3) you want to use to detect timeout of the cell collection time threshold; default value is 1. When the timer expires, the router forwards the packet even if the number of concatenated ATM cells in the packet is fewer than the specified maximum number of cells per packet.

Mode Subinterface Configuration

- Related Topics**
- *Configuring an MPLS Pseudowire with VCC Cell Relay Encapsulation* in the *JUNOS BGP and MPLS Configuration Guide*

atm-cell-mode

Syntax [no] atm-cell-mode

Release Information Command introduced in JUNOS Release 7.2.0.

Description Accounts for the ATM cell tax in rate calculations for interface types that support rate-limiting and are stackable over ATM. The **no** version restores the default, which uses the frame size with the layer 2 header included.

Mode Policy List Configuration

Related Topics ■ [Enabling ATM Cell Mode](#)

atm classifier-list

Syntax atm classifier-list *classifierName* [traffic-class *trafficClassName*]
 [color { green | yellow | red }] [user-packet-class *userPacketClassValue*]
 [clp *clpValue*]

no atm classifier-list *classifierName* [*classifierNumber*]

Release Information Command introduced in JUNOS Release 7.1.0.

Description Creates a classifier control list that can only be used in ATM policy lists. The **no** version removes the ATM classifier control list. ATM packets are classified on CLP. The CLP bit is not available on frame-based interfaces on E Series Broadband Services Router line modules.

- Options**
- *classifierName*—Name of the classifier control list entry
 - *trafficClassName*—Name of the traffic class to match
 - green—Matches packet color to green, indicating a low drop preference
 - yellow—Matches packet color to yellow, indicating a medium drop preference
 - red—Matches packet color to red, indicating a high drop preference
 - *userPacketClassValue*—User packet value to match in the range 0–15
 - *clpValue*—Value of the CLP, 0 or 1
 - *classifierNumber*—Index of the classifier control list entry to be deleted

Mode Global Configuration

Related Topics ■ Creating or Modifying Classifier Control Lists for ATM Policy Lists

atm class-vc

Syntax atm class-vc *vcClassName*
 no atm class-vc [*vcClassName*]

Release Information Command introduced in JUNOS Release 7.3.0.

Description Assigns a previously configured VC class to a base profile for a dynamic ATM 1483 subinterface. Issuing this command applies the set of attributes in the specified VC class to all bulk-configured VC ranges that are dynamically created from this profile. The **no** version removes the VC class association with the base profile.

Options ■ *vcClassName*—Name of the VC class configured with the vc-class atm command

Mode Profile Configuration

atm clock internal

Syntax [no] atm clock internal [*internalSource*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Causes the ATM interface to generate the transmit clock internally. The **no** version causes ATM interfaces to recover the clock from the received signal. If the internal clock is chosen and no internal source is specified, then the internal clock source is taken from the line module.

Options ■ *internalSource*—One of the following:

- module—Specifies that the internal clock is from the line module
- chassis—Specifies that the internal clock is from the configured router clock

Mode Interface Configuration

atm description

Syntax atm description *name*
 no atm description

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns a text description or alias to the ATM interface. The first 32 characters of the description are pushed out to RADIUS during authentication and accounting. The show atm interface command displays the text description. The **no** version removes the text description or alias.

Options ■ *name*—Text string or alias of up to 255 characters; can include the # (pound sign) character

Mode Interface Configuration

atm dos-protection-group

Syntax atm dos-protection-group *groupName*
 no atm dos-protection-group

Release Information Command introduced in JUNOS Release 8.1.0.

Description Attaches an ATM denial of service (DoS) protection group to an interface. The **no** version removes the DoS protection group.

Options ■ *groupName*—Name of the DoS protection group; string of up to 31 alphanumeric characters

Mode Interface Configuration

atm framing

Syntax atm framing *framingType*
 no atm framing

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures T3 or E3 framing on an ATM interface. The **no** version returns framing to the default. For a T3 interface, the default value is cbitplcp. For an E3 interface, the default value is g751plcp.

- Options** ■ *framingType*—One of the following:
- cbitadm—c-bit with ATM direct mapping for a DS3 (T3) interface
 - cbitplcp—c-bit with PLCP framing for a DS3 (T3) interface (default for T3)
 - g832adm—G.832 ATM direct mapping for an E3 interface
 - g751adm—G.751 ATM direct mapping for an E3 interface
 - g751plcp—G.751 PLCP mapping for an E3 interface (default for E3)
 - m23adm—M23 ATM direct mapping for a DS3 (T3) interface
 - m23plcp—M23 with PLCP framing for a DS3 (T3)

Mode Interface Configuration

atm ilmi-enable

Syntax [no] atm ilmi-enable

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables ILMI on the interface. The **no** version removes the ILMI PVC.

Mode Interface Configuration

atm ilmi-keepalive

Syntax [no] atm ilmi-keepalive [*seconds*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables generation of ILMI keepalive messages on the router, affecting the operational state of the ATM interface. The **no** version disables the generation of keepalive messages.

Options ■ *seconds*—Number in the range 0–4294967295; the interval in seconds between two consecutive ILMI keepalive requests

Mode Interface Configuration

atm lbo

Syntax atm lbo { long | short }
 no atm lbo

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the cable length (line build-out) for the ATM T3 or E3 interface. The length of cable determines power requirements. The **no** version restores the default value.

- Options** ■ long—Specifies cable length in the range 226–450 feet
 ■ short—Specifies cable length in the range 0–225 feet (the default)

Mode Interface Configuration

atm mcpt-timers

Syntax atm mcpt-timers *timer1 timer2 timer3*
 no atm mcpt-timers

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures systemwide values for the three ATM Martini cell packing timers. These timers define the time threshold that the router uses to collect and concatenate ATM cells in a single VCC cell relay–encapsulated packet and transmit the packet on an MPLS pseudowire connection. When the timer expires, the router forwards the packet even if the number of concatenated ATM cells in the packet is fewer than the specified maximum number of cells per packet. The **no** version restores the default values for all three timers.



NOTE: See the **atm cell-packing** command for information about specifying the maximum number of concatenated cells per packet and identifying which of the three ATM Martini cell packing timers you want to use to detect timeout of the cell collection threshold.

- Options**
- *timer1*—Number of microseconds in the range 100–4095; default value is 100
 - *timer2*—Number of microseconds in the range 100–4095; default value is 500
 - *timer3*—Number of microseconds in the range 100–4095; default value is 1000

Mode Global Configuration

Related Topics

- *Configuring an MPLS Pseudowire with VCC Cell Relay Encapsulation in the JUNOS BGP and MPLS Configuration Guide*

atm oam

Syntax `atm oam [vpi] [[seg-loopback | end-loopback [loopback-timer time]]`
`[cc { source | sink | both }]]`

`no atm oam [vpi] [[seg-loopback | end-loopback [loopback-timer time]]]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures F4 OAM on an interface or circuit. The no version deletes F4 OAM circuits.



NOTE: If you do not specify any options, both F4 end-to-end OAM and F4 segment OAM are enabled on all VPIs on the interface.

- Options**
- *vpi*—VPI on which you want to enable F4 OAM. If you do not specify a VPI, F4 OAM flow is enabled on all VPIs on the interface.
 - *seg-loopback*—Enables F4 segment OAM
 - *end-loopback*—Enables F4 end-to-end OAM
 - *loopback-timer*—To generate F4 loopback cells on the VPI, you must configure the loopback timer; you can set the loopback timer only for end-to-end loopback
 - *time*—Time interval in the range 1–600 seconds between transmissions of F4 loopback cells.
 - *cc*—Enables CC cells on the PVC; you can enable CC cells only on data circuits, not on control circuits, such as ILMI or signaling circuits
 - *sink*—Enables this VC as a sink point (cell receiver)
 - *source*—Enables this VC as the source point (cell generator)
 - *both*—Enables this VC as both a sink point and a source point

Mode Interface Configuration, Subinterface Configuration

atm oam flush

Syntax [no] atm oam flush [alarm-cells]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the router to ignore all OAM cells received on an ATM interface, and to stop sending OAM cells on this interface. OAM performs fault management and performance management functions on an ATM interface. The **no** version disables OAM flush on the interface.

Options ■ alarm-cells—Causes the router to ignore only AIS and RDI cells and to accept all other OAM cells

Mode Interface Configuration

atm oam loopback-location

Syntax atm oam loopback-location *locationID*

[no] atm oam loopback-location

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the location ID of the ATM interface. The **no** version returns the loopback location to the default setting of all 1s (ones).

Options ■ *locationID*—Value of the four-octet long location ID of the ATM interface

Mode Interface Configuration

atm policy

Syntax atm policy { input | output } *policyName*
 [statistics { enabled [preserve | merge] | disabled [merge] } | merge]
 no atm policy { input | output } [*policyName*]

Release Information Command introduced in JUNOS Release 7.1.0.
merge keyword added in JUNOS Release 7.2.0.

Description Assigns a policy list to the ingress or egress of an ATM interface. If you enter this command when the policy list does not exist, the router creates a policy list with a filter rule as the default. You must specify the **input** or **output** keyword to assign the policy list to the ingress or egress of the interface. The **no** version removes the association between a policy list and an interface.

- Options**
- input—Applies policy to data arriving at this interface
 - output—Applies policy to data leaving this interface
 - *policyName*—Name of the policy; a maximum of 40 characters
 - statistics—Enables or disables collection of policy routing statistics
 - enabled—Enables collection of policy routing statistics
 - preserve—Preserves existing statistics for any classifier-list that is the same for both the new and old policy attachments when you attach a new policy to an interface
 - disabled—Disables collection of policy routing statistics
 - merge—Enables merging of multiple policies to form a single policy

Mode Interface Configuration

Related Topics ■ Setting a Statistics Baseline for Policies

atm policy-list

Syntax [no] atm policy-list *policyName*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Creates an ATM policy list and accesses Policy List Configuration mode. If you execute an **atm policy-list** command and type **exit**, the router creates a policy list with a filter rule as the default. Attaching this policy list to an interface filters all packets on that interface. The **no** version removes a policy list.

Options ■ *policyName*—Name of the policy list; a maximum of 40 characters

Mode Global Configuration

Related Topics ■ Creating Policy Lists for ATM

atm pvc

Syntax To create a PVC on an ATM interface when using the **aal5snap**, **aal5autoconfig**, or **aal5mux ip** encapsulation type:

```
atm pvc vcd vpi vci encapsulation [ cbr cbr | peak [ average burst [ rt ] ] ]
[ oam [ seconds | cc [ segment | end-to-end ] { source | sink | both } ] ]
[ inArp [ minutes ] ]
```

```
no atm pvc vcd
```

To create a PVC on an ATM interface when using the **aal5all**, **aal0**, or **ilmi** encapsulation type:

```
atm pvc vcd vpi vci encapsulation [ cbr cbr | peak [ average burst [ rt ] ] ]
```

```
no atm pvc vcd
```

To use a profile to apply encapsulation and traffic-shaping parameters to a bulk range of PVCs configured for a dynamic ATM 1483 subinterface:

```
atm pvc encapsulation [ cbr cbr | peak [ average burst [ rt ] ] ] [oam seconds]
```

```
no atm pvc
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description From Interface Configuration or Subinterface Configuration mode, creates a PVC on an ATM interface. The **no** version removes the specified PVC.

From Profile Configuration mode, applies encapsulation, traffic-shaping, and OAM parameters to the range of PVCs configured on a static ATM AAL5 interface for use by a dynamic ATM 1483 subinterface. The **no** version restores the default service type, UBR, on the VC range.



NOTE: The optional *peak*, *average*, and *burst* parameters configure traffic-shaping parameters for the circuit. The allowable traffic-shaping features and range specifications depend on the line module capabilities.

- Options**
- *vcd*—Virtual circuit descriptor that is an identifier for the VC in other commands; in the range 1–2147483647
 - *vpi*—Virtual path identifier of this PVC. The allowable numeric range depends on the line module capabilities and current configuration. The VPI and VCI cannot both be set to 0; if one is 0, the other cannot be 0.
 - *vci*—Virtual circuit identifier of this PVC. The allowable numeric range depends on the line module capabilities and current configuration. The VPI and VCI cannot both be set to 0; if one is 0, the other cannot be 0.

- *encapsulation*—Available options differ for ATM interfaces and dynamic ATM 1483 subinterfaces, as follows:
 - For PVCs created on ATM interfaces:
 - *aal5all*—Causes the router to pass through all ATM AAL5 traffic without interpreting it; supported for ATM layer 2 services over MPLS
 - *aal0*—Causes the router to receive raw ATM cells on this circuit and forward the cells without performing AAL5 packet reassembly; supported for ATM layer 2 services over MPLS
 - *aal5snap*—LLC encapsulated circuit; LLC/SNAP header precedes the protocol datagram
 - *aal5mux ip*—VC-based multiplexed circuit used for IP only
 - *aal5autoconfig*—Enables autodetection of the 1483 encapsulation (LLC/SNAP or VC multiplexed)
 - *ilmi*—Integrated local management interface encapsulation
 - For PVCs created on dynamic ATM 1483 subinterfaces:
 - *aal5snap*—LLC encapsulated circuit; LLC/SNAP header precedes the protocol datagram
 - *aal5mux ip*—VC-based multiplexed circuit used for IP only
 - *aal5autoconfig*—Enables autodetection of the 1483 encapsulation (LLC/SNAP or VC multiplexed)
- *cbr*—Constant bit rate in Kbps
- *peak*—PCR in Kbps
- *average*—Average rate in Kbps; also referred to as SCR
- *burst*—Length in cells of the burst; also referred to as MBS
- *rt*—Selects VBR-RT as the service type; the default type is VBR-NRT. You can select **rt** only if you set the *peak*, *average*, and *burst* parameters.
- *oam*—Enables generation of OAM F5 loopback cells on this circuit. This option enables VC integrity features that affect the operational state of the ATM PVC. You can use the **oam** keyword only if you specify the **aal5snap**, **aal5autoconfig**, or **aal5mux ip** encapsulation type.
- *seconds*—Time interval in the range 1–600 seconds between transmissions of OAM F5 end-to-end loopback cells for VC connectivity verification.
- *inArp*—Enables Inverse ARP. You can use the **inArp** keyword only if you specify the **aal5snap** encapsulation type.
- *minutes*—Inverse ARP refresh rate in minutes; 15 minutes is the default
- *cc*—Enables CC cells on the PVC; you can enable CC cells only on data circuits, not on control circuits, such as ILMI or signaling circuits
- *segment*—Opens an OAM CC segment cell flow
- *end-to-end*—Opens an OAM CC end-to-end cell flow

- sink—Enables this VC as a sink point (cell receiver)
- source—Enables this VC as the source point (cell generator)
- both—Enables this VC as both a sink point and a source point

Mode Interface Configuration, Profile Configuration, Subinterface Configuration

Related Topics ■ *Configuring an MPLS Pseudowire with VCC Cell Relay Encapsulation, Configuring Local ATM Cross-Connects with AAL5 Encapsulation, and Configuring MPLS LSPs for L2VPNs in the JUNOS BGP and MPLS Configuration Guide*

atm shutdown

Syntax [no] atm shutdown

Release Information Command introduced before JUNOS Release 7.1.0.

Description Administratively disables an ATM interface. The **no** version enables a disabled interface.

Mode Interface Configuration

atm snmp trap link-status

Syntax [no] atm snmp trap link-status

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables SNMP link status traps on the ATM layer on a per-interface basis. The **no** version disables the traps.

Mode Interface Configuration

atm sonet stm-1

Syntax [no] atm sonet stm-1

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the mode of operation on the physical interface to SDH STM-1. The **no** version restores the default value, SONET STS-3c operation.

Mode Interface Configuration

atm uni-version

Syntax atm uni-version *versionNumber*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the UNI version the interface should use. There is no **no** version.

Options ■ *versionNumber*—UNI version number: 3.0, 3.1, or 4.0

Mode Interface Configuration

atm vc-per-vp

Syntax atm vc-per-vp [*vcCount*]
 no atm vc-per-vp

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the number of virtual circuits per virtual path. This command controls the VPI and VCI range on the ATM interface. The allowable configuration range depends on the line module. The router will not execute the command if any virtual circuits are open on the interface. The **no** version restores the default.



NOTE: This command is not available for ATM interfaces on the E120 router and the E320 router because they support the entire VPI/VCI range.

The minimum number of VCs per VP is 4096 for OC3-4 modules and 1024 for T3 ATM modules. If you enter a value that is below the minimum, the router uses the minimum value.

VCs and VP tunnels must not exist when you issue this command. If they do, you must delete the VC and VP tunnel configuration before you issue this command.

Options ■ *vcCount*—Number of virtual circuits per virtual path

Mode Interface Configuration

atm vp-description

Syntax atm vp-description *vpi description*
 no atm vp-description *vpi*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns a text description to an individual virtual path (VP) on an ATM interface. Use the show atm vp-description command to display the description. The **no** version restores the default value, a null string.

- Options** ■ *vpi*—Virtual path identifier number in the range 0–255
 ■ *description*—Text string or alias for the specified VPI; up to 32 characters

Mode Interface Configuration

atm-vp qos-parameter

Syntax atm-vp *vpi* qos-parameter *qosParameterInstanceName* *qosParameterInstanceValue*
 no atm-vp *vpi* qos-parameter *qosParameterInstanceName*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Attaches a QoS parameter instance to the specified VP on the ATM major interface. The **no** version detaches the parameter instance from the specified VP.

- Options**
- *vpi*—Virtual path identifier of this PVC; number in the range 0–255
 - *qosParameterInstanceName*—Name of the parameter instance that you want to attach to the VP
 - *qosParameterInstanceValue*—Number of the scheduler rate for the parameter instance; the default value is the minimum value defined in the parameter definition

Mode Interface Configuration

Related Topics ■ Creating Parameter Instances

atm-vp qos-profile

Syntax [no] atm-vp *vpi* qos-profile *qosProfileName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Attaches a QoS profile to the specified VP on the interface. The **no** version detaches the QoS profile from the VP.

- Options**
- *vpi*—Virtual path identifier of this PVC; number in the range 0–255
 - *qosProfileName*—Name of the QoS profile that you want to attach to the VP

Mode Interface Configuration

Related Topics

- Attaching a QoS Profile to an Interface

atm vp-tunnel

Syntax atm vp-tunnel *vpi* { cbr *kbps* | *kbps* }
 no atm vp-tunnel *vpi*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a virtual path tunnel and configures the rate of traffic flow within the tunnel. For QoS configurations, use to configure a shapeless VP tunnel. The **no** version removes the restriction.

- Options**
- *vpi*—Number in the range 0–255; virtual path identifier of this PVC
 - cbr—Specifies the service class as constant bit rate
 - *kbps*—Tunnel rate for a virtual path. The tunnel rate can be a value in the range 0–4294967295, when you specify the rate of traffic flow without the constant bit rate (CBR) service category, and can be a value in the range 1–4294967295, when you specify the rate of traffic flow with the CBR service class. Because the CBR service category guarantees a fixed amount of bandwidth to be allotted to the client, an error message is displayed if you configure a value of 0 for the tunnel rate for CBR traffic flows. The aggregate to this traffic from all circuits configured in the tunnel is held to the specified rate. Certain line modules may have minimum rates for VP tunnels. Using a rate of 0 configures a shapeless tunnel (a tunnel with no rate) that is used for VP shaping in the SAR.

Mode Interface Configuration

authentication

Syntax authentication { rsa-sig | pre-share }
no authentication

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the authentication method to use in the IKE policy. The **no** version restores the default, preshared keys.

- Options**
- rsa-sig—Specifies RSA signature as the authentication method
 - pre-share—Specifies preshared keys as the authentication method

Mode IKE Policy Configuration

authentication key

Syntax authentication key [0 | 8] *authkey*
no authentication key

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the password for text authentication and the key for MD5 authentication for RIP remote-neighbor interface. The **no** version clears the key for the interface. Supported only in RIP version 2. Authentication is disabled by default.

- Options**
- 0—Indicates the *authKey* is entered in unencrypted form (plaintext); this is the default option
 - 8—Indicates the *authKey* is entered in encrypted form (ciphertext)
 - *authkey*—Password sent with RIP messages or the key used to encrypt/decrypt RIP messages, depending on the authentication mode set for this remote-neighbor interface.

Mode Remote Neighbor Configuration

authentication-key

Syntax authentication-key [0 | 8] *authKey*
no authentication-key

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables simple password authentication and assigns a password used by OSPF remote neighbors. The **no** version deletes the password.

- Options**
- 0—Indicates the *authKey* is entered in unencrypted form (plaintext); this is the default option
 - 8—Indicates the *authKey* is entered in encrypted form (ciphertext)
 - *authKey*—Password; string of up to 8 characters

Mode Remote Neighbor Configuration

authentication message-digest

Syntax authentication message-digest

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that MD5 authentication is used for the OSPF remote-neighbor interface. There is no **no** version.

Mode Remote Neighbor Configuration

authentication mode

Syntax authentication mode { text | md5 *keyID* }
no authentication mode

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the type of authentication used on the RIP remote-neighbor interface. Authentication is disabled by default. The **no** version removes authentication from the interface. Supported only in RIP version 2.

- Options**
- text—Sends a simple text password with each RIP message; if the password is not possessed by remote neighbors, the message is rejected
 - md5—Encrypts and compresses the RIP message with MD5 message-digest algorithms
 - *keyID*—Number identifying the MD5 key in the range 1–255; remote neighbors must share the MD5 key to decrypt the message and encrypt the response

Mode Remote Neighbor Configuration

authentication-none

Syntax authentication-none

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that no authentication is to be used for the OSPF remote-neighbor interface. There is no **no** version.

Mode Remote Neighbor Configuration

authorization

Syntax `authorization { exec | commands level } authorListName`
 `no authorization {exec | commands level }`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables AAA authorization for a specified vty line or group of vty lines. Associates the authorization list with the specified line. If the list does not exist or is empty, authorization always succeeds. For a command to be authorized, its level must match exactly with the level of one of the configured lists. The **no** version disables authorization.

- Options**
- `exec`—Applies this authorization to CLI access in general
 - `commands`—Applies this authorization to user commands of the specified privilege level
 - `level`—Privilege level; a number in the range 0–15
 - `authorListName`—Name of an authorization method list of up to 32 characters; if no methods list is specified, the default is used

Mode Line Configuration

authorization change

Syntax [no] authorization change

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the router to receive change-of-authorization messages, such as packet mirroring attributes and Service Manager attributes, from the RADIUS server. The **no** version restores the default, in which support for RADIUS-initiated change-of-authorization messages is disabled on the router.

Mode RADIUS Configuration

Related Topics ■ Configuring RADIUS-Based Mirroring

auth-router-name

Syntax [no] auth-router-name [*routerName*]

Release Information Command introduced in JUNOS Release 9.0.0.

Description Assigns an access virtual router. The **no** version restores the default router.



NOTE: This command replaces the deprecated **router-name** command, which may be removed completely in a future release.

Options ■ *routerName*—Name of the virtual router; string of 1–32 alphanumeric characters

Mode Domain Map Configuration

auto-configure

Syntax `auto-configure upperInterfaceType [lockout-time { minValue maxValue | none }]`
 `no auto-configure upperInterfaceType [lockout-time]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the type(s) of dynamic encapsulations that are accepted or detected by the static ATM 1483 interface. Optionally, specifies the lockout time range for the encapsulation type. You can enter this command repeatedly in Subinterface Configuration mode. The **no** version terminates detection of the specified encapsulation type or, if the **lockout-time** keyword is specified, restores the lockout time range to its default values.



NOTE: Encapsulation type lockout is available for bridged Ethernet, IP, PPP, and PPPoE encapsulation types.

- Options**
- `upperInterfaceType`—One of the following dynamic encapsulation types:
 - `bridgedEthernet`
 - `ip`
 - `ppp`
 - `pppoe`
 - `minValue`—Minimum lockout time in the range 1–86400 seconds (24 hours); default value is 1 second
 - `maxValue`—Maximum lockout time in the range 1–86400 seconds (24 hours); default value is 300 seconds (5 minutes)
 - `none`—Disables lockout for the specified dynamic encapsulation type

Mode Interface Configuration, Subinterface Configuration

auto-configure atm1483

Syntax [no] auto-configure atm1483

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the static ATM AAL5 interface to support autodetection of an ATM 1483 dynamic encapsulation type. The **no** version terminates autodetection of the ATM 1483 encapsulation type.

Mode Interface Configuration

auto-configure vlan

Syntax [no] auto-configure vlan

Release Information Command introduced in JUNOS Release 7.1.0.

Description Configures the static VLAN major interface to support autodetection of a dynamic VLAN subinterface. The **no** version terminates autodetection of the VLAN subinterface.

Mode Interface Configuration

auto-cost reference-bandwidth

Syntax [no] auto-cost reference-bandwidth *refBw*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Controls how OSPFv3 calculates default metrics for the interface. The **no** version assigns cost based only on the interface type.

Options ■ *refBw*—Bandwidth in megabits per second in the range 1–4294967; default value is 100

Mode Router Configuration

automatic-virtual-link

Syntax [no] automatic-virtual-link

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables or disables automatic virtual link configuration. The **no** version disables an automatic virtual link.

Mode Router Configuration

auto-summary

Syntax [no] auto-summary

Release Information Command introduced before JUNOS Release 7.1.0.

Description Reenables the automatic summarization of routes redistributed into BGP to their natural network masks. Automatic summarization is enabled by default. The **no** version disables automatic summarization.

Mode Address Family Configuration, Router Configuration

average-length-exponent

Syntax average-length-exponent *exponent*
 no average-length-exponent

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the exponent used to weight the average queue length over time, controlling WRED responsiveness. The **no** version negates the average-length-exponent.

Options ■ *exponent*—Total average queue length (TAQL) coefficient

Mode Drop Profile Configuration

Related Topics ■ Configuring RED
 ■ Configuring WRED

avp

Syntax *avp avpType action*
 no avp avpType

Release Information Command introduced in JUNOS Release 7.2.0.

Description Configures the L2TP tunnel switching behavior for a specified L2TP AVP type. The **no** version restores the default L2TP tunnel switching behavior for AVPs of the specified type.

- Options** ■ *avpType*—One of the following L2TP AVPs
- *bearer-type*—L2TP Bearer Type AVP 18; by default, the router regenerates this AVP at the outbound LAC session, based on the local policy that is in effect
 - *calling-number*—L2TP Calling Number AVP 22; by default, the router regenerates this AVP at the outbound LAC session, based on the local policy that is in effect
 - *cisco-nas-port*—Cisco NAS Port Info AVP 100; by default, the router drops this AVP
- *action*—One of the following actions that characterize the tunnel switching behavior; currently, only the **relay** action is supported
- *relay*—Causes the router to preserve the value of an incoming AVP of the specified type when packets are switched between an inbound LNS session and an outbound LAC session

Mode L2TP Tunnel Switch Profile Configuration

Chapter 3

B Commands

backup-address-pool-name

Syntax backup-address-pool-name *poolName*
 no address-pool-name

Release Information Command introduced in JUNOS Release 10.0.0.

Description Specifies a backup local address pool name to associate with the domain name being configured. This pool is used to assign IP addresses to users, if the primary local pool has been fully allocated. The **no** version removes the backup pool name.



NOTE: You must configure a primary local address pool for the backup local address pool to take effect.

Options ■ *poolName*—Name of the backup pool to associate with the domain name; string of up to 16 alphanumeric characters

Mode Domain Map Configuration

Related Topics ■ *Configuring Local Address Servers* in the *JUNOS BGP and MPLS Configuration Guide*

bandwidth

Syntax `bandwidth bandwidth`

`no bandwidth`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the total bandwidth available on the interface. For total reservable bandwidth, see the **mpls bandwidth** command. The **no** version removes the admission control configuration from the interface.

Options ■ *bandwidth*—Available bandwidth in kilobits per second, a value from 1–10,000,000

Mode Interface Configuration, Subinterface Configuration

Related Topics `ospf bandwidth`

bandwidth oversubscription

Syntax [no] bandwidth oversubscription

Release Information Command introduced before JUNOS Release 7.1.0.

Description Allows the line modules to operate below line rate performance. The **no** version forces the line modules to operate at line rate performance.

Mode Privileged Exec

banner

Syntax banner [motd | login | exec] *bannerText*
 no banner [motd | login | exec]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures message-of-the-day, login, or exec banners to be displayed by the CLI. If you do not specify an option, the behavior is the same as if you specified the **motd** option. The **no** version deletes the banner.

- Options**
- motd—Displays the banner when a console or vty connection is initiated
 - login—Displays the banner before any user authentication (line or RADIUS authentication); the banner is also displayed if user authentication is not configured
 - exec—Displays the banner after user authentication (if any) and before the first prompt of a CLI session
 - *bannerText*—Alphanumeric string truncated at 1024 characters; delimited by the first character of the string, which must be repeated at the end of the string and must not occur anywhere else in the string

Mode Global Configuration

baseline aaa

Syntax baseline aaa

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for authentication and authorization statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline aaa route-download

Syntax baseline aaa route-download

Release Information Command introduced in JUNOS Release 8.1.0.

Description Sets a statistics baseline for route downloads. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline atm vp interface

Syntax baseline atm vp interface atm *interfaceSpecifier* *vpi*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Sets a statistics baseline for an ATM virtual path (VP) interface. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

- Options**
- *interfaceSpecifier*—ATM interface specifier; see Interface Types and Specifiers on page 5
 - *vpi*—Virtual path identifier of the PVC. The numeric range depends on the line module capabilities and current configuration.

Mode Privileged Exec

baseline bridge

Syntax baseline bridge { *bridgeGroupName* | *vplsName* }

Release Information Command introduced before JUNOS Release 7.1.0.
vplsName variable added in JUNOS Release 7.1.0.

Description Sets a statistics baseline for a bridge group or VPLS instance. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Options

- *bridgeGroupName*—Name of a bridge group specified with the **bridge** command
- *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command

Mode Privileged Exec

Related Topics

- *Setting a Baseline for VPLS Statistics* in the *JUNOS BGP and MPLS Configuration Guide*

baseline bridge interface

Syntax `baseline bridge interface interfaceType interfaceSpecifier`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for a specified network interface belonging to a bridge group or VPLS instance. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.



NOTE: Using the **baseline bridge interface** command for a VPLS instance affects the specified network interface associated with the VPLS instance, but has no effect on the VPLS virtual core interface, which represents all of the MPLS tunnels from the router to the remote VPLS edge (VE) devices. To set a statistics baseline for the VPLS virtual core interface, use the **baseline bridge interface vpls** command.

- Options**
- *interfaceType*—One of the following interface types listed in Interface Types and Specifiers on page 5
 - atm
 - fastEthernet
 - gigabitEthernet
 - tenGigabitEthernet
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec

Related Topics

- *Setting a Baseline for VPLS Statistics in the JUNOS BGP and MPLS Configuration Guide*

baseline bridge interface vpls

Syntax baseline bridge interface vpls *vplsName*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Sets a statistics baseline for a VPLS instance on the VPLS virtual core interface, which represents all of the MPLS tunnels from the router to the remote VPLS edge (VE) devices. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.



NOTE: Using the **baseline bridge interface vpls** command affects the VPLS virtual core interface, but has no effect on the network interfaces associated with the VPLS instance. To set a statistics baseline for a VPLS network interface, use the **baseline bridge interface** command.

Options ■ *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command

Mode Privileged Exec

Related Topics ■ *Setting a Baseline for VPLS Statistics* in the *JUNOS BGP and MPLS Configuration Guide*

baseline clns

Syntax `baseline clns [interfaceType interfaceSpecifier]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for CLNS. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

- Options** ■ *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec

baseline cops

Syntax baseline cops

Release Information Command introduced in JUNOS Release 7.1.0.

Description Sets a baseline for the Common Open Policy Service (COPS) statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline dhcp

Syntax baseline dhcp { server | relay }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for DHCP relay and DHCP relay proxy statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

- Options**
- server—Sets baseline for DHCP proxy server statistics
 - relay—Sets baseline for DHCP relay statistics

Mode Privileged Exec

Related Topics ■ Setting Baselines for DHCP Statistics

baseline frame-relay interface

Syntax baseline frame-relay interface *interfaceType interfaceSpecifier* [*dlci*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for Frame Relay and MLFR interfaces, subinterfaces, and circuits. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

- Options**
- *interfaceType*—One of the following interface types listed in Interface Types and Specifiers on page 5
 - mlframe-relay
 - pos
 - serial
 - tunnel
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *dlci*—DLCI number to be used on the specified subinterface to identify a virtual circuit in the range 16–1007

Mode Privileged Exec

baseline frame-relay multilinkinterface

Syntax baseline frame-relay multilinkinterface *interfaceType interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for MLFR links. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

- Options**
- *interfaceType*—One of the following interface types listed in Interface Types and Specifiers on page 5
 - serial
 - pos
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec

baseline hdlc interface

Syntax baseline hdlc interface *interfaceType* *interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for Cisco HDLC interfaces. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

- Options**
- *interfaceType*—One of the following interface types listed in Interface Types and Specifiers on page 5
 - pos
 - serial
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec

baseline interface

Syntax baseline interface *interfaceType interfaceSpecifier* [*vcd*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for an interface or a specific ATM virtual circuit. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

- Options**
- *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *vcd*—Virtual circuit descriptor; number in the range 1–4294967295; an identifier for the VC in other commands (ATM interfaces only)

Mode Privileged Exec

baseline ip

Syntax `baseline ip [vrf vrfName]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the baseline on general IP traffic statistics as the current value. There is no **no** version.

Options ■ *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters

Mode Privileged Exec

baseline ip bgp

Syntax baseline ip bgp

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the baseline on all BGP statistics as the current value. There is no **no** version.

Mode Privileged Exec

baseline ip dhcp-external

Syntax baseline ip dhcp-external

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a baseline for DHCP external server statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

Related Topics ■ Setting Baselines for DHCP Statistics

baseline ip dhcp-local

Syntax baseline ip dhcp-local [interface *interfaceType* *interfaceSpecifier*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a baseline for DHCP local server statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

- Options**
- *interfaceType*—One of the following interface types listed in Interface Types and Specifiers on page 5
 - atm
 - fastEthernet
 - gigabitEthernet
 - tenGigabitEthernet
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec

baseline ip dvmrp

Syntax baseline ip dvmrp

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a baseline for DVMRP statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline ip http

Syntax baseline ip http

Release Information Command introduced in JUNOS Release 7.2.0.

Description Sets a baseline for HTTP local server statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline ip igmp

Syntax baseline ip igmp

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a baseline for IGMP statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline ip igmp-proxy interface

Syntax baseline ip igmp-proxy interface

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the baseline on all IGMP statistics by setting the counters for the numbers of queries received and reports sent on the upstream interface to zero. There is no **no** version.

Mode Privileged Exec

baseline ip interface

Syntax `baseline ip interface [vrf vrfName] interfaceType interfaceSpecifier`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a baseline for IP interface statistics. There is no **no** version.

- Options**
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec

baseline ip mobile home-agent

Syntax baseline ip mobile home-agent

Release Information Command introduced in JUNOS Release 9.0.0.

Description Sets a statistics baseline for a specified Mobile IP home agent for control traffic. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline ip nat

Syntax baseline ip nat

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a baseline for NAT statistics and counters. There is no **no** version.

Mode Privileged Exec

baseline ip ospf

Syntax baseline ip ospf

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a baseline for OSPF statistics and counters. There is no **no** version.

Mode Privileged Exec

baseline ip rip

Syntax baseline ip rip

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for RIP interfaces. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline ip tunnel-reassembly

Syntax baseline ip tunnel-reassembly

Release Information Command introduced in JUNOS Release 8.0.0.

Description Sets a statistics baseline for tunnel reassembly statistics on the current virtual router. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever you retrieve baseline-relative statistics. There is no **no** version.

Mode Privileged Exec

baseline ip udp

Syntax baseline ip udp [vrf *vrfName*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for UDP statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Options ■ *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters

Mode Privileged Exec

baseline ip vrrp

Syntax baseline ip vrrp

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for VRRP statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline ipv6

Syntax baseline ipv6 [udp]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the baseline on general IPv6 traffic statistics as the current value. Use the **udp** keyword to set a baseline for UDP statistics. There is no **no** version.

Options ■ udp—Sets a baseline for UDP statistics

Mode Privileged Exec

baseline ipv6 dhcpv6-local

Syntax baseline ipv6 dhcpv6-local

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a baseline for DHCPv6 local server statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

Related Topics ■ Setting Baselines for DHCP Statistics

baseline ipv6 interface

Syntax `baseline ipv6 interface interfaceType interfaceSpecifier`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a baseline for IPv6 interface statistics. There is no **no** version.

- Options**
- *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec

baseline ipv6 local pool

Syntax baseline ipv6 local pool

Release Information Command introduced in JUNOS Release 10.1.0.

Description Sets a baseline for the IPv6 local pool prefix assignment statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec, User Exec

baseline ipv6 mld

Syntax baseline ipv6 mld

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a baseline for MLD statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline ipv6 mld-proxy interface

Syntax baseline ipv6 mld-proxy interface

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the baseline on all MLD statistics by setting the counters for the numbers of queries received and reports sent on the upstream interface to zero. There is no **no** version.

Mode Privileged Exec

baseline ipv6 ospf

Syntax `baseline ipv6 ospf [processId]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a baseline for OSPFv3 statistics and counters. There is no **no** version.

Options ■ *processId*—Integer in the range 1–65535

Mode Privileged Exec

baseline ipv6 tcp

Syntax `baseline ipv6 tcp [vrf vrfName] [localAddress localPort remoteAddress remotePort]`

Release Information Command introduced before JUNOS Release 7.1.0.
ip keyword removed and **ipv6** keyword added in JUNOS Release 7.2.0.

Description Sets a statistics baseline for only IPv6 TCP statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

- Options**
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
 - *localAddress*—Local IPv6 address on the router
 - *localPort*—Local TCP port number on the router
 - *remoteAddress*—IPv6 address of remote router
 - *remotePort*—TCP port number on remote router

Mode Privileged Exec

baseline line interface sonet

Syntax baseline line interface sonet *interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for SONET/SDH statistics at the line layer. The router implements the baseline by reading and storing the MIB statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Options ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec

baseline local pool

Syntax baseline local pool

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for the router local address pool statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline log

Syntax baseline log [last-reset | *time* [*utc*] *month day year*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a baseline for logging events. To use the current system time, do not enter any options. There is no **no** version.

- Options**
- *last-reset*—Causes the router to display log messages generated since the last time the router was reset
 - *time*—Time and date after which the router displays messages that are timestamped. To set the time, use the following syntax:
Hour:Minute[:Second]—Current time in 24-hour format; seconds are optional
 - *utc*—Indicates that the time entered is UTC (GMT) time; if you do not include this keyword, the router considers the time entered to be local time
 - *month*—Name of the month in English
 - *day*—Number of the day in the range 1–31
 - *year*—Four-digit number of the year

Mode Privileged Exec

baseline mpls interface

Syntax baseline mpls interface *interfaceName*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Sets a statistics baseline for the specified MPLS major interface or MPLS shim interface. By default, the interface counters are baselined at zero. There is no **no** version.

Options ■ *interfaceName*—Name of interface; up to 15 alphanumeric characters

Mode Privileged Exec

Related Topics ■ *Setting Baselines for Layer 2 Services over MPLS* in the *JUNOS BGP and MPLS Configuration Guide*

baseline mpls label

Syntax baseline mpls label { interface *interfaceName* atm *vpi vci* | *labelValue* }

Release Information Command introduced in JUNOS Release 7.1.0.

Description Sets a statistics baseline for the specified MPLS in label. Statistics for an in label must be enabled with the **mpls statistics label** command before they can be baselined. By default, the in-label counters are baselined at zero. There is no **no** version.

- Options**
- *interfaceName*—Name of interface for label in interface label space on an ATM AAL5 interface; up to 15 alphanumeric characters
 - *vpi*—Virtual path identifier for a label, a value in the range 0–255
 - *vci*—Virtual circuit identifier for a label, a value in the range 33–65535
 - *labelValue*—Integer identifying a label in the platform label space, a value in the range 16–1048575

Mode Privileged Exec

baseline mpls next-hop

Syntax baseline mpls next-hop *nextHopIndex*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Sets a statistics baseline for the specified MPLS next hop. Statistics for a next hop must be enabled with the **mpls statistics next-hop** command before they can be baselined. By default, the next-hop counters are baselined at zero. There is no **no** version.

Options ■ *nextHopIndex*—Number identifying a next hop; displayed by the **show mpls forwarding** command

Mode Privileged Exec

baseline mpls tunnel

Syntax `baseline mpls tunnel tunnelName`

Release Information Command introduced in JUNOS Release 7.1.0.

Description Sets a statistics baseline for the specified MPLS tunnel. Statistics for a tunnel must be enabled with the **mpls statistics policy** command before they can be baselined. By default, the next-hop counters are baselined at zero. There is no **no** version.

Options ■ *tunnelName*—Name identifying a tunnel; displayed by the **show mpls tunnels** command

Mode Privileged Exec

baseline path interface sonet

Syntax baseline path interface sonet *interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for SONET/SDH statistics at the path layer. The router implements the baseline by reading and storing the MIB statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Options ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec

baseline ppp interface

Syntax baseline ppp interface { atm | fastEthernet | gigabitEthernet | serial | mlppp | pos } *interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.
fastEthernet and **gigabitEthernet** keywords added in JUNOS Release 11.0.0

Description Sets a statistics baseline for PPP interfaces. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

- Options**
- atm—Specifies an ATM interface
 - fastEthernet—Specifies a Fast Ethernet interface
 - gigabitEthernet—Specifies a Gigabit Ethernet interface
 - mlppp—Specifies an MLPPP interface
 - pos—Specifies a POS interface
 - serial—Specifies a serial interface
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec

baseline pppoe interface

Syntax baseline pppoe interface *interfaceType interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for PPPoE interfaces, subinterfaces, and/or circuits. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

- Options**
- *interfaceType*—One of the following interface types listed in Interface Types and Specifiers on page 5
 - atm
 - fastEthernet
 - gigabitEthernet
 - lag
 - serial—PPPoE is not currently supported on serial interfaces
 - tenGigabitEthernet
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec

baseline radius

Syntax baseline radius

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for RADIUS statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline radius dynamic-request

Syntax baseline radius dynamic-request

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for RADIUS dynamic-request statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

Related Topics ■ Monitoring Packet Mirroring Overview

baseline radius relay

Syntax baseline radius relay

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a baseline for RADIUS relay statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline section interface sonet

Syntax baseline section interface sonet *interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a statistics baseline for SONET/SDH statistics at the section layer. The router implements the baseline by reading and storing the MIB statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Options ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec

baseline show-delta-counts

Syntax [no] baseline show-delta-counts

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the router to always display the statistics relative to the most recent appropriate baseline. The **no** version removes the configuration.

Mode Global Configuration

baseline snmp

Syntax baseline snmp

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a baseline for SNMP statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline ssc

Syntax baseline ssc

Release Information Command introduced in JUNOS Release 7.1.0.

Description Sets a baseline for the SRC statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline suspicious-control-flow-detection counts

Syntax baseline suspicious-control-flow-detection counts

Release Information Command introduced in JUNOS Release 7.3.0.

Description Sets a baseline for statistics for suspicious control flow detection. There is no **no** version.

Mode Privileged Exec, User Exec

baseline tacacs

Syntax baseline tacacs

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a baseline for TACACS+ statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

Mode Privileged Exec

baseline tcp

Syntax `baseline [ip | ipv6] tcp [vrf vrfName] [localAddress localPort remoteAddress remotePort]`

Release Information Command introduced in JUNOS Release 7.2.0.
ip keyword made optional in JUNOS Release 7.2.0.
ipv6 keyword added in JUNOS Release 7.2.0.

Description Sets a baseline for all TCP statistics or for only IPv4 or IPv6 TCP statistics. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved. There is no **no** version.

- Options**
- **ip**—Implements a baseline for only IPv4 statistics
 - **ipv6**—Implement a baseline for only IPv6 statistics
 - **vrfName**—Name of the VRF; string of 1–32 alphanumeric characters
 - **localAddress**—Local IP or IPv6 address on the router
 - **localPort**—Local TCP port number on the router
 - **remoteAddress**—IP or IPv6 address of remote router
 - **remotePort**—TCP port number on remote router

Mode Privileged Exec

bert

Syntax bert pattern *pattern* interval *time* [unframed]
no bert

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables bit error rate tests using the specified pattern on T3 interfaces on channelized and unchannelized T3 modules. The **no** version stops the test that is running.



NOTE: The BERT patterns supported can vary depending on the line module and I/O module assembly you are using.

- Options**
- *pattern*—One of the following test patterns:
 - 0s—Repetitive test pattern of all zeros, 00000...
 - 1s—Repetitive test pattern of all ones, 11111...
 - 2^9—Pseudorandom test pattern, 511 bits in length
 - 2^11—Pseudorandom test pattern, 2047 bits in length
 - 2^15—Pseudorandom test pattern, 32,767 bits in length
 - 2^20-O153—Pseudorandom test pattern, 1,048,575 bits in length
 - 2^20-QRSS—Pseudorandom QRSS test pattern, 1,048,575 bits in length
 - 2^23—Pseudorandom test pattern, 8,388,607 bits in length
 - alt-0-1—Repetitive alternating test pattern of zeros and ones, 01010101...
 - *time*—Duration of the test in the range 1–1440 minutes
 - unframed—(available for E1 and T1 interfaces only) if specified, the test bit pattern occupies all bits on the link, overwriting the framing bits; if not specified, the test bit pattern occupies only the payload bits

Mode Controller Configuration

bfd adapt

Syntax [no] bfd adapt

Release Information Command introduced in JUNOS Release 7.3.0.

Description Enables all BFD sessions to adapt timer intervals on all virtual routers on the router. The **no** version disables subsequent BFD sessions from adapting timer intervals without resetting any already adapted intervals.

Mode Global Configuration

bgp advertise-best-external-to-internal

Syntax [no] bgp advertise-best-external-to-internal

Release Information Command introduced before JUNOS Release 7.1.0.

Description Causes the BGP selection process to select two best routes to every destination. BGP advertises to external peers the best route selected from the complete set of routes known to that destination. BGP advertises to internal peers the best route from the set of routes received from external and confederation peers. The **no** version restores the default condition, wherein BGP selects only one best route for each destination from the complete set of routes; if the best route was received from an internal peer, BGP does not advertise any route to that destination to the internal peers.

Mode Router Configuration

bgp advertise-inactive

Syntax [no] bgp advertise-inactive

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the advertisement of inactive BGP received routes—routes that are considered by BGP to be “best routes” and therefore are present in the IP forwarding table, but that are *not* being used for forwarding. The **no** version restores the default state of normal route advertisement, whereby BGP advertises received routes only if they are in the IP forwarding table and are being used to forward traffic, or if synchronization is enabled.

Mode Router Configuration

bgp always-compare-med

Syntax [no] bgp always-compare-med

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the comparison of the MED for paths from neighbors in different ASs. The **no** version disables the feature.

Mode Router Configuration

bgp bestpath med confed

Syntax [no] bgp bestpath med confed

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that BGP considers the MED when comparing routes originated from different sub-ASs within the confederation to which this BGP speaker belongs. The **no** version restores the default state, where the MED attribute is not considered.

Mode Router Configuration

bgp bestpath missing-as-worst

Syntax [no] bgp bestpath missing-as-worst

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that a route with a MED is always considered to be better than a route without a MED by causing the missing MED attribute to have a value of infinity. The **no** version restores the default state, where the missing MED attribute is considered to have a value of zero.

Mode Router Configuration

bgp client-to-client reflection

Syntax [no] bgp client-to-client reflection

Release Information Command introduced before JUNOS Release 7.1.0.

Description Restores route reflection from a BGP route reflector to clients. The **no** version disables client-to-client reflection. By default, BGP reflects routes received from any route reflector client to all other route reflector clients. This command can be used to disable or restore this behavior.

Mode Router Configuration

bgp cluster-id

Syntax `bgp cluster-id { clusterId | ipAddress }`
 `no bgp cluster-id [clusterId | ipAddress]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures a cluster ID if the BGP cluster has more than one route reflector. The **no** version causes BGP to use the router ID as the cluster ID.

- Options** ■ *clusterId*—Number in the range 0–4294967295; the cluster ID of this router acting as a route reflector
- *ipAddress*—Cluster ID of this router acting as a route reflector specified as an IP address

Mode Router Configuration

bgp confederation identifier

Syntax `bgp confederation identifier autonomousSystem`
 `no bgp confederation identifier [autonomousSystem]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures a BGP confederation identifier. The **no** version removes a BGP confederation identifier.

Options ■ *autonomousSystem*—Number in the range 1–4294967295; the confederation identifier

Mode Router Configuration

bgp confederation peers

Syntax `bgp confederation peers { autonomousSystem [autonomousSystem]* |
filter-list filterListName }`

`no bgp confederation peers [autonomousSystem [autonomousSystem]* |
filter-list filterListName]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the sub-ASs that belong to a confederation by listing individual AS numbers or by reference to an AS-path access list (the filter list). If the remote AS of a peer appears in the list of sub-AS numbers or in the filter list, then the peer is considered to be in the same confederation. The **no** version removes individually specified sub-ASs, all sub-ASs specified by the filter list, or all sub-ASs from the confederation.

- Options**
- *autonomousSystem*—AS number in the range 1–4294967295
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line
 - *filterListName*—Name of an AS-path access list; a string of up to 32 characters

Mode Router Configuration

bgp dampening

Syntax [no] bgp dampening [*halfLife* [*reuse suppress maxSuppressTime*
[*halfLifeUnreachable*]]] [route-map *mapTag*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables BGP route dampening. The router assesses a penalty of 1000 each time a route flaps and adds this to any previously accumulated penalty value. Penalties are cumulative. The **no** version disables route flap dampening.

- Options**
- *halfLife*—Half-life period in minutes in the range 1–45; default value is 15. When a BGP route has been assigned a penalty, the penalty is decreased by half after the half-life period.
 - *reuse*—Reuse limit in the range 1–20000; default value is 750. As the penalty for a flapping route decreases and falls below this reuse limit, the route is unsuppressed. That is, the route is added back to the BGP table and used for forwarding.
 - *suppress*—Suppress limit in the range 1–20000; default value is 2000. A route is suppressed when its penalty exceeds this limit.
 - *maxSuppressTime*—Maximum suppression time in minutes in the range 1–255. This value is the maximum amount of time a route can be suppressed. The default value is four times the half-life value.
 - *halfLifeUnreachable*—Alternate half-life period in minutes for unreachable routes; a number in the range 1–45. If this value is not specified, the same half-life period is used for both reachable and unreachable routes.
 - *route-map*—Specifies that dampening can be applied to routes according to the route map behavior. If the route map *permits* a route, the route is subject to dampening. If the route map *denies* a route, the route is not subject to dampening. The route map can contain a *no dampening* clause that determines dampening characteristics.
 - *mapTag*—Name of the route map; a string of up to 32 alphanumeric characters.

Mode Address Family Configuration, Router Configuration

bgp default ipv4-unicast

Syntax [no] bgp default ipv4-unicast

Release Information Command introduced before JUNOS Release 7.1.0.

Description Causes all neighbors subsequently created with the neighbor remote-as or neighbor peer-group commands to be automatically activated in the IPv4 unicast address family. The **no** version disables the IPv4 unicast address family on all neighbors.

Mode Address Family Configuration, Router Configuration

bgp default local-preference

Syntax `bgp default local-preference value`
 `no bgp default local-preference [value]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Changes the default local preference value. Generally, the default value of 100 allows you to easily define a particular path as less preferable than paths with no local preference attribute. The preference is sent to all routers in the local AS. The preferred path is the one with the highest preference value. The **no** version restores the default setting.

Options ■ *value*—Local preference number in the range 0–4294967295

Mode Router Configuration

bgp default route-target filter

Syntax [no] bgp default route-target filter

Release Information Command introduced before JUNOS Release 7.1.0.

Description Controls whether incoming BGP routes are filtered according to membership in route-target communities. Automatic filtering is enabled by default. The **no** version disables automatic filtering.

Mode Router Configuration

bgp enforce-first-as

Syntax [no] bgp enforce-first-as

Release Information Command introduced before JUNOS Release 7.1.0.

Description Forces BGP to compare the configured remote AS number of an external peer with the first AS in the AS path of routes received from the peer. If the AS numbers do not match, BGP sends the peer an error message. The **no** version restores the default condition, which does not perform the AS comparison.

Mode Router Configuration

bgp fast-external-fallover

Syntax [no] bgp fast-external-fallover

Release Information Command introduced before JUNOS Release 7.1.0.

Description Automatically brings down a BGP session to any adjacent external peer immediately after the link fails (as opposed to waiting for the TCP connection to fail or the hold timer to expire). The **no** version disables automatic session termination.

Mode Router Configuration

bgp graceful-restart

Syntax [no | default] bgp graceful-restart

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the BGP graceful restart capability globally, which enables BGP to maintain its forwarding state during a peer restart, avoiding network-wide route flaps and interruptions in traffic forwarding. Graceful restart is disabled by default. The **default** version restores the default condition, wherein graceful restart is disabled, and consequently, advertisement of the BGP graceful restart capability is stopped. The **no** version disables the graceful restart capability.



NOTE: The E Series router supports graceful restart, both as a receiving peer and a restarting peer.

Mode Router Configuration

bgp graceful-restart path-selection-defer-time-limit

Syntax `bgp graceful-restart path-selection-defer-time-limit seconds`
`no bgp graceful-restart path-selection-defer-time-limit [seconds]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the maximum time period after a peer session restart during which the best-path selection process is deferred. The period is measured from when the session is detected in a down state. The **no** version restores the default value, 360 seconds.

Options ■ *seconds*—Integer in the range 1–3600; default value is 600 seconds

Mode Router Configuration

bgp graceful-restart restart-time

Syntax `bgp graceful-restart restart-time seconds`
`no bgp graceful-restart restart-time [seconds]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the time period advertised to all peers during which a restart is expected to be complete on this BGP speaker. If the speaker does not reestablish peering sessions within this period, the peers flush all routes from this speaker that they marked as stale when the speaker restarted and the sessions went down. The **no** version restores the default value, 120 seconds.

Options ■ *seconds*—Integer in the range 1–3600; default value is 120 seconds

Mode Router Configuration

bgp graceful-restart stalepaths-time

Syntax `bgp graceful-restart stalepaths-time seconds`
`no bgp graceful-restart stalepaths-time [seconds]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the time period after a peer session restart for all peers during which BGP waits for an End-of-RIB marker from a peer before flushing all stale routes from that peer. The period is measured from when the session is detected in a down state. The **no** version restores the default value, 360 seconds.

Options ■ *seconds*—Integer in the range 1–3600; default value is 360 seconds

Mode Router Configuration

bgp log-neighbor-changes

Syntax [no] bgp log-neighbor-changes

Release Information Command introduced before JUNOS Release 7.1.0.

Description Causes BGP to log a message of severity notice to the bgpNeighborChanges log whenever a peer enters or leaves the Established state for any reason. No other messages are logged to the bgpNeighborChanges log. The **no** version disables this log.

Mode Router Configuration

bgp maxas-limit

Syntax `bgp maxas-limit limit`
 `no bgp maxas-limit [limit]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Causes BGP to check the length of AS paths received in update messages and to not forward routes whose AS paths are greater than the specified length. The **no** version halts checking of the AS path length.

Options ■ *limit*—Maximum acceptable length of a received AS path; number in the range 1–1000

Mode Router Configuration

bgp redistribute-internal

Syntax [no] bgp redistribute-internal

Release Information Command introduced before JUNOS Release 7.1.0.

Description Authorizes redistribution of internal BGP routes (in addition to external BGP routes) into protocols that have BGP route redistribution enabled. This command is not required for IBGP routes within a VRF, for which redistribution is always enabled. The **no** version restores the default, redistributing only external BGP routes.

Mode Router Configuration

bgp router-id

Syntax `bgp router-id ipAddress`
 `no bgp router-id [ipAddress]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the BGP identifier. The **no** version restores the router ID as the identifier.

Options ■ *ipAddress*—IP address to be used as the BGP identifier; ignored if present in the **no** version

Mode Router Configuration

bgp shutdown

Syntax [no] bgp shutdown

Release Information Command introduced before JUNOS Release 7.1.0.

Description Administratively disables BGP. The **no** version reenables BGP.

Mode Router Configuration

bgp wait-on-end-of-rib

Syntax `bgp wait-on-end-of-rib seconds`
`no bgp wait-on-end-of-rib`

Release Information Command introduced in JUNOS Release 8.2.0.

Description Specifies how long BGP waits to receive an End-of-RIB marker sent by route-target address family peers to signal the peer has finished advertising route-target membership information. Applies to all peers in the route-target address family. The **no** version restores the default value.

Options ■ *seconds*—Number of seconds BGP wait for End-of-RIB marker, in the range 1–3600; default is 60 seconds

Mode Address Family Configuration, Router Configuration

boolean-test

Syntax `boolean-test { comparison comparisonType | event eventOwner eventName
| startup |
value booleanValue }`

`no boolean-test [comparison | event | startup | value]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines Boolean test values for the trigger that you are configuring, including comparison settings, a Boolean value, a startup condition, and binding an event to the boolean-test trigger. The **no** version deletes the Boolean-test values for this trigger or removes either the startup condition or event binding.

- Options**
- *comparisonType*—One of the following types of Boolean comparison to perform: (equal, greater, greaterOrEqual, less, lessOrEqual, unequal)
 - *eventOwner*—Name of event owner that partially specifies event to trigger the Boolean test; string of up to 32 alphanumeric characters
 - *eventName*—Name of event that partially specifies event to trigger the Boolean test; string of up to 32 alphanumeric characters
 - *startup*—Specifies not to perform the Boolean comparison when this trigger first becomes active
 - *booleanValue*—Value in the range -2147483648–2147483647 to use for the Boolean test

Mode SNMP Trigger Configuration

boot backup

Syntax `boot backup relFilename { cnfFilename | scrFilename | factory-defaults }`
 `no boot backup`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the release and the configuration to be used the next (and every subsequent) time the boot logic chooses backup mode. The **no** version removes the setting.

- Options**
- *relFilename*—System software file
 - *cnfFilename*—Name of an existing configuration file (.cnf)
 - *scrFilename*—Name of an existing script file (.scr)
 - *factory-defaults*—Specifies that the router reverts to factory default configuration when rebooted

Mode Global Configuration

boot config

Syntax boot config { *cnfFilename* [once] | *scrFilename* | running-configuration | startup-configuration | factory-defaults }

no boot config

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies how the router obtains its startup configuration. The **no** version clears a previous request to reboot in a specified manner; the next reboot uses the configuration saved in nonvolatile storage.



CAUTION: All **boot config** commands except for **boot config running-configuration** and **boot config startup-configuration** erase the existing running configuration when you reboot the router. Before executing this command, you might want to save the current configuration to a .cnf file using the **copy running-configuration** command.

- Options**
- *cnfFilename*—Name of an existing startup configuration file (.cnf) to be used on all subsequent reboots
 - once—Restores a configuration from the specified configuration file only on the next reboot. Subsequent reboots revert to the running-configuration settings.
 - *scrFilename*—Name of an existing script file (.scr)
 - running-configuration—Specifies that the running configuration is to be used for reboot; only available if the router is in Automatic Commit mode
 - startup-configuration—Specifies that the running configuration is to be used for reboot; only available if the router is in Manual Commit mode
 - factory-defaults—Specifies that the factory default configuration is to be used for the next reboot. Subsequent reboots revert to the running-configuration settings.

Mode Global Configuration

boot force-backup

Syntax [no] boot force-backup

Release Information Command introduced before JUNOS Release 7.1.0.

Description Forces the router to use the backup software release file or router configuration file on the next boot. The **no** version sets the router to use the default release or configuration file on the next boot.



NOTE: After the router has used the backup settings, the **no boot force-backup** command is the only way to get the router to use the default settings again.

Mode Global Configuration

boot hotfix

Syntax `boot hotfix hfixFilename`
 `no boot hotfix { hfixFilename | all-releases }`

Release Information Command introduced in JUNOS Release 7.2.0.

Description Arms the specified hotfix as a startup hotfix that is automatically activated during system initialization when the SRP module is reloaded. The **no** version disarms the specified armed hotfix or all armed hotfixes.



NOTE: See also the `no boot hotfix all-releases` command.

- Options** ■ *hfixFileName*—Name of a hotfix software file (.hfx) on the local file system
 ■ all-releases—Disarms all hotfixes currently armed for the armed release

Mode Global Configuration

boot revert-tolerance

Syntax `boot revert-tolerance count time`
`no boot revert-tolerance`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the reversion tolerances that the boot logic uses to determine whether the router should use the normal or backup settings. Issuing this command when high availability is enabled results in the system cold-restarting the router and using the backup settings if the tolerance settings are met. The **no** version restores the default reversion tolerance settings. The default settings are 3 crashes in 30 minutes.

- Options**
- *count*—Number of times the operational SRP software crashes; in the range 0–4294967295; default value is 3
 - *time*—Time in the range 0–4294967295 seconds in which the set number (count) of crashes occurs; the default setting is 1800

Mode Global Configuration

boot revert-tolerance never

Syntax boot revert-tolerance never

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the boot logic to never revert to the backup release or configuration. There is no **no** version.

Mode Global Configuration

boot subsystem

Syntax `boot [backup] subsystem subsysName relFileName`
 `no boot [backup] subsystem [subsysName]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the selected subsystem to use the specified release the next time the subsystem is booted. The **no** version disables the subsystem. The **backup** option enables you to specify a backup release for the module in the specified slot in case the module reboots more times than allowed within the period specified by the **boot revert-tolerance** command.

- Options**
- `backup`—Configures a backup setting
 - `subsysName`—Name of the subsystem to be configured
 - `relFileName`—Name of system software file to use

Mode Global Configuration

boot system

Syntax boot system *relFileName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the software release (.rel) file to use on reboot. There is no **no** version.



NOTE: In a dual SRP module configuration, when this information is synchronized to the standby SRP module, the standby SRP module is reloaded to boot the specified release. The high availability feature requires the release to be the same on the active and the standby SRP modules. This means that arming the system to boot with a different release causes the standby module to reload and prevent high availability from becoming active or to disable high availability if it is active or pending.

Options ■ *relFileName*—Name of the software release file (.rel) that contains the software release

Mode Global Configuration

bridge1483 dos-protection-group

Syntax bridge1483 dos-protection-group *groupName*
 no bridge1483 dos-protection-group

Release Information Command introduced in JUNOS Release 8.1.0.

Description Attaches a bridge 1483 denial of service (DoS) protection group to an interface. The **no** version removes the attachment of the DoS protection group from the interface.

Options ■ *groupName*—Name of the DoS protection group; string of up to 31 alphanumeric characters

Mode Interface Configuration

bridge1483 mtu

Syntax bridge1483 mtu *mtuSize*
 no bridge1483 mtu

Release Information Command introduced in JUNOS Release 7.3.0.

Description Sets the maximum allowable size, in bytes, of the maximum transmission unit (MTU) for bridged Ethernet interfaces. The **no** version restores the default MTU size for bridged Ethernet interfaces, 1518 bytes.

Options ■ *mtuSize*—Maximum allowable size of the MTU, in the range 64–9180 bytes; default value is 1518

Mode Profile Configuration, Subinterface Configuration

bridge1483 service-profile

Syntax [no] bridge1483 service-profile *profileName*

Release Information Command introduced in JUNOS Release 9.0.0.

Description Assigns the specified IP service profile to the interface profile from which a dynamic bridged Ethernet interface is created. The IP service profile must be defined in the default virtual router. The **no** version removes the IP service profile assignment from the interface profile.

Options ■ *profileName*—Name of the IP service profile; maximum of 32 alphanumeric characters

Mode Profile Configuration

bridge

Syntax [no] bridge *bridgeGroupName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates a bridge group to use for transparent bridging. A bridge group is a named collection of network interfaces (ports) on an E Series router that forms a broadcast domain. Each bridge group has its own set of forwarding tables and filters and, as such, functions as a logical bridging device. The **no** version removes the bridge group configuration from the router.

To configure an existing bridge group as a VPLS instance, you must use the **bridge vpls transport-virtual-router** command.



NOTE: Do not assign the bridge group the same name as an existing virtual router configured on the router.

Options ■ *bridgeGroupName*—Name of the bridge group; string of up to 32 alphanumeric characters

Mode Global Configuration

bridge acquire

Syntax [no] bridge { *bridgeGroupName* | *vplsName* } acquire

Release Information Command introduced before JUNOS Release 7.1.0.
vplsName variable added in JUNOS Release 7.1.0.

Description Configures a bridge group or VPLS instance to acquire dynamically learned MAC addresses. Issuing this command enables the router to forward any frames it receives for nodes (stations) whose addresses it has learned dynamically. The **no** version prevents the router or VPLS instance from acquiring dynamically learned MAC addresses, and limits forwarding only to those nodes that have a statically configured address entry in the forwarding table.

To configure the maximum number of MAC addresses that the router can learn, use the **bridge learn** command (for a bridge group or VPLS instance) or the **bridge-group learn** command (for a network interface associated with a bridge group or VPLS instance).

Options

- *bridgeGroupName*—Name of a bridge group specified with the **bridge** command
- *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command

Mode Global Configuration

Related Topics

- *Configuring Optional Attributes for VPLS Instances in the JUNOS BGP and MPLS Configuration Guide*

bridge address

Syntax `bridge { bridgeGroupName | vplsName } address macAddress`
`{ forward interfaceType interfaceSpecifier | discard }`

`no bridge { bridgeGroupName | vplsName } address macAddress`

Release Information Command introduced before JUNOS Release 7.1.0.
vplsName variable added in JUNOS Release 7.1.0.

Description Enables a bridge group or VPLS instance to filter (forward or discard) frames based on their MAC address. Use this command to filter frames by a specific MAC address and to add a static (nonlearned) entry to the forwarding table. The **no** version removes the static MAC address entry from the forwarding table.



NOTE: For a VPLS instance, you cannot create a static (nonlearned) MAC address entry to forward to the VPLS virtual core interface.

- Options**
- *bridgeGroupName*—Name of a bridge group specified with the **bridge** command
 - *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command
 - *macAddress*—Unique 48-bit (6-byte) number that is programmed into each LAN network interface card (NIC) at the time of manufacture; also known as a hardware address or physical address. The MAC address format is a dotted triple of four-digit hexadecimal numbers; for example, 0090.1a40.4c7c
 - **forward**—Forwards frames destined for the specified MAC address out the specified network interface
 - *interfaceType*—One of the following interface types listed in “Interface Types and Specifiers” on page 5
 - atm
 - fastEthernet
 - gigabitEthernet
 - tenGigabitEthernet
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - **discard**—Discards (drops) frames sent from or destined for the specified MAC address without further processing

Mode Global Configuration

Related Topics ■ *Configuring Optional Attributes for VPLS Instances in the JUNOS BGP and MPLS Configuration Guide*

bridge aging-time

Syntax bridge { *bridgeGroupName* | *vplsName* } aging-time *seconds*
 no bridge { *bridgeGroupName* | *vplsName* } aging-time

Release Information Command introduced before JUNOS Release 7.1.0.
 vplsName variable added in JUNOS Release 7.1.0.

Description Sets the aging time of a dynamic (learned) entry in the forwarding table of a bridge group or VPLS instance. The aging time is the length of time, in seconds, that an entry can remain in the forwarding table. An entry expires from the forwarding table when it reaches the specified aging time. The **no** version restores the default value, 300 seconds.

- Options** ■ *bridgeGroupName*—Name of a bridge group specified with the **bridge** command
- *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command
- *seconds*—Aging time in the range 10–1000000 seconds

Mode Global Configuration

Related Topics ■ *Configuring Optional Attributes for VPLS Instances in the JUNOS BGP and MPLS Configuration Guide*

bridge crb

Syntax [no] bridge crb

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables concurrent routing and bridging (CRB) for all bridge groups configured on the router except those bridge groups configured as VPLS instances. When CRB is enabled, the router can route a protocol among a group of interfaces in one bridge group and concurrently bridge the same protocol among a separate group of interfaces in a different bridge group on the router. The **no** version disables CRB on all bridge groups and restores the default bridging capability.

The command takes effect for all bridge groups on the router not configured as VPLS instances; you cannot enable CRB for some bridge groups but not for others.

Mode Global Configuration

bridge-group

Syntax `bridge-group { bridgeGroupName | vplsName }
[subscriber-trunk | snmp-trap link-status | learn addressCount]`

`no bridge-group { bridgeGroupName | vplsName } [subscriber-trunk | snmp-trap
link-status | learn]`

Release Information Command introduced before JUNOS Release 7.1.0.
vplsName variable added in JUNOS Release 7.1.0.

Description Assigns a network interface to a bridge group or VPLS instance. You can also use this command to configure the type of interface, enable SNMP link-status processing for the interface, and set the maximum number of dynamic MAC addresses that the interface can learn. The **no** version removes the network interface from the bridge group or VPLS instance and restores the default values for the interface type (subscriber client interface), SNMP link-status processing (disabled), or number of maximum learned MAC addresses (0 addresses).

- Options**
- *bridgeGroupName*—Name of the bridge group to which the interface belongs, as specified with the **bridge** command
 - *vplsName*—Name of the VPLS instance to which the interface belongs, as specified with the **bridge vpls transport-virtual-router** command
 - subscriber-trunk—Creates a trunk (server) interface in the bridge group or VPLS instance; if you omit this keyword, the router creates a subscriber (client) interface by default
 - snmp-trap link-status—Enables SNMP link-status processing only for the specified interface in the bridge group or VPLS instance
 - *addressCount*—Maximum number of MAC addresses that the interface in the bridge group or VPLS instance can learn, up to the maximum number that the router supports, in the range 0–64000

Mode Interface Configuration, Subinterface Configuration

Related Topics

- *Configuring VPLS Network Interfaces* in the *JUNOS BGP and MPLS Configuration Guide*

bridge learn

Syntax bridge { *bridgeGroupName* | *vplsName* } learn *addressCount*
 no bridge { *bridgeGroupName* | *vplsName* } learn

Release Information Command introduced before JUNOS Release 7.1.0.
 vplsName variable added in JUNOS Release 7.1.0.

Description Sets the maximum number of dynamic MAC addresses that a bridge group or VPLS instance can learn. The **no** version restores the default value, 0 (zero) learned addresses. The default value implies that there is no maximum number of learned entries for an individual bridge group or VPLS instance; that is, a bridge group or VPLS instance can learn an unlimited number of MAC addresses, up to the maximum number that the router supports.

To enable or disable the ability of a bridge group or VPLS instance to learn dynamic MAC addresses, use the **bridge acquire** command.



NOTE: For information about the maximum number of learned MAC address entries combined for all bridge groups and VPLS instances supported per chassis, see *JUNOS Release Notes, Appendix A, System Maximums*.

- Options** ■ *bridgeGroupName*—Name of a bridge group specified with the **bridge** command
- *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command
- *addressCount*—Maximum number of MAC addresses that the bridge group can learn, in the range 0–64000

Mode Global Configuration

- Related Topics** ■ *Configuring Optional Attributes for VPLS Instances in the JUNOS BGP and MPLS Configuration Guide*

bridge route

Syntax [no] bridge *bridgeGroupName* route { ip | mpls | pppoe }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables routing of IP, MPLS, or PPPoE packets in a specified bridge group when concurrent routing and bridging (CRB) is enabled for all bridge groups on the router. The command uses the routing table entries to determine the path on which to send the packet toward its final destination. The **no** version disables routing of the specified protocol in the specified bridge group.

If you issue this command for a protocol that is not currently configured in the interface stack for that bridge group, the bridge group discards (drops) those packets.



NOTE: The **bridge route** command is available for a bridge group only after you issue the **bridge crb** command to enable CRB for all bridge groups on the router.

The **bridge route** command is not valid for bridge groups configured as VPLS instances. If you attempt to issue the **bridge route** command for a VPLS instance, the router displays an error message and rejects the command.

- Options**
- *bridgeGroupName*—Name of a bridge group specified with the **bridge** command
 - ip—Specifies that the bridge group routes IP packets
 - mpls—Specifies that the bridge group routes MPLS packets
 - pppoe—Specifies that the bridge group routes PPPoE packets

Mode Global Configuration

bridge snmp-trap link-status

Syntax [no] bridge { *bridgeGroupName* | *vplsName* } snmp-trap link-status

Release Information Command introduced before JUNOS Release 7.1.0.
vplsName variable added in JUNOS Release 7.1.0.

Description Enables SNMP link-status processing for all network interfaces associated with a bridge group or VPLS instance. The **no** version disables SNMP link-status processing for all interfaces in the bridge group or VPLS instance.

Options

- *bridgeGroupName*—Name of a bridge group specified with the **bridge** command
- *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command

Mode Global Configuration

Related Topics

- *Configuring Optional Attributes for VPLS Instances in the JUNOS BGP and MPLS Configuration Guide*

bridge subscriber-policy

Syntax bridge { *bridgeGroupName* | *vplsName* } subscriber-policy *subscriberPolicyName*
 no bridge { *bridgeGroupName* | *vplsName* } subscriber-policy
 [*subscriberPolicyName*]

Release Information Command introduced before JUNOS Release 7.1.0.
 vplsName variable added in JUNOS Release 7.1.0.

Description Associates the subscriber (client) interfaces that belong to a bridge group or to a VPLS instance with a nondefault subscriber policy. The **no** version removes the association with the subscriber policy.

You cannot associate a nondefault subscriber policy with trunk (server) interfaces that belong to a bridge group or to a VPLS instance. You also cannot associate a nondefault subscriber policy with the VPLS virtual core interface, which acts as a trunk interface. The VPLS virtual core interface represents all of the MPLS tunnels from the router to the remote VPLS edge (VE) devices.

- Options** ■ *bridgeGroupName*—Name of a bridge group specified with the **bridge** command
- *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command
- *subscriberPolicyName*—Name of the subscriber policy specified with the subscriber-policy command

Mode Global Configuration

bridge vpls rd

Syntax `bridge vplsName vpls rd routeDistinguisher`
 `no bridge vplsName vpls rd`

Release Information Command introduced in JUNOS Release 7.1.0.

Description Specifies the unique two-part route distinguisher for a VPLS instance that uses BGP as the signaling protocol. Because you cannot change or remove the route distinguisher for a VPLS instance after you set it, issuing the **no** version fails, and causes the router to display an error message.

The following rules apply when you configure the route distinguisher for a VPLS instance:

- After you set the route distinguisher for a VPLS instance, you cannot change it for that VPLS instance. To change the route distinguisher, you must either remove the transport virtual router configuration from the VPLS instance or delete the VPLS instance from the router. You can then reconfigure the VPLS instance with a new route distinguisher.
- Multiple VPLS instances that use the same transport virtual router cannot have the same route distinguisher. Conversely, multiple VPLS instances that use different transport virtual routers can have the same route distinguisher.

The **bridge vpls rd** command is not valid for a VPLS instance that uses LDP as the signaling protocol. To configure a VPLS instance with LDP signaling, use the **mpls ldp vpls vpls-id** command and the **mpls ldp vpls neighbor** command.



NOTE: The **bridge vpls rd** command is available for a VPLS instance only after you issue the **bridge vpls transport-virtual-router** command, which creates the VPLS instance and configures the transport virtual router.

- Options**
- *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command
 - *routeDistinguisher*—Unique two-part identifier in the format *number1:number2*, where:
 - *number1*—Autonomous system (AS) number or an IP address
 - *number2*—Unique integer; 32 bits if *number1* is an AS number; 16 bits if *number1* is an IP address

Mode Global Configuration

Related Topics ■ *Configuring VPLS Instances with BGP Signaling in the JUNOS BGP and MPLS Configuration Guide*

bridge vpls route-target

Syntax [no] bridge *vplsName* vpls route-target { import | export | both } *extendedCommunity*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Creates or adds to a list of VPN extended communities that the router uses to determine which routes are imported by a VPLS instance that uses BGP as the signaling protocol. The **no** version removes a route target from the specified list.

A route is imported into the BGP address family for a specified VPLS instance when both of the following conditions are met:

- An update message with a route-target export list advertises a route.
- That list contains at least one route target that matches a route target in the route-target import list associated with a VPLS instance.

The **bridge vpls route-target** command is not valid for a VPLS instance that uses LDP as the signaling protocol. To configure a VPLS instance with LDP signaling, use the **mpls ldp vpls vpls-id** command and the **mpls ldp vpls neighbor** command.



NOTE: The **bridge vpls route-target** command is available for a VPLS instance only after you issue the **bridge vpls transport-virtual-router** command, which creates the VPLS instance and configures the transport virtual router.

- Options**
- *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command
 - import—Adds the route target to the specified VPLS instance's import list; the VPLS instance accepts only routes that have at least one route target that matches a route target in the import list
 - export—Adds the route target to the specified VPLS instance's export list; all routes advertised from this VPLS instance are associated with the export list
 - both—Adds the route target to both the import list and export list of the specified VPLS instance. This is the recommended setting for a VPLS instance
 - *extendedCommunity*—Two-part number in the format *number1:number2* that identifies an extended community of VPNs, where:
 - *number1*—Autonomous system (AS) number or an IP address
 - *number2*—Unique integer; 32 bits if *number1* is an AS number; 16 bits if *number1* is an IP address

Mode Global Configuration

Related Topics ■ *Configuring VPLS Instances with BGP Signaling in the JUNOS BGP and MPLS Configuration Guide*

bridge vpls site-name site-id

Syntax [no] bridge *vplsName* vpls site-name *siteName* site-id *siteId*
[multi-homed priority *priority*]

Release Information Command introduced in JUNOS Release 7.1.0.
multi-homed priority keywords and *priority* variable added in JUNOS Release 9.3.0.

Description Configures a customer site name and a unique site identifier that belongs to the specified VPLS instance that uses BGP as the signaling protocol. Optionally configures the site to be multihomed. In a VPLS configuration, each customer site is represented by a customer edge (CE) device located at the edge of the customer's network. The router (VPLS edge device, also known as VE router) communicates with the customer site by means of a bridge network interface connection to the CE device. The **no** version removes the site name and site identifier from the VPLS instance, or removes the multihomed configuration for the customer site and returns it to a single-homed state.

The **bridge vpls site-name site-id** command is not valid for a VPLS instance that uses LDP as the signaling protocol. To configure a VPLS instance with LDP signaling, use the **mpls ldp vpls vpls-id** command and the **mpls ldp vpls neighbor** command.



NOTE: The **bridge vpls site-name site-id** command is available for a VPLS instance only after you issue the **bridge vpls transport-virtual-router** command, which creates the VPLS instance and configures the transport virtual router.

- Options**
- *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command
 - *siteName*—Name of the site; string of up to 128 alphanumeric characters
 - *siteId*—Numerical identifier for the site; must be an unsigned 16-bit integer greater than zero that is unique across the VPLS domain associated with the VPLS instance
 - *priority*—Number that sets the priority of this VPLS instance for a multi-homed site, in the range 1–65535; priority is sent in BGP advertisements as the Local-Preference attribute and determines whether the router hosting the VPLS instance becomes the designated VE router for this multihomed site

Mode Global Configuration

Related Topics

- *Configuring VPLS Instances with BGP Signaling in the JUNOS BGP and MPLS Configuration Guide*

bridge vpls site-range

Syntax `bridge vplsName vpls site-range siteRange`
 `no bridge vplsName vpls site-range`

Release Information Command introduced in JUNOS Release 7.1.0.

Description Configures the maximum number of customer sites that can participate in the specified VPLS domain that uses BGP as the signaling protocol. In a VPLS configuration, each customer site is represented by a customer edge (CE) device located at the edge of the customer's network. The router (VPLS edge device) communicates with the customer site by means of a bridge network interface connection to the CE device. The **no** version restores the default site range, 1.

The **bridge vpls site-range** command is not valid for a VPLS instance that uses LDP as the signaling protocol. To configure a VPLS instance with LDP signaling, use the **mpls ldp vpls vpls-id** command and the **mpls ldp vpls neighbor** command.



NOTE: The **bridge vpls site-range** command is available for a VPLS instance only after you issue the **bridge vpls transport-virtual-router** command, which creates the VPLS instance and configures the transport virtual router.

- Options** ■ *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command
- *siteRange*—Maximum number of sites that can participate in the VPLS domain, in the range 1–65534; default value is 1

Mode Global Configuration

Related Topics ■ *Configuring VPLS Instances with BGP Signaling in the JUNOS BGP and MPLS Configuration Guide*

bridge vpls transport-virtual-router

Syntax `bridge vplsName vpls transport-virtual-router virtualRouterName`
 `no bridge vplsName vpls transport-virtual-router`

Release Information Command introduced in JUNOS Release 7.1.0.

Description Configures the transport virtual router for a VPLS instance that uses either BGP or LDP as the signaling protocol. Issuing this command creates a new VPLS instance on the router or causes an existing bridge group to become a VPLS instance. The **no** version removes the VPLS instance from the router and clears any attributes configured for the deleted VPLS instance.

A VPLS instance is a single instance of the virtual private LAN service (VPLS). VPLS employs a layer 2 virtual private network (VPN) to connect multiple individual LANs across a service provider's MPLS network. The multiple LANs function as a single virtual LAN.

The transport virtual router specifies the name of the virtual router on which the BGP or LDP instance that signals reachability for this VPLS instance is configured.

To create a new VPLS instance or configure an existing bridge group as a VPLS instance, you must issue the **bridge vpls transport-virtual-router** command before you issue any other commands to configure VPLS attributes; otherwise, the VPLS configuration fails.

- Options** ■ *vplsName*—Name of the new VPLS instance, or name of an existing bridge group specified with the **bridge** command that you want to configure as a VPLS instance; string of up to 32 alphanumeric characters
- *virtualRouterName*—Name of the virtual router on which the BGP or LDP instance that signals reachability for this VPLS instance is configured

Mode Global Configuration

Related Topics ■ *Configuring VPLS Instances with BGP Signaling and Configuring VPLS Instances with LDP Signaling* in the *JUNOS BGP and MPLS Configuration Guide*

broadcast

Syntax broadcast { permit | deny }
no broadcast

Release Information Command introduced before JUNOS Release 7.1.0.

Description Modifies the subscriber policy for the broadcast protocol to define whether the subscriber (client) interfaces that belongs to a bridge group or to a VPLS instance forward (permit) or filter (deny) broadcast packets. The **no** version restores the default value, deny broadcast packets.

You cannot change the default subscriber policy values for trunk (server) interfaces that belongs to a bridge group or to a VPLS interface. You also cannot change the default subscriber policy values for a VPLS virtual core interface, which acts as a trunk interface. The VPLS virtual core interface represents all of the MPLS tunnels from the router to the remote VPLS edge (VE) device.

- Options**
- permit—Specifies that the subscriber interface associated with the bridge group or VPLS instance forwards broadcast packets
 - deny—Specifies that the subscriber interface associated with the bridge group or VPLS instance filters broadcast packets

Mode Subscriber Policy Configuration

buffer-weight

Syntax `buffer-weight bufferWeight`
 `no buffer-weight`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the buffer weight of the queue. The **no** version returns the queue to its default buffer weight.

Options ■ *bufferWeight*—Range 1–63; default value is 8

Mode Queue Profile Configuration

Related Topics ■ Configuring Queue Profiles to Manage Buffers and Thresholds

bulkstats

Syntax no bulkstats

Description This command has only a **no** version. See the no bulkstats command for a complete description.

Mode Router Configuration

bulkstats collector

Syntax bulkstats collector *collectorIndex*
 [collect-mode { auto-xfer | on-file-full | manual-xfer } | description *descrip* |
 interval *intrvl* | max-size *maxSize* | primary-receiver *primRecvIndex* |
 secondary-receiver *secRecvIndex* | single-interval]

no bulkstats collector *collectorIndex* [collect-mode | description | interval | max-size
 |primary-receiver | secondary-receiver | single-interval]*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates and configures a collector of bulk statistical data to collect MIB-2 ifTable MIB objects. You can configure up to six collectors. The **no** version restores the default value for specified options; if no options are specified, the **no** version deletes the collector.

- Options**
- *collectorIndex*—Number in the range 1–65535 that identifies the particular data collector
 - collect-mode—Specifies one of the following collection modes:
 - auto-xfer—Agent automatically transfers file when interval expires
 - on-file-full—Agent automatically transfers file when it is full
 - manual-xfer—Router or user-initiated transfers; default collection mode
 - *descrip*—Descriptive information to insert into the bulkstats file
 - *intrvl*—Time period in the range 300– 86400 seconds for which the collector transfers data from the router to the receivers; default interval is 360 seconds
 - *maxSize*—Maximum size of the file in the range 10240–20971520 bytes; default file size is 2,621,440 bytes
 - *primRecvIndex*—Number in the range 1–65535 that identifies the primary receiver to which the router transfers the data; by default the primary receiver is cleared
 - *secRecvIndex*—Number in the range 1–65535 that identifies the secondary (backup) receiver to which the router transfers the data; by default the secondary receiver is cleared
 - single-interval—Specifies that the collector retrieves the bulk statistics data only once; by default, the collector receives the data periodically
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

bulkstats file-format endOfLine-LF

Syntax [no] bulkstats file-format endOfLine-LF

Release Information Command introduced before JUNOS Release 7.1.0.

Description Removes the carriage return (CR) and leaves only a line feed (LF) at the end of each line in the bulkstats file. The **no** version returns the end of line format to the default, CR and LF.

Mode Global Configuration

bulkstats interfaces description-format common

Syntax [no] bulkstats interfaces description-format common

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the conventional industry method of encoding the SNMP ifDescr object that the bulkstats application reports. The **no** version returns the encoding method to a proprietary encoding scheme.

Mode Global Configuration

bulkstats interfaces rfc1213

Syntax [no] bulkstats interfaces rfc1213

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables RFC 1213 interface numbering mode on bulkstats. The **no** version disables RFC 1213 interface numbering mode on bulkstats.

Mode Global Configuration

bulkstats interface-type

Syntax [no] bulkstats interface-type *interfaceType* [*interfaceSpecifier*]*
[collector *collectorIndex*]

Release Information Command introduced before JUNOS Release 7.1.0.
mplsL2shim, **mplsMajor**, and **mplsMinor** keywords added in JUNOS Release 8.2.0.

Description Configures the interface type on which you want to collect statistics. The **no** version deletes the interface type from bulkstats collection.

- Options**
- *interfaceType*—One of the following interface types for which you can collect statistics: ATM, ATM 1483, Ethernet, Frame Relay, Frame Relay subinterface, Cisco HDLC, IP, MPLS minor, MPLS major, MPLS shim, PPP, VLAN subinterface
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line
 - *collectorIndex*—Number in the range 1–65535 that identifies the particular data collector. Always specify this option if you defined more than one collector.

Mode Global Configuration

bulkstats receiver remote-name

Syntax bulkstats receiver *receiverIndex* remote-name *remoteName*.sts
 [*receiverAttrib* [*receiverAttrib*]*]

no bulkstats receiver *receiverIndex* [remote-name *remoteName*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the bulk statistics receiver parameters. The **no** version deletes the receiver.

- Options**
- *receiverIndex*—Number in the range 1–65535 that identifies the receiver of the data
 - *remoteName*—Composed of the remote host, path, filename, and formatters; include a .sts filename extension
 - *receiverAttrib*—One of the following dynamic attributes
 - *sysName*—Inserts the router name into the stored remote filename
 - *sysUpTime*—Inserts the router up time into the stored remote filename
 - *collectorSequence*—Inserts a sequence number into the stored remote filename
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

bulkstats schema

Syntax `bulkstats schema schemaIndex [collector collectorIndex]`
 `no bulkstats schema schemaIndex`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the schema for collecting bulk statistics. The **no** version removes the schema.

- Options** ■ *schemaIndex*—Identifier for the schema in the range 1–65535
 ■ *collectorIndex*—Identifier for the collector in the range 1–65535

Mode Global Configuration

bulkstats schema subtree

Syntax bulkstats schema *schemaIndex* subtree
 { if-stack | if-stats { subtree-list [*ifstatsList* [*ifstatsList*]*] |
 if-create-delete-time-stats interfaceType *interfaceType* } | igmp | system }

 bulkstats schema *schemaIndex* subtree
 { if-stack | if-stats | igmp [subtree-list *igmpList* [*igmpList*]*] | system }

 no bulkstats schema *schemaIndex*

Release Information Command introduced before JUNOS Release 7.1.0.
mplsL2shim, **mplsMajor**, and **mplsMinor** keywords added in JUNOS Release 8.2.0.

Description Configures the schema for collecting if-stack, if-stats, or router data. The **no** version removes the schema.

- Options**
- *schemaIndex*—Identifier for the schema in the range 1–65535
 - if-stack—Retrieves ifStackTable
 - if-stats—Retrieves ifTable/ifXTable counters
 - *ifstatsList*—Type of statistics and **time-offset** keyword, which includes the offset from the master interval at which the record was collected in each bulkstats interface record
 - if-create-delete-time-stats—Retrieves interface final statistics (interface statistics that may be lost during higher create or delete frequency)
 - *interfaceType*—One of the following interface types for which you can collect statistics: ATM 1483, IP, MPLS minor, MPLS major, MPLS shim, PPP
 - igmp—Retrieves IGMP statistics
 - *igmpList*—Type of statistics and **time-offset** keyword, which includes the offset from the master interval at which the record was collected in each bulkstats interface record
 - system—Retrieves sysUpTime and nvsUtilPct global statistics; retrieves slotDescr, the cpuUtilPct, and memUtilPct per-slot statistics
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

bulkstats schema subtree policy

Syntax bulkstats schema *schemaIndex* subtree policy [policy-name *policyName*]
 [policy-type *policyType*] [policy-subtreelist *policyList* [*policyList*]*]
 no bulkstats schema *schemaIndex*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the schema to collect statistics on a specific policy, a type of policy, or based on color-coded tags applied by a policy. The **no** version removes the schema.

- Options**
- *schemaIndex*—Identifier for the schema in the range 1–65535
 - *policyName*—Name of policy for which you want to collect statistics
 - *policyType*—Select one of the following types:
 - input—Collect data on input policies
 - localInput—Collect data on local input policies
 - output—Collect data on output policies
 - *policyList* —Retrieves statistics based on color-coded tags applied by a policy
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

bulkstats schema subtree qos

Syntax bulkstats schema *schemaIndex* subtree qos [subtree-list *qosList* [*qosList*]* | export-summarized-stats]

no bulkstats schema *schemaIndex*

Release Information Command introduced in JUNOS Release 11.1.0.

Description Configures the bulk statistics schema to collect QoS statistics and configuration information on egress queues belonging to different interface types. The **no** version removes the schema.

- Options**
- *schemaIndex*—Identifier for the schema in the range 1–65535
 - *qosList*—Select one of the following queue attributes:
 - aggregate-drop-rate—Configures QoS schema to export the average drop rate within the rate-period specified in the statistics profile of the egress queue
 - all—Configures QoS schema to export all statistics; this is the default option
 - assured-rate—Configures QoS schema to export the assured rate attribute
 - burst—Configures QoS schema to export the burst attribute
 - byte-adjustment-bytes—Configures QoS schema to export the number of bytes configured for the byte-adjustment application, if the byte-adjustment application is enabled on the queue
 - byte-adjustment-type—Configures QoS schema to export the type of byte-adjustment , if byte-adjustment application is enabled on the queue
 - drop-profile—Configures QoS schema to export the drop profile name associated with the queue
 - forwarded-bytes—Configures QoS schema to export the number of bytes forwarded from the queue
 - forwarded-packets—Configures QoS schema to export the number of forwarded packets from the queue
 - forwarded-rate—Configures QoS schema to export the average forwarded rate within the rate period specified on the statistics profile of the queue
 - green-dropped-bytes—Configures QoS schema to export the number of bytes of green traffic that was dropped on this queue
 - green-dropped-packets—Configures QoS schema to export the number of packets of green traffic that was dropped on this queue
 - parent-shaping-rate—Configures QoS schema to export the shaping rate enabled on the parent interface in the scheduling hierarchy

- parent-shared-shaping-rate—Configures QoS schema to export the shared shaping rate enabled on the parent interface in the scheduling hierarchy
- parent-weight—Configures QoS schema to export the aggregate weight of the parent interface
- queue-length—Configures QoS schema to export the queue length attribute
- queue-profile—Configures QoS schema to export the queue profile name
- red-dropped-bytes—Configures QoS schema to export the number of bytes of red traffic that was dropped on the queue
- red-dropped-packets—Configures QoS schema to export the number of red packets that was dropped on the queue
- RED-enabled—Configures QoS schema to verify whether the Random Early Detect (RED) option is enabled on the queue
- scheduler-profile—Configures QoS schema to export the scheduler profile name
- shaping-mode—Configures QoS schema to export the shaping mode attribute
- shaping-rate—Configures QoS schema to export the shaping rate attribute
- shared-shaping-mode—Configures QoS schema to export the shared shaping mode attribute
- shared-shaping-rate—Configures QoS schema to export the shared shaping rate attribute
- statistics-profile—Configures QoS schema to export the statistics profile name
- weight—Configures QoS schema to export the weight assigned to the queue
- yellow-dropped-bytes—Configures QoS schema to export the number of bytes of yellow traffic that was dropped on the queue
- yellow-dropped-packets—Configures QoS schema to export the number of yellow packets that were dropped on the queue
- export-summarized-stats—Exports the summarized QoS rate statistics over each S-VLAN or ATM VP (virtual path)
- *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

- Related Topics**
- *Configuring SNMP in JUNOS System Basics Configuration Guide*
 - QoS Statistics Overview

bulkstats traps

Syntax bulkstats traps { nearly-full [*threshold*] | full }
 no bulkstats traps { nearly-full | full }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the bulkstats traps. The **no** version disables the trap.

- Options**
- nearly-full—Specifies a percentage less than 100 percent
 - *threshold*—Percentage less than 100 percent; if not specified, defaults to 99 percent
 - full—100 percent

Mode Global Configuration

bulkstats virtual-router-group

Syntax [no] bulkstats virtual-router-group collector *collectorindex* *VRnames*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Configures the bulkstats for virtual router groups. The **no** version prevents bulkstats from being reported for virtual router groups.

- Options**
- *virtual-router-group*—Specifies the name or unique index number that contains from 1 to the maximum number of routers supported in the system
 - *collectorIndex*—Number that identifies the particular data collector, in the range 1–65535
 - *VRnames*—List of virtual router names

Mode Global Configuration

bundled-group-id

Syntax [no] bundled-group-id *bundledGroupID*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns a bundled group identifier when no endpoint discriminator is available for bundled sessions using an L2TP destination host profile. When multiple tunnel-service modules are installed in a router that is deployed as an LNS and the tunnel sessions carry MLPPP, the router can use the bundled group identifier when selecting a tunnel-service module for bundled sessions. The **no** version restores the default value, no assigned bundled group identifier.



NOTE: We recommend that you assign a bundled group identifier for bundled sessions only when you are certain that endpoint discriminators are unavailable to identify bundle membership.

Options ■ *bundledGroupID*—Identifier for a bundled group in the range 0–4294967295

Mode L2TP Destination Profile Host Configuration

bundled-group-id-overrides-mlppp-ed

Syntax [no] bundled-group-id-overrides-mlppp-ed

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that the router uses the bundled group identifier you assigned using the **bundled-group-id** command when selecting a tunnel-service module instead of any endpoint discriminator. The **no** version removes the override.



NOTE: We strongly recommend that you use this command only with the support of JTAC.

Mode L2TP Destination Profile Host Configuration

Chapter 4

C Commands

cache entries

Syntax `cache entries entryNumber`
`no cache entries`

Release Information Command introduced in JUNOS Release 8.1.0.

Description Sets the number of entries in the aggregation cache. The **no** version sets the number of entries to the default value.

Options ■ *entryNumber*—Number of entries in the aggregation cache in the range 1024—524288; default value is 4096

Mode Flow Cache Configuration

cache timeout

Syntax cache timeout { active *activeTimer* | inactive *inactiveTimer* }
 no cache timeout

Release Information Command introduced in JUNOS Release 8.1.0.

Description Sets the active and inactive aging timers. The **no** version resets the default values.

- Options** ■ *activeTimer*—Active aging timer in the range 1—60
 ■ *inactiveTimer*—Inactive aging timer in the range 10—600

Mode Flow Cache Configuration

cablelength

Syntax `cablelength length`
 `no cablelength`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the length of the cable, which determines power requirements. The **no** version uses the default value, 0 feet.

Options ■ *length* —Cable length in the range 0–450 feet

Mode Controller Configuration

cbr

Syntax *cbr pcr**no cbr***Release Information** Command introduced in JUNOS Release 7.1.0.
ATM VC Class Configuration mode added in JUNOS Release 7.3.0.**Description** In ATM VC Configuration mode, configures the constant bit rate (CBR) service category on an ATM PVC. You must specify the peak cell rate (PCR) value. The **cbr** command is valid only for data PVCs; you cannot use this command for control (ILMI or signaling) PVCs. The **no** version restores the default service category, unspecified bit rate (UBR) without a PCR.In ATM VC Class Configuration mode, configures the CBR service category as part of a VC class definition that you assign to an ATM data PVC. The **no** version restores the default service category, UBR without a PCR, in the VC class.**Options** ■ *pcr*—Peak cell rate, in Kbps, in the range 1–149760 (for OC3 ATM modules) or 1–599040 (for OC12 ATM modules)**Mode** ATM VC Configuration, ATM VC Class Configuration

channelized

Syntax [no] channelized

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures a port on the CT3/T3-F0 line module and associated I/O module to support channelized T3 operation. The **no** version configures the port for unchannelized operation.

Mode Controller Configuration

check-disk

Syntax `check-disk [repair] [disk0 | disk1]`

Release Information Command introduced before JUNOS Release 7.1.0.
 disk0 and **disk1** keywords added in JUNOS Release 7.2.0.
 Privileged Exec mode added in JUNOS Release 8.0.0.

Description Finds and repairs structural inconsistencies and damage in the DOS file system in unmounted flash cards on the primary SRP module. There is no **no** version.

- Options**
- `disk0`—Specifies flash card in slot 0 of the SRP module; default value is `disk0`; available only in Boot mode, because `disk0` cannot be in an unmounted state in a router outside of Boot mode
 - `disk1`—Specifies flash card in slot 1 of the SRP module; supported only on the E120 router and the E320 router

Mode Boot, Privileged Exec

check-vpn-next-hops

Syntax [no] check-vpn-next-hops

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables a BGP speaker to take the reachability of the next hop on received VPNv4 or VPNv6 routes into account when it determines the best route to a prefix. Checking the reachability is disabled by default. The **no** version explicitly disables reachability checking.

Mode Address Family Configuration

classifier-group

Syntax classifier-group { * | *classifierName* } [precedence *precValue*] [parent-group *parentGroupName*] [external parent-group *externalParentGroupName* parameter *parameterName*]

no classifier-group { * | *classifierName*]

Release Information Command introduced before JUNOS Release 7.1.0.
parent-group keyword and *parentGroupName* variable added in JUNOS Release 7.2.0.
external parent-group keyword and *externalParentGroupName* variable added in JUNOS Release 8.0.0.

Description Creates a classifier group for a policy list and assigns precedence to the specific CLACL in the group. This command accesses Classifier Group Configuration mode, in which you create policy rule configurations related to the specified CLACL. If a parent group was not created by the **parent-group** command, the **parent-group** keyword creates a parent group in a rate-limit hierarchy for IP, IPv6, L2TP, and MPLS. All packets matching the classifier are sent to the parent group for further processing, except for packets dropped by the classifier using the filter rule. More than one classifier group can have the same parent group, which enables you to create hierarchies. The **no** version removes the classifier group and its rules from the policy list.

- Options**
- *—Specifies that the router selects all packets from the interface associated with the policy list for this classifier group
 - *classifierName*—Name of a specific CLACL used to classify packets in this policy list
 - *precValue*—Precedence value for the CLACL, in the range 0–65535; a value of 100 is assigned if no value is specified
 - *parentGroupName*—Name of the parent group; if the parent group does not exist, naming the parent group creates an empty parent group



NOTE: Secure policy lists, which are used for packet mirroring operations, do not support named classifier groups. You must use **classifier-group ***. Also, secure policy lists do not support the **precedence** keyword.

- *externalParentGroupName*—External parent group name
- *parameterName*—Parameter name

Mode Policy List Configuration

Related Topics ■ Creating a Classifier Group for a Policy List

- Configuring CLI-Based Mirroring

class-int

Syntax `class-int vcClassName`
`no class-int [vcClassName]`

Release Information Command introduced in JUNOS Release 7.3.0.

Description When issued from Interface Configuration mode, assigns a previously configured VC class to an ATM major interface. When issued from Subinterface Configuration mode, assigns a previously configured VC class to a static ATM 1483 subinterface. Issuing this command applies the set of attributes in the specified VC class to the ATM data PVCs statically or dynamically created on the ATM major interface or ATM 1483 subinterface. The **no** version removes the VC class association with the interface or subinterface, and causes the router to set the PVC attributes to their systemwide default values, or to the values set in the associated VC class with the next highest order of precedence.

Options ■ *vcClassName*—Name of the VC class configured with the `vc-class atm` command

Mode Interface Configuration, Subinterface Configuration

class-vc

Syntax `class-vc vcClassName`
`no class-vc [vcClassName]`

Release Information Command introduced in JUNOS Release 7.3.0.

Description Assigns a previously configured VC class to an individual ATM data PVC. The **class-vc** command is valid only for data PVCs created with the `pvc` command; it has no effect for data PVCs created with the **atm pvc** command, or for control (ILMI or signaling) PVCs. Issuing this command applies the set of attributes in the specified VC class to the ATM data PVC. The **no** version removes the VC class association with the ATM PVC.

Options ■ *vcClassName*—Name of the VC class configured with the `vc-class atm` command

Mode ATM VC Configuration

cleanup-timeout-factor

Syntax cleanup-timeout-factor *lostRefreshes*
no cleanup-timeout-factor

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the number of refresh messages that can be lost before the PATH or RESV state is ended. The **no** version restores the default value, 3.

Options ■ *lostRefreshes*—Number of lost refresh messages

Mode RSVP Profile Configuration

clear access-list

Syntax clear access-list [*accessListName*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears counters for entries in IP access lists. There is no **no** version.

Options ■ *accessListName*—Name of the access list; string of 1–32 alphanumeric characters

Mode Privileged Exec

clear arp

Syntax clear [ip] arp [vrf *vrfName*] { *ipAddress interfaceType interfaceSpecifier* | * }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears entries from the ARP cache. There is no **no** version.

- Options**
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
 - *ipAddress*—IP address in 32-bit dotted-decimal format of the entry to be cleared
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *—Clears all dynamic ARP entries

Mode Privileged Exec

clear bfd adapted-intervals

Syntax clear bfd adapted-intervals

Release Information Command introduced in JUNOS Release 7.3.0.

Description Resets adapted timer intervals for all BFD sessions on the router. There is no **no** version.

Mode Global Configuration

clear bfd session

Syntax clear bfd session [address *ipAddress* | discriminator *discriminatorID*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Restarts all BFD sessions or a specified BFD session. There is no **no** version.

- Options**
- *ipAddress*—IP address of the destination to which the session has been established
 - *discriminatorID*—Unique system-wide identifier for the BFD session; integer in the range 1–4294967295

Mode Privileged Exec, User Exec

clear bgp ipv6

Syntax clear bgp ipv6 [unicast | multicast | vpngv6 | route-target signaling]
 [*ipAddress* | *ipv6Address* | peer-group *peerGroupName* | *] [vrf *vrfName*]
 [soft [in | out]]

Release Information Command introduced before JUNOS Release 7.1.0.
ipv6Address variable added in JUNOS Release 8.0.0.
route-target signaling keywords added in JUNOS Release 8.2.0.

Description Resets the IPv6 BGP session. If the **soft** option is not used, brings down the underlying TCP connection and then brings it back up again, causing both peers to resend their complete BGP routing table. If the **soft out** option is used, the BGP speaker reapplies outbound policy and resends all routes to the specified peer(s). If the **soft in** option is used, the BGP speaker reapplies inbound policy to the routes received from the specified peers. This is possible only if soft reconfiguration inbound has been enabled for the peer or the peer supports the route-refresh capability. There is no **no** version.

- Options**
- unicast—Clears the unicast routing table; the default option
 - multicast—Clears the multicast routing table
 - vpngv6—Clears the VPNv6 unicast routing and forwarding table
 - route-target signaling—Clears the route-target membership information
 - *ipAddress*—IP address of identified BGP neighbor to clear
 - *ipv6Address*—IPv6 address of identified BGP neighbor to clear
 - *peerGroupName*—Name of a BGP peer group to clear
 - *—Clears all connections
 - *vrfName*—Name of a virtual routing and forwarding instance to clear
 - soft—Specifies soft reconfiguration
 - in—Triggers inbound soft reconfiguration
 - out—Triggers outbound soft reconfiguration

Mode Privileged Exec

clear bgp ipv6 dampening

Syntax To clear IPv6-specific information for only the route-target address family:

```
clear bgp ipv6 route-target signaling
{ dampening | flap-statistics } [ rtfPrefix | rtfAddress ]
```

To clear IPv6-specific information for any case other than for the route-target address family:

```
clear bgp ipv6 [ vrf vrfName ] [ unicast | multicast | vpnv6 ]
{ dampening | flap-statistics } [ ipv6Prefix ]
```

Release Information Command introduced before JUNOS Release 7.1.0.
route-target signaling keywords and *rtMemNlri* variable added in JUNOS Release 8.2.0.
rtMemNlri variable replaced by two variables, *rtfAddress* and *rtfPrefix*, in JUNOS Release 9.1.0.

Description Clears IPv6-specific BGP route flap dampening information and reinstates the suppressed routes. If the *ipv6Prefix* option is not used, clears the entire IPv6 BGP routing table. The **dampening** keyword and the **flap-statistics** keyword both have the same effect. There is no **no** version.

- Options**
- route-target signaling—Clears the route-target membership information
 - *rtfPrefix*—Prefix representing the route-target membership NLRI (RT-MEM-NLRI), in the format *asNumber* : *extendedCommunity* / *prefixLength* (for example, 320:320:524/36) where:
 - *asNumber*—AS number for origin of route target information, in the range 1–4294967295
 - *extendedCommunity*—Two-part number in the format *number1*:*number2* that identifies an extended community of VPNs, in the format *number1* : *number2*, where:
 - *number1*—Autonomous system (AS) number, in the range 1–4294967295, or an IP address
 - *number2*—Unique integer, in the range 1–4294967295; 32 bits if *number1* is a 16-bit AS number; 16 bits if *number1* is an IP address or a 32-bit AS number
 - *prefixLength*—Number that specifies the length of the route prefix, in the range 32–96
 - *rtfAddress*—*rtfPrefix* with a prefix length of 96; representing the route-target membership NLRI (RT-MEM-NLRI), in the format *asNumber*:*extendedCommunity* (for example, 320:320:524 or 320:50.2.3.4:524)
 - *vrfName*—Name of a virtual routing and forwarding instance to clear

- unicast—Clears the unicast routing table; the default option
- multicast—Clears the multicast routing table
- vpnv6—Clears the VPNv6 unicast routing and forwarding table
- *ipv6Prefix*—IPv6 network for which to clear dampening information

Mode Privileged Exec

clear bgp ipv6 dynamic-peers

Syntax clear bgp ipv6 [*ipAddress* | *ipv6Address* | peer-group *peerGroupName* | *]
[vrf *vrfName*] dynamic-peers

Release Information Command introduced before JUNOS Release 7.1.0.
ipv6Address variable added in JUNOS Release 8.0.0.

Description Removes all IPv6-specific dynamic peers in the specified scope. There is no **no** version.

- Options**
- *ipAddress*—IP address of identified BGP neighbor to clear
 - *ipv6Address*—IPv6 address of identified BGP neighbor to clear
 - *peerGroupName*—Name of a BGP peer group to clear
 - *—Clears all connections
 - *vrfName*—Name of a virtual routing and forwarding instance to clear

Mode Privileged Exec

clear bgp ipv6 redistribution

Syntax clear bgp ipv6 [unicast | multicast] redistribution

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears all IPv6 routes that have been redistributed into BGP. There is no **no** version.

- Options**
- unicast—Clears the unicast routing table; the default option
 - multicast—Clears the multicast routing table

Mode Privileged Exec

clear bgp ipv6 wait-end-of-rib

Syntax clear bgp ipv6 [unicast | multicast | vpnv6 | route-target signaling] [vrf *vrfName*] [*ipAddress* | *ipv6Address* | peer-group *peerGroupName* | *] wait-end-of-rib

Release Information Command introduced before JUNOS Release 7.1.0.
ipv6Address variable added in JUNOS Release 8.0.0.
route-target signaling keywords added in JUNOS Release 8.2.0.

Description Resets the IPv6 BGP session and brings down the underlying TCP connection and then brings it back up again, causing both peers to resend their complete BGP routing table. Clears the specified peer from the set of peers for which BGP is waiting to receive an End-of-RIB marker after a peer restart. Hard clearing a peer has the same effect for that peer. There is no **no** version.

- Options**
- unicast—Clears the unicast routing table; the default option
 - multicast—Clears the multicast routing table
 - vpnv6 —Clears the VPNv6 unicast routing and forwarding table
 - route-target signaling—Clears the route-target membership information
 - *vrfName*—Name of a virtual routing and forwarding instance to clear
 - *ipAddress*—IP address of identified BGP neighbor to clear
 - *ipv6Address*—IPv6 address of identified BGP neighbor to clear
 - *peerGroupName*—Name of a BGP peer group to clear
 - *—Clears all connections

Mode Privileged Exec

clear bridge

Syntax clear bridge { *bridgeGroupName* | *vplsName* }

Release Information Command introduced before JUNOS Release 7.1.0.
vplsName variable added in JUNOS Release 7.1.0.

Description Removes all dynamic (learned) MAC address entries from the forwarding table for the specified bridge group or VPLS instance . There is no **no** version.

Options

- *bridgeGroupName*—Name of a bridge group specified with the **bridge** command
- *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command

Mode Privileged Exec

Related Topics

- *Clearing Dynamic MAC Addresses from the VPLS Forwarding Table* in the *JUNOS BGP and MPLS Configuration Guide*

clear bridge address

Syntax clear bridge { *bridgeGroupName* | *vplsName* } address *macAddress*

Release Information Command introduced in JUNOS Release 7.1.0.
vplsName variable added in JUNOS Release 7.1.0.

Description Removes a specific dynamic (learned) MAC address entry from the forwarding table for the specified bridge group or VPLS instance. There is no **no** version.

- Options**
- *bridgeGroupName*—Name of a bridge group specified with the **bridge** command
 - *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command
 - *macAddress*—Unique 48-bit (6-byte) number that is programmed into each LAN network interface card (NIC) at the time of manufacture; also known as a hardware address or physical address. The MAC address format is a dotted triple of four-digit hexadecimal numbers; for example, 0090.1a40.4c7c

Mode Privileged Exec

- Related Topics**
- *Clearing Dynamic MAC Addresses from the VPLS Forwarding Table* in the *JUNOS BGP and MPLS Configuration Guide*

clear bridge interface

Syntax clear bridge interface *interfaceType interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Removes from the forwarding table all dynamic (learned) MAC address entries for a specified network interface that belongs to a bridge group or to a VPLS instance . There is no **no** version.



NOTE: Using the **clear bridge interface** command for a VPLS instance affects the specified network interface associated with the VPLS instance, but has no effect on the VPLS virtual core interface, which represents all of the MPLS tunnels from the router to the remote VPLS edge (VE) devices. To remove all MAC addresses from the forwarding table for the VPLS virtual core interface, use the **clear bridge interface vpls** command.

- Options**
- *interfaceType*—One of the following interface types listed in “Interface Types and Specifiers” on page 5
 - atm
 - fastEthernet
 - gigabitEthernet
 - tenGigabitEthernet
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec

Related Topics

- *Clearing Dynamic MAC Addresses from the VPLS Forwarding Table* in the *JUNOS BGP and MPLS Configuration Guide*

clear bridge interface vpls

Syntax clear bridge interface vpls *vplsName*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Removes from the forwarding table for a VPLS instance all dynamic (learned) MAC address entries on the VPLS virtual core interface, which represents all of the MPLS tunnels from the router to the remote VPLS edge (VE) devices. There is no **no** version.



NOTE: Using the **clear bridge interface vpls** command affects the VPLS virtual core interface, but has no effect on the network interfaces associated with the VPLS instance. To remove all MAC addresses from the forwarding table for a VPLS network interface, use the **clear bridge interface** command.

Options ■ *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command

Mode Privileged Exec

Related Topics ■ *Clearing Dynamic MAC Addresses from the VPLS Forwarding Table* in the *JUNOS BGP and MPLS Configuration Guide*

clear egress-queue

Syntax clear egress-queue *interfaceType interfaceSpecifier* [*explicit*]
[*traffic-class trafficClassName*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears egress queue statistics for the all queues bound to the specified interface for queues stacked at and above the interface, or only for the specified traffic class. There is no **no** version.

- Options**
- *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *explicit*—Clears queues only on the specified interface and not queues stacked above the interface
 - *trafficClassName*—Name of a traffic class for which egress queue statistics are cleared

Mode Privileged Exec

clear fabric-queue

Syntax clear fabric-queue [traffic-class *trafficClassName*] [egress-slot *egressSlot*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears statistics for all fabric queues or for the specified traffic-class, egress-slot, or both. There is no **no** version.

- Options**
- *trafficClassName*—Name of a traffic class for which fabric-queue statistics will be cleared
 - *egressSlot*—Number of an egress slot for which fabric-queue statistics will be cleared

Mode Privileged Exec

clear ip bgp

Syntax clear ip bgp [*ipAddress* | *ipv6Address* | peer-group *peerGroupName* | *] [vrf *vrfName*] [ipv4 unicast | ipv4 multicast | vpnv4 unicast | l2vpn all | l2vpn vpls *vplsName* | l2vpn vpws *vpwsName* | route-target signaling] soft [in [prefix-filter] | out]]

Release Information Command introduced before JUNOS Release 7.1.0.
l2vpn keyword added in JUNOS Release 7.1.0.
ipv6Address variable added in JUNOS Release 8.0.0.
route-target signaling keywords added in JUNOS Release 8.2.0.
all, **vpls**, and **vpws** keywords and *vplsName* and *vpwsName* variables added in JUNOS Release 9.3.0.

Description If the **soft** option is not used, brings down the underlying TCP connection and then brings it back up again, causing both peers to resend their complete BGP routing table. If the **soft out** option is used, the BGP speaker reapplies outbound policy and resends all routes to the specified peers. If the **soft in** option is used, the BGP speaker reapplies inbound policy to the routes received from the specified peers. This is possible only if soft reconfiguration inbound has been enabled for the peer or the peer supports the route-refresh capability. There is no **no** version.

- Options**
- *ipAddress*—IP address of identified BGP neighbor to clear
 - *ipv6Address*—IPv6 address of identified BGP neighbor to clear
 - *peerGroupName*—Name of a BGP peer group to clear
 - *—Clears all connections
 - *vrfName*—Name of a virtual routing and forwarding instance to clear
 - ipv4 unicast—Clears the IPv4 unicast routing table; the default option
 - ipv4 multicast—Clears the IPv4 multicast routing table
 - vpnv4 unicast—Clears the VPNv4 unicast routing and forwarding table
 - l2vpn all—Clears the L2VPN reachability information for all VPLS and VPWS instances in the L2VPN address family
 - l2vpn vpls *vplsName*—Clears the L2VPN reachability information for the VPLS instance with the name *vplsName*
 - l2vpn vpws *vpwsName*—Clears the L2VPN reachability information for the VPWS instance with the name *vpwsName*
 - route-target signaling—Clears the route-target membership information
 - soft—Specifies soft reconfiguration
 - in—Triggers inbound soft reconfiguration
 - prefix-filter—Pushes out prefix list and Cisco-proprietary prefix list outbound route filters and triggers inbound soft reconfiguration
 - out—Triggers outbound soft reconfiguration

Mode Privileged Exec

Related Topics ■ *Clearing BGP Attributes for L2VPNs Clearing BGP Attributes for VPLS in the JUNOS BGP and MPLS Configuration Guide*

clear ip bgp dampening

Syntax To clear IP-specific information for only the route-target address family:

```
clear ip bgp route-target signaling { dampening | flap-statistics } [ rtfPrefix
| rtfAddress ]
```

To clear IP-specific information for any case other than for the route-target address family:

```
clear ip bgp
[ vrf vrfName ] [ ipv4 unicast | ipv4 multicast | vprv4 unicast |
l2vpn all | l2vpn vpls vplsName | l2vpn vpws vpwsName ]
{ dampening | flap-statistics } [ ipAddress [ addressMask ] ]
```

Release Information Command introduced before JUNOS Release 7.1.0.
l2vpn keyword added in JUNOS Release 7.1.0.
vpls keyword and *vplsName* variable added in JUNOS Release 7.1.0.
all, **vpws**, and **route-target signaling** keywords and *rtMemNlri* and *vpwsName* variables added in JUNOS Release 8.2.0.
rtMemNlri variable replaced by two variables, *rtfAddress* and *rtfPrefix*, in JUNOS Release 9.1.0.

Description Clears IP route flap dampening information and reinstates the suppressed routes. The **dampening** keyword and the **flap-statistics** keyword both have the same effect. There is no **no** version.

- Options**
- route-target signaling—Clears the route-target membership information
 - *rtfPrefix*—Prefix representing the route-target membership NLRI (RT-MEM-NLRI), in the format *asNumber* : *extendedCommunity* / *prefixLength* (for example, 320:320:524/36) where:
 - *asNumber*—AS number for origin of route target information, in the range 1–4294967295
 - *extendedCommunity*—Two-part number in the format *number1*:*number2* that identifies an extended community of VPNs, in the format *number1* : *number2*, where:
 - *number1*—Autonomous system (AS) number, in the range 1–4294967295, or an IP address
 - *number2*—Unique integer, in the range 1–4294967295; 32 bits if *number1* is a 16-bit AS number; 16 bits if *number1* is an IP address or a 32-bit AS number
 - *prefixLength*—Number that specifies the length of the route prefix, in the range 32–96

- *rtfAddress*—*rtfPrefix* with a prefix length of 96; representing the route-target membership NLRI (RT-MEM-NLRI), in the format *asNumber: extendedCommunity* (for example, 320:320:524 or 320:50.2.3.4:524)
- *vrfName*—Name of a virtual routing and forwarding instance to clear
- *ipv4 unicast*—Clears the IPv4 unicast routing table; the default option
- *ipv4 multicast*—Clears the IPv4 multicast routing table
- *vpnv4 unicast*—Clears the VPNv4 unicast routing and forwarding table
- *l2vpn all*—Clears the L2VPN reachability information for all VPLS and VPWS instances in the L2VPN address family
- *l2vpn vpls vplsName*—Clears the L2VPN reachability information for the VPLS instance with the name *vplsName*
- *l2vpn vpws vpwsName*—Clears the L2VPN reachability information for the VPWS instance with the name *vpwsName*
- *ipAddress*—IP address of the BGP neighbor to clear
- *addressMask*—Address mask to be applied to the network IP address

Mode Privileged Exec

Related Topics ■ *Clearing BGP Attributes for L2VPNs and Clearing BGP Attributes for VPLS in the JUNOS BGP and MPLS Configuration Guide*

clear ip bgp dynamic-peers

Syntax clear ip bgp [*ipAddress* | *ipv6Address* | peer-group *peerGroupName*
| *] [vrf *vrfName*]
dynamic-peers

Release Information Command introduced before JUNOS Release 7.1.0.
ipv6Address variable added in JUNOS Release 8.0.0.

Description Removes all dynamic peers in the specified scope. There is no **no** version.

- Options**
- *ipAddress*—IP address of identified BGP neighbor to clear
 - *ipv6Address*—IPv6 address of identified BGP neighbor to clear
 - *peerGroupName*—Name of a BGP peer group to clear
 - *—Clears all connections
 - *vrfName*—Name of a virtual routing and forwarding instance to clear

Mode Privileged Exec

clear ip bgp redistribution

Syntax clear ip bgp [ipv4 { unicast | multicast }] redistribution

Release Information Command introduced before JUNOS Release 7.1.0.

Description Reapplies policy to routes that have been redistributed into BGP. There is no **no** version.

- Options**
- ipv4 unicast—Reapplies policy to redistributed IPv4 unicast routes
 - ipv4 multicast—Reapplies policy to redistributed IPv4 multicast routes

Mode Privileged Exec, User Exec

clear ip bgp wait-end-of-rib

Syntax clear ip bgp [*ipAddress* | *ipv6Address* | peer-group *peerGroupName* | *] [vrf *vrfName*] [ipv4 unicast | ipv4 multicast | vpnv4 unicast | l2vpn all | l2vpn vpls *vplsName* | l2vpn vpws *vpwsName* | route-target signaling] wait-end-of-rib

Release Information Command introduced before JUNOS Release 7.1.0.
l2vpn keyword added in JUNOS Release 7.1.0.
ipv6Address variable added in JUNOS Release 8.0.0.
route-target signaling keywords added in JUNOS Release 8.2.0.
all, **vpls**, and **vpws** keywords and *vplsName* and *vpwsName* variables added in JUNOS Release 9.3.0.

Description Brings down the underlying TCP connection and then brings it back up again, causing both peers to resend their complete BGP routing table, but clears the specified peer from the set of peers for which BGP is waiting to receive an End-of-RIB marker after a peer restart. Hard clearing a peer has the same effect for that peer. There is no **no** version.

- Options**
- *ipAddress*—IP address of identified BGP neighbor to clear
 - *ipv6Address*—IPv6 address of identified BGP neighbor to clear
 - *peerGroupName*—Name of a BGP peer group to clear
 - *—Clears all connections
 - *vrfName*—Name of a virtual routing and forwarding instance to clear
 - ipv4 unicast—Clears the IPv4 unicast routing table; the default option
 - ipv4 multicast—Clears the IPv4 multicast routing table
 - vpnv4 unicast—Clears the VPNv4 unicast routing and forwarding table
 - l2vpn all—Clears the L2VPN reachability information for all VPLS and VPWS instances in the L2VPN address family
 - l2vpn vpls *vplsName*—Clears the L2VPN reachability information for the VPLS instance with the name *vplsName*
 - l2vpn vpws *vpwsName*—Clears the L2VPN reachability information for the VPWS instance with the name *vpwsName*
 - route-target signaling—Clears the route-target membership information

Mode Privileged Exec

Related Topics ■ *Clearing BGP Attributes for L2VPNs and Clearing BGP Attributes for VPLS in the JUNOS BGP and MPLS Configuration Guide*

clear ip demux

Syntax clear ip demux

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears all dynamically created demultiplexer table entries associated with route-map processing of the **set ip source-prefix** command. There is no **no** version.

Mode Interface Configuration

clear ip dhcp-local binding

Syntax clear ip dhcp-local binding *ipAddress*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears the specified IP DHCP address binding. There is no **no** version.



NOTE: This command is deprecated and might be removed completely in a future release. The function provided by this command has been replaced by the **dhcp delete-binding** command.

Options ■ *ipAddress*—DHCP IP address binding to clear

Mode Privileged Exec

clear ip dvmrp routes

Syntax clear ip dvmrp routes [*ipAddress* [*addressMask*]]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears DVMRP routes from the routing table. There is no **no** version.

- Options**
- *ipAddress*—IP address for which longest match is cleared
 - *addressMask*—Address mask to be applied to the IP address

Mode Privileged Exec

clear ip flow stats

Syntax clear ip flow stats

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears all entries from all flow caches on the router. There is no **no** version.



CAUTION: Using this command may temporarily disrupt flow data collection.

Mode Privileged Exec

clear ip interface

Syntax `clear ip interface [vrf vrfName] interfaceType interfaceSpecifier`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears the counters on the specified IP interface. The default is all interface types and all interfaces. There is no **no** version.

- Options**
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec

clear ip isis redistribution

Syntax clear ip isis redistribution

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears all the routes that have previously been redistributed into IS-IS and redistributes them using the current policy configuration. There is no **no** version.

Mode Privileged Exec

clear ip mobile binding

Syntax clear ip mobile binding { nai { *user@realm* | *@realm* | *@* } | *ipAddress* | all }

Release Information Command introduced in JUNOS Release 9.0.0.

Description Clears the binding table in a virtual router or a specified binding determined by the mobile node home address or network access identifier (NAI). There is no **no** version.

- Options**
- *user@realm*—Name of the user for the mobile node specification when the **nai** keyword is specified, in the format *user@realm*, where *realm* is the domain name
 - *@realm*—Name of the user for the mobile node specification when the **nai** keyword is specified, in the format *@realm*, where *realm* is the domain name
 - *@*—Name of the user for the mobile node specification when the **nai** keyword is specified, in the format *@*
 - *ipAddress*—IP address of the home agent
 - *all*—Clears all the bindings in the binding table

Mode Privileged Exec

clear ip mroute

Syntax clear ip mroute { * | *grpAddress* [*sourceAddress*] }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears all or the specified multicast forwarding entries. There is no **no** version.

- Options**
- *—Clears all IP multicast forwarding entries
 - *grpAddress*—Address of the multicast group for which forwarding entries should be cleared
 - *sourceAddress*—Address of the multicast source for which forwarding entries should be cleared

Mode Privileged Exec, User Exec

clear ip nat translation

Syntax clear ip nat translation *

clear ip nat translation inside *insideGlobalIpAddress* *insideLocalIpAddress*

clear ip nat translation outside *outsideLocalIpAddress* *outsideGlobalIpAddress*

clear ip nat translation { icmp | tcp | udp }
inside *insideGlobalIpAddress* *insideGlobalPort* *insideLocalIpAddress* *insideLocalPort*

clear ip nat translation { gre | icmp | tcp | udp }
inside *insideGlobalIpAddress* * *insideLocalIpAddress* *

clear ip nat translation { icmp | tcp | udp }
inside *insideGlobalIpAddress* *insideGlobalPort* *insideLocalIpAddress* *insideLocalPort*
outside *outsideLocalIpAddress* *outsideLocalPort* *outsideGlobalIpAddress* *outsideGlobalPort*

Release Information Command introduced before JUNOS Release 7.1.0.
gre keyword added in JUNOS Release 7.3.0.

Description Clears all or the specified NAT table entries. There is no **no** version.

- Options**
- *—Clears all translations when used in the **clear ip nat translation** version of this command
 - *—Matches any global or local port to remove inside source extended GRE, ICMP, TCP, or UDP translations for the specified global IP address and local IP address when used in the **clear ip nat translation { gre | icmp | tcp | udp } inside *insideGlobalIpAddress* * *insideLocalIpAddress* *** version of this command
 - inside—Specifies an inside address
 - *insideGlobalIpAddress*—Inside global IP address
 - *insideLocalIpAddress*—Inside local IP address
 - outside—Specifies an outside address
 - *outsideLocalIpAddress*—Outside local IP address
 - *outsideGlobalIpAddress*—Outside global IP address
 - tcp—Specifies a TCP port translation
 - udp—Specifies a UDP port translation
 - icmp—Specifies an ICMP port translation
 - gre—Specifies a GRE translation
 - *insideGlobalPort*—Inside global port number
 - *insideLocalPort*—Inside local port number

- *outsideGlobalPort*—Outside global port number
- *outsideLocalPort*—Outside local port number

Mode Privileged Exec

clear ip ospf database

Syntax clear ip ospf database

Release Information Command introduced in JUNOS Release 7.1.0.

Description Deletes all entries from the OSPF link-state database and resets all adjacencies. There is no **no** version.

Mode Privileged Exec

clear ip ospf neighbor

Syntax clear ip ospf neighbor [*neighborAddress*]

Release Information Command introduced in JUNOS Release 7.1.0.

Description Clears or resets adjacency with a specified neighbor session. There is no **no** version.



NOTE: When OSPF is configured and running over an NBMA network, do not issue the **clear ip ospf neighbor** command simultaneously on both ends of the OSPF link. Doing so brings the OSPF link down completely. In this event, you must do one of the following on both sides of the link to bring the link back up:

- Reconfigure the OSPF neighbors on the NBMA interface with the **neighbor** command.
 - Issue the **clear ip ospf database** command to clear and reset the OSPF adjacencies.
 - Issue the **shutdown** command followed by the **no shutdown** command on the interface.
-

Options ■ *neighborAddress*—IP address of identified neighbor to clear or reset

Mode Privileged Exec

clear ip ospf redistribution

Syntax clear ip ospf redistribution

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears and readvertises all of the routes that have been previously redistributed into OSPF. Exercise caution when using this command as it purges all external LSAs and reoriginates. There is no **no** version.

Mode Privileged Exec

clear ip pim auto-rp

Syntax clear ip pim auto-rp [*ipAddress*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears the group-to-RP router mappings the router learned via autoRP. There is no **no** version.

Options ■ *ipAddress*—IP address of the router designated as an RP router

Mode Privileged Exec, User Exec

clear ip pim interface count

Syntax clear ip pim interface [*interfaceType interfaceSpecifier*] count

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears the counters for multicast packet statistics on all interfaces or the specified interface. There is no **no** version.

Options

- *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec, User Exec

clear ip pim remote-neighbor count

Syntax clear ip pim remote-neighbor [*ipAddress*] count

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears the counters for remote neighbor statistics on all interfaces or the specified interface. There is no **no** version.



NOTE: This command is typically used when you configure PIM remote neighbors to run multicast services over BGP/MPLS VPNs. That functionality is no longer supported.

Options ■ *ipAddress*—IP address of the interface

Mode Privileged Exec, User Exec

clear ip prefix-list

Syntax clear ip prefix-list [*listName* [*network/length*]]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears all hit counts in the prefix lists, the specified prefix list, or the specified entry from the specified prefix list. There is no **no** version.

- Options**
- *listName*—Name of the prefix list; string of up to 32 characters
 - *network*—Base address of the network route to be filtered; for example, 192.168.32.0 or 10.10.0.0
 - *length*—Length of the network prefix; number of bits masking base address to produce address to be matched

Mode Privileged Exec, User Exec

clear ip prefix-tree

Syntax clear ip prefix-tree [*treeName* [*network/length*]]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears all prefix trees, the specified prefix tree, or the specified entry from the specified prefix tree. There is no **no** version.

- Options**
- *treeName*—Name of the prefix list; string of up to 32 characters
 - *network*—Base address of the network route to be filtered; for example, 192.168.32.0 or 10.10.0.0
 - *length*—Length of the network prefix; number of bits masking base address to produce address to be matched

Mode Privileged Exec, User Exec

clear ip rip dynamic-interfaces

Syntax clear ip rip dynamic-interfaces

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears all existing dynamic, unnumbered interfaces that were created since issuing the **ip rip copy-to-dynamic** command. There is no **no** version.

Mode Privileged Exec, User Exec

clear ip rip redistribution

Syntax clear ip rip redistribution

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears all the routes that have previously been redistributed into RIP. There is no **no** version.

Mode Privileged Exec, User Exec

clear ip routes

Syntax clear ip routes [vrf *vrfName*] { * | *ipAddress ipMask* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears a specified route or all dynamic routes from the routing table of a specified VRF or all VRFs. There is no **no** version.

- Options**
- *vrfName*—Name of the VRF context from which routes are to be cleared
 - *—Clears all dynamic routes
 - *ipAddress*—IP address prefix for routes that are cleared; in 32-bit dotted-decimal format
 - *ipMask*—Mask of the IP address prefix for routes that are cleared; in 32-bit dotted-decimal format

Mode Privileged Exec

clear ip routes download

Syntax For a specific VRF

```
clear ip routes download [ vrf vrfName ] { ipAddress ipMask | * }
```

For all virtual routers

```
clear ip routes download { all | reload }
```

Release Information Command introduced in JUNOS Release 8.1.0.

Description Synchronizes downloaded access routes and the routes installed in the routing table. This command has no effect if a download operation is in progress. There is no **no** version.

- Options**
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters; the current virtual router is used by default
 - *ipAddress*—IP address prefix to clear
 - *ipMask*—Network mask of the IP address prefix to clear
 - *—Clears all dynamic routes that are installed in the routing table of the current virtual router or specified VRF
 - all—Clears all downloaded routes that are installed in the routing tables of all virtual routers and VRFs.
 - reload—Performs a route download operation, then clears all downloaded routes from the routing tables in all virtual routers and VRFs.

Mode Privileged Exec

clear ip tunnel-routes

Syntax clear ip tunnel-routes [vrf *vrfName*] { * | *ipAddress ipMask* }

Release Information Command introduced in JUNOS Release 7.1.0.

Description Clears and then refreshes a specified route or all dynamic routes from the tunnel routing table of the virtual router or a specified VRF. There is no **no** version.

- Options**
- *vrfName*—Name of the VRF context from which routes are to be cleared
 - *—Clears all dynamic routes
 - *ipAddress*—IP address prefix for routes that are cleared; in 32-bit dotted-decimal format
 - *ipMask*—Mask of the IP address prefix for routes that are cleared; in 32-bit dotted-decimal or /N format

Mode Privileged Exec

clear ipv6 access-list

Syntax clear ipv6 access-list [*accessListName*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears counters for entries in IP access lists. There is no **no** version.

Options ■ *accessListName*—Name of the access list; a string of up to 32 characters

Mode Privileged Exec

clear ipv6 bfd session

Syntax clear ipv6 bfd session [address *ipv6Address*]

Release Information Command introduced in JUNOS Release 7.1.0.

Description Restarts all IPv6 BFD sessions or a specified BFD session. There is no **no** version.

Options ■ *ipAddress*—IP address of the destination to which the session has been established

Mode Privileged Exec, User Exec

clear ipv6 interface

Syntax clear ipv6 interface *interfaceType interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears the counters on the specified IPv6 interface. The default is all interface types and all interfaces. There is no **no** version.

- Options**
- *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec

clear ipv6 mroute

Syntax clear ipv6 mroute { * | *grpAddress* [*sourceAddress*] }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears all or the specified IPv6 multicast forwarding entries. There is no **no** version.

- Options**
- *—Clears all IPv6 multicast forwarding entries
 - *grpAddress*—Address of the multicast group for which forwarding entries should be cleared
 - *sourceAddress*—Address of the multicast source for which forwarding entries should be cleared

Mode Privileged Exec, User Exec

clear ipv6 neighbors

Syntax clear ipv6 neighbors [include-statics | statics-only]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears all IPv6 dynamic neighbors. The **include-statics** keyword clears both dynamic neighbors and static neighbors. The **statics-only** keyword clears only IPv6 static neighbors. There is no **no** version.

- Options**
- include-statics—Clears both dynamic and static neighbors
 - statics-only—Clears only static neighbors

Mode Privileged Exec

clear ipv6 ospf counters

Syntax clear ipv6 ospf [*processId*] counters

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears all OSPF IPv6 statistical counters for the virtual router. There is no **no** version.

Options ■ *processId*—Number in the range 1–65535 that identifies the OSPF process

Mode Privileged Exec

clear ipv6 ospf process

Syntax clear ipv6 ospf [*processId*] process

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears the OSPF IPv6 process on the virtual router. There is no **no** version.

Options ■ *processId*—Number in the range 1–65535 that identifies the OSPF process

Mode Privileged Exec

clear ipv6 ospf redistribution

Syntax clear ipv6 ospf redistribution

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears and readvertise all of the routes that have been previously redistributed into OSPF. Exercise caution when using this command as it purges all external LSAs and reoriginates. There is no **no** version.

Mode Privileged Exec

clear ipv6 pim interface

Syntax clear ipv6 pim interface [*interfaceType interfaceSpecifier*] count

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears the counters for multicast packet statistics on all IPv6 interfaces or the specified IPv6 interface. There is no **no** version.

- Options**
- *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec, User Exec

clear ipv6 pim remote-neighbor

Syntax clear ipv6 pim remote-neighbor [*ipv6Address*] count

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears the counters for remote neighbor statistics on all IPv6 interfaces or the specified IPv6 interface. There is no **no** version.

Options ■ *ipv6Address*—IPv6 address of the interface

Mode Privileged Exec, User Exec

clear ipv6 prefix-list

Syntax clear ipv6 prefix-list [*listName* [*network/length*]]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears all hit counts in all IPv6 prefix lists, the specified prefix list, or the specified entry from the specified prefix list. There is no **no** version.

- Options**
- *listName*—Name of the IPv6 prefix list; string of up to 32 characters
 - *network*—Base address of the network route to be filtered; for example, ::ffff:a:b:c:d
 - *length*—Length of the network prefix; number of bits masking base address to produce address to be matched

Mode Privileged Exec, User Exec

clear ipv6 routes

Syntax clear ipv6 routes [*ipv6Prefix* | *]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears IPv6 routes. To clear the routes for a specific IPv6 network, specify the IPv6 prefix. To clear all dynamic IPv6 routes, use the * (asterisk) option. There is no **no** version.

- Options**
- *ipv6Prefix*—IPv6 network for which to clear route information
 - *—Clears all dynamic IPv6 routes

Mode Privileged Exec

clear ipv6 tunnel-routes

Syntax clear ipv6 tunnel-routes [*ipv6Prefix* | *]

Release Information Command introduced in JUNOS Release 7.1.0.

Description Clears and then refreshes IPv6 routes from the tunnel routing table. To clear the routes for a specific IPv6 network, specify the IPv6 prefix. To clear all dynamic IPv6 routes, use the * (asterisk) option. There is no **no** version.

- Options**
- *ipv6Prefix*—IPv6 network for which to clear route information
 - *—Clears all dynamic IPv6 routes

Mode Privileged Exec

clear isis adjacency

Syntax clear isis adjacency [*systemId* | *hostname*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears all entries from the adjacency database, or clears only adjacencies with a specified neighbor. There is no **no** version.

Options

- *systemID*—System ID of an IS-IS neighbor
- *hostname*—Hostname of an IS-IS neighbor

Mode Privileged Exec

clear isis database

Syntax clear isis database [*systemId* | *hostname*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears all entries from the IS-IS link-state database, or clears only entries associated with a specified neighbor. There is no **no** version.

- Options**
- *systemId*—System ID of an IS-IS neighbor
 - *hostname*—Hostname of an IS-IS neighbor

Mode Privileged Exec

clear isis ipv6 redistribution

Syntax clear isis ipv6 redistribution

Release Information Command introduced in JUNOS Release 8.2.0.

Description Clears all the IPv6 routes that have previously been redistributed into IS-IS and redistributes them using the current policy configuration. There is no **no** version.

Mode Privileged Exec

clear l2c discovery-table

Syntax clear l2c discovery-table { neighbor *neighborName* | end-user-id *userId* | neighbor *neighborName* end-user-id *userId* }

Release Information Command introduced in JUNOS Release 7.2.0.

Description Clears all entries or a specified entry from the topology discovery table. There is no **no** version.

- Options**
- *neighborName*—Name of the neighbor you want to reset
 - *userId*—User ID you want to reset

Mode Privileged Exec

clear l2c neighbor

Syntax clear l2c neighbor *neighborName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Resets the specified GSMP neighbor session. There is no **no** version.

Options ■ *neighborName*—Name of the neighbor you want to reset

Mode Privileged Exec

clear line

Syntax clear line { *absoluteLine* | *cliType relativeLine* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Removes all services on any line on the system and closes any files opened as a result of services on that line. There is no **no** version.

- Options**
- *absoluteLine*—Absolute number of the line to which the user is connected; see the line number field in the **show users** command output
 - *cliType*—One of the following types of lines:
 - console
 - vty
 - *relativeLine*—Relative number for a line; see the line name field in the **show users** command output

Mode User Exec

clear mirror log

Syntax clear mirror log

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears all log entries for packet mirroring operations. By default, you must have CLI user access level 13 or above to use this command; an administrator can modify the user access level requirement. There is no **no** version.

Mode Privileged Exec, User Exec

Related Topics

- Monitoring Packet Mirroring Overview
- Logging Packet Mirroring Information

clear mpls dynamic-interfaces on-major-interfaces

Syntax clear mpls dynamic-interfaces [ip | ipv6] on-major-interfaces
[*interfaceType interfaceSpecifier*]

Release Information Command introduced in JUNOS Release 7.2.0.

Description Removes and re-creates both dynamic IPv4 interfaces and dynamic IPv6 interfaces that are on top of all MPLS major interfaces or on top of the specified MPLS major interface. There is no **no** version.

- Options**
- ip—Specifies that only IPv4 dynamic interfaces are removed and re-created
 - ipv6—Specifies that only IPv6 dynamic interfaces are removed and re-created
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec

clear mpls ldp

Syntax clear mpls ldp [prefix *destAddr* [*maskLen* | *mask*] | neighbor [*neighborAddress*]]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Removes and reestablishes existing LDP LSPs, thereby forcing the reapplication of policies on the reestablished topology-driven LDP LSPs. You can clear all LDP LSPs or limit the clearance to only LSPs to a specified prefix or neighbor. Affects the data traffic on LSPs that are in use when the command is issued. There is no **no** version.

- Options**
- *destAddr*—IP address of the prefix to be cleared
 - *maskLen*—Length of the prefix to be cleared; number in the range 0–32
 - *mask*—Mask for the prefix to be cleared
 - *neighborAddress*—IP address of a neighbor 32-bit dotted-decimal format of the entry to be cleared

Mode Privileged Exec

clear redundancy history

Syntax clear redundancy history

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears the high availability switchover history for the router. There is no **no** version.

Mode Privileged Exec

clear rsvp authentication

Syntax clear { ip | mpls } rsvp authentication [*ipAddress*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Clears the security association and resets the sequence number on the receiving peer for the specified sending peer. There is no **no** version.

- Options**
- ip—Specifies keyword for compatibility with non-E Series implementations
 - mpls—Indicates JUNOS MPLS implementation
 - *ipAddress*—IP address of sending peer

Mode Privileged Exec

clear suspicious-control-flow-detection

Syntax clear suspicious-control-flow-detection
 [interface *interfaceSpecifier* protocol *protocolValue* address *ethernetAddress* slot
slotNumber]

Release Information Command introduced in JUNOS Release 7.3.0.

Description Clears one or more suspicious flows. If you do not specify a slot, interface, or IP address, clears all suspicious flows. If you specify a slot, clears all specified suspicious flows on that slot. If you specify an interface and protocol, clears flows that are identified down to the Ethernet mac address level. There is **no no** version.

- Options**
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *protocolValue*—Name of the protocol to be cleared
 - *ethernetAddress*—Ethernet address to be cleared
 - *slotNumber*—Number of the slot to be cleared

Mode Privileged Exec, User Exec

client-name

Syntax client-name *clientname*
 no client-name

Release Information Command introduced before JUNOS Release 7.1.0.

Description From Domain Map Tunnel Configuration or Tunnel Group Tunnel Configuration mode, sets a hostname for a tunnel that the LAC uses when communicating with the LNS about the tunnel. The **no** version removes the hostname from the tunnel.



NOTE: In Domain Map Tunnel Configuration mode, this command is replacing the **hostname** command. The **hostname** command may be removed completely from Domain Map Tunnel Configuration mode in a future release.

Options ■ *clientname*—String of up to 64 characters (no spaces)

Mode Domain Map Tunnel Configuration, Tunnel Group Tunnel Configuration

clns configuration-time

Syntax clns configuration-time *configTime*
 no clns configuration-time

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the rate at which ES hellos and IS hellos are sent. The **no** version restores the default value, 10 seconds.

Options ■ *configTime*—Number in the range 1–65535; rate in seconds at which ES and IS hello packets are sent; default value is 10 seconds

Mode Global Configuration

clns holding-time

Syntax clns holding-time *holdTime*
 no clns holding-time

Release Information Command introduced before JUNOS Release 7.1.0.

Description Allows the sender of an ES hello or IS hello to specify the length of time you consider the information in the hello packets to be valid. The **no** version restores the default value, 30 seconds.

Options ■ *holdTime*—Number in the range 1–65535; length of time in seconds during which the information in the hello packets is considered valid

Mode Global Configuration

clns host

Syntax `clns host name nsap`
`no clns host name`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a name-to-NSAP mapping that can then be used with commands requiring NSAPs. Enables dynamic resolution of hostnames to system IDs (within the NSAP address). The hostname mapping is sent in the LSPs within the dynamic hostname TLV tuple. Display the TLV by issuing the **show isis database detail** command. Use the **show hosts** command to display the mapping. The **no** version restores the default of no mapping defined.

Options ■ *name*—Name for the NSAP; first character can be either a letter or a number. If a number is used, the operations you can perform are limited.
 ■ *nsap*—NSAP to which that name maps

Mode Global Configuration

clock set

Syntax clock set *time* { *month day* | day month } *year*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Allows you to manually set the system clock. There is no **no** version.

- Options**
- *time*—Current time (in 24-hour format – *HH:MM:SS*)
 - *month*—Name of the month (January, February, ...)
 - *day*—Day of the month (1–31)
 - *year*—Year (2000, 2001, ...)

Mode Privileged Exec

clock source

Syntax clock source { line | internal { module | chassis } }
no clock source

Release Information Command introduced before JUNOS Release 7.1.0.

Description Determines how an interfaces obtains clocking signals. The **no** version restores the default value, **line**.

- Options**
- line—Interface clocks data from a clock recovered from the line's receive data stream; the default.
 - internal—Internal clock source transmits data from its internal clock. You must specify one of the following for internal clocking:
 - module—Internal clock is from the line module itself
 - chassis—Internal clock is from the configured system clock

Mode Controller Configuration, Interface Configuration (POS only)

clock summer-time date

Syntax clock summer-time name date { *startDay startMonth* | *startMonth startDay* }
startYear startTime { *stopDay stopMonth* | *stopMonth stopDay* }
stopYear stopTime [*dstOffset*]

no clock summer-time

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the router to automatically switch to summer time (Daylight Saving Time—DST). It should start on the first specific date listed in the command and end on the second specific date in the command. The **no** version configures the software so that it does not automatically switch to summer time.

- Options**
- *name*—Name of the time zone (for example, PDT) to be displayed when daylight saving (summer) time is in effect
 - *date*—Indicates that summer time should start on the first specific date listed in the command and end on the second specific date in the command
 - *startDay*—DST start day (1–31)
 - *startMonth*—DST start month (January, February, ...)
 - *startYear*—DST start year (2000, 2001, ...)
 - *startTime*—DST start time (24-hour format) in hours and minutes (hh:mm)
 - *stopDay*—DST stop day
 - *stopMonth*—DST stop month
 - *stopYear*—DST stop year
 - *stopTime*—DST stop time (24-hour format)
 - *dstOffset*—Number of minutes to add during summer time in the range 1–1440; default = 60

Mode Global Configuration

clock summer-time recurring

Syntax clock summer-time name recurring [{ *startWeekNumber* | *startWeekEnum* } *startDay* *startMonth* *startTime* { *stopWeekNumber* | *stopWeekEnum* } *stopDay* *stopMonth* *stopTime* [*dstOffset*]]

no clock summer-time

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the router to automatically switch to summer time (Daylight Saving Time) on the specified dates every year. The **no** version configures the software not to automatically switch to summer time.

- Options**
- *name*—Name of the time zone (for example, EDT for Eastern Daylight Savings Time) to be displayed when daylight saving (summer) time is in effect
 - *recurring*—Indicates that summer time should start and end on the specified days every year
 - *startWeekNumber*—DST start week of the month (1–5)
 - *startWeekEnum*—First week in month (first); or last week in month (last)
 - *startDay*—DST start day of the week (Sunday, Monday, ...)
 - *startMonth*—DST start month (January, February, ...)
 - *startTime*—DST start time (24-hour format) in hours and minutes (hh:mm)
 - *stopWeekNumber*—DST stop week of the month (1–5)
 - *stopWeekEnum*—First week in month (first); or last week in month (last)
 - *stopDay*—DST stop day of the week
 - *stopMonth*—DST stop month
 - *stopTime*—DST stop time in hours and minutes (hh:mm)
 - *dstOffset*—Number of minutes to add during summer time in the range 1–1440; default = 60

Mode Global Configuration

clock timezone

Syntax clock timezone *name hours* [*minutes*]
 no clock timezone

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the time zone for display. The **no** version sets the time zone to UTC.

- Options**
- *name*—Name of the time zone to be displayed when Standard time is in effect, such as EST or PST.
 - *hours*—Hours offset from UTC (-23, -22 ... 23)
 - *minutes*—Minutes offset from UTC (0–59)

Mode Global Configuration

color

Syntax [no] [suspend] color { green | yellow | red }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a policy rule that assigns a color to packets defined in the current classifier control list. The **no** version removes the rule from the policy list; the **suspend** version temporarily suspends the policy rule; the **no suspend** version resumes application of a suspended rule.



NOTE: This command replaces the Policy List Configuration mode version of the **color** command, which may be removed completely in a future release.

- Options**
- green—Assigns green color to packets; highest precedence
 - yellow—Assigns yellow color to packets; intermediate precedence
 - red—Assigns red color to packets; lowest precedence

Mode Classifier Group Configuration

- Related Topics**
- Hierarchical Rate Limits Overview
 - Policy Rule Precedence

color-aware

Syntax [no] color-aware

Release Information Command introduced in JUNOS Release 7.2.0.

Description Configures rate-limit profile to operate in color-aware mode. (Supported only on hierarchical rate limits.) Color-aware rate limits can change the algorithm used depending on the color of the incoming packet, which might have been set in the previous rate limit, in a policy action, or in an earlier policy. The **no** version restores the default value, which is not color-aware.

Mode Rate Limit Profile Configuration

Related Topics ■ Creating a Two-Rate Rate-Limit Profile

color-mark-profile

Syntax [no] [ip | ipv6 | mpls] color-mark-profile *profileName*

Release Information Command introduced in JUNOS Release 7.2.0.

Description Translates the packet color (independent of its type) to a type-dependent mark (for ToS or EXP), which is applied to a packet after it has exited a rate-limit hierarchy. If translation is not configured for a color, then packets of that color are not changed. The **no** version deletes the color-mark profile.

Options ■ *profileName*—Name of the rate-limit profile to be used in a policy (up to 40 alphanumeric characters)

Mode Color Mark Profile Configuration, Global Configuration

Related Topics ■ Hierarchical Rate Limits Overview
■ Policy Rule Precedence

committed-action

Syntax For IP and IPv6 rate-limit profiles:

```
[ no ] committed-action { drop | transmit | mark markVal }
```

For L2TP rate-limit profiles:

```
[ no ] committed-action { drop | transmit }
```

For MPLS rate-limit profiles:

```
[ no ] committed-action { drop | transmit | mark-exp expValue }
```

For hierarchical rate-limit profiles:

```
[ no ] committed-action { drop | transmit [ conditional | unconditional | final ] }
```

Release Information Command introduced before JUNOS Release 7.1.0.
conditional, **unconditional**, and **final** keywords added in JUNOS Release 7.2.0.

Description Sets the action for packets conforming to the committed rate and committed burst size and conforming to the exceed rate and exceed burst size for a rate-limit profile. The **no** version restores the value to the default value, drop.

- Options**
- drop—Drops the packet
 - transmit—Transmits the packet; for hierarchical rate limits:
 - conditional—Packets must pass the next rate limit
 - unconditional—Packets take resources, but are not affected by the rest of the hierarchy
 - final—Packets exit the hierarchy at rate limit
 - *markVal*—Value in the range 0–255
 - *expValue*—EXP bit value in the range 0–7

Mode Rate Limit Profile Configuration

Related Topics

- Creating a Two-Rate Rate-Limit Profile

committed-burst

Syntax committed-burst { *size* | millisecond *milliseconds* }
no committed-burst

Release Information Command introduced before JUNOS Release 7.1.0.
milliseconds variable added in JUNOS Release 8.1.0.

Description Sets the committed burst for a rate limit profile. The **no** version restores the default value, 100 ms; if 100ms is less than 8K, then 8K (8192).

- Options**
- *size*—Size in bytes in the range 1–4294967295
 - *milliseconds*—Milliseconds in the range 1–10000

Mode Rate Limit Profile Configuration

Related Topics

- Creating a Two-Rate Rate-Limit Profile

committed-drop-threshold

Syntax committed-drop-threshold *committedDropThreshold*
no committed-drop-threshold

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the threshold above which committed-drop-events are logged. The **no** version removes the threshold.

Options ■ *committedDropThreshold*—Bits per second in the range 0–1073741824

Mode Statistics Profile Configuration

Related Topics ■ Configuring Event Statistics

committed-length

Syntax committed-length *minimumCommittedLength* [*maximumCommittedLength*]
no committed-length

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets minimum and maximum constraints for the queue's committed lengths. The **no** version removes constraints on the queue's committed length.

- Options**
- *minimumCommittedLength*—Range 0–1073741824
 - *maximumCommittedLength*—Range 0–1073741824

Mode Queue Profile Configuration

Related Topics

- Configuring Queue Profiles to Manage Buffers and Thresholds

committed-rate

Syntax committed-rate { *rate* | *parameterName* percentage *percentValue* }
no committed-rate

Release Information Command introduced before JUNOS Release 7.1.0.
parameterName and *percentValue* variables added in JUNOS Release 8.1.0.

Description Sets the committed rate for a rate-limit profile as a specified value or as a percentage of a reference rate defined in the specified policy parameter. The **no** version restores the default value, 0.

- Options**
- *rate*—Rate in bits per second in the range 0–4294967295
 - *parameterName*—Name of policy parameter up to 40 characters
 - *percentValue*—Percentage in the range 0–100

Mode Rate Limit Profile Configuration

- Related Topics**
- Creating a Two-Rate Rate-Limit Profile
 - Setting the Committed Rate for a Rate-Limit Profile

committed-threshold

Syntax committed-threshold { percent *MinThresholdPercent* *MaxThresholdPercent* | *MinThresholdBytes* *MaxThresholdBytes* } *MaxDropProbability*

no committed-threshold

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the committed queue thresholds and maximum drop probability. The **no** version removes committed threshold.

- Options**
- percent—Specifies committed queue thresholds as percentages
 - *MinThresholdPercent*—Minimum queue threshold as a percentage of queue length
 - *MaxThresholdPercent*—Maximum queue threshold as a percentage of queue length
 - *MinThresholdBytes*—Minimum queue threshold in bytes
 - *MaxThresholdBytes*—Maximum queue threshold in bytes
 - *MaxDropProbability*—Maximum drop probability

Mode Drop Profile Configuration

- Related Topics**
- Configuring RED
 - Configuring WRED

common-name

Syntax [no] common-name *commonName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a common name used to generate certificate requests. The **no** version removes the common name.

Options ■ *commonName*—Name of up to 60 characters

Mode IPSec Identity Configuration

configure

Syntax configure [terminal | file [*fileName*] [verbose | show-progress [*dotPeriod*]]]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enters Global Configuration mode. There is no **no** version.



NOTE: This command is not allowed for a short time after a warm restart (warm switchover) occurs. This behavior allows some applications time to complete their warm-restart initialization. However, if the warm-restart does not complete in 5 minutes, the warm-start is cancelled and configuration access is restored.

- Options**
- terminal—Enables manual configuration from a terminal
 - file—Configures the router from a script file
 - *fileName*—Script file to execute
 - verbose—Echoes each command as the script is executed
 - show-progress—Displays a '.' during script execution
 - *dotPeriod*—Number of commands executed before a '.' is displayed; default value is 100

Mode Privileged Exec

confirmations explicit

Syntax [no] confirmations explicit

Release Information Command introduced before JUNOS Release 7.1.0.

Description Requires the user to enter **y**, **ye**, or **yes** to confirm a prompt, and to enter **n** or **no** to deny a prompt. The **no** version restores the default state, which permits pressing <Enter> or <y> to confirm a prompt and entering any other characters to deny a prompt.

Mode Global Configuration

conformed-action

Syntax For IP and IPv6 rate-limit profiles:

```
[ no ] conformed-action { drop | transmit | mark markVal }
```

For L2TP rate-limit profiles:

```
[ no ] conformed-action { drop | transmit }
```

For MPLS rate-limit profiles:

```
[ no ] conformed-action { drop | transmit | mark-exp expValue }
```

For hierarchical rate-limit profiles:

```
[ no ] conformed-action { drop | transmit [ conditional | unconditional | final ] }
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the action for packets not conforming to the committed rate and committed burst size, but conforming to the peak rate and peak burst size for a rate-limit profile. The **no** version restores the value to the default value, drop.

- Options**
- drop—Drops the packet
 - transmit—Transmits the packet; for hierarchical rate limits:
 - conditional—Packets must pass the next rate limit
 - unconditional—Packets take resources, but are not affected by the rest of the hierarchy
 - final—Packets exit the hierarchy at rate limit
 - *markVal*—Value in the range 0–255
 - *expValue*—EXP bit value in the range 0–7

Mode Rate Limit Profile Configuration

Related Topics

- Creating a Two-Rate Rate-Limit Profile

conformed-drop-threshold

Syntax conformed-drop-threshold *conformedDropThreshold*
 no conformed-drop-threshold

Release Information Command introduced before JUNOS Release 7.1.0.
 conditional, **unconditional**, and **final** keywords added in JUNOS Release 7.2.0.

Description Configures the threshold above which conformed-drop-events are logged. The **no** version removes the threshold.

Options ■ *conformedDropThreshold*—Bits per second in the range 0–1073741824

Mode Statistics Profile Configuration

Related Topics ■ Configuring Event Statistics

conformed-fraction

Syntax conformed-fraction *conformedFraction*
no conformed-fraction

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the percentage of the total queue that can be occupied before dropping conformed packets. The **no** version returns the conformed fraction to its default setting.

Options ■ *conformedFraction*—Percentage in the range 0–100; default value is 50

Mode Queue Profile Configuration

Related Topics ■ [Configuring Queue Profiles to Manage Buffers and Thresholds](#)

conformed-length

Syntax conformed-length *minimumConformedLength* [*maximumConformedLength*]
 no conformed-length

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets minimum and maximum constraints for the queue's conformed lengths. The **no** version removes constraints on the queue's conformed length.

- Options** ■ *minimumConformedLength*—Number in the range 0–1073741824
 ■ *maximumConformedLength*—Number in the range 0–1073741824

Mode Queue Profile Configuration

- Related Topics** ■ Configuring Queue Profiles to Manage Buffers and Thresholds

conformed-threshold

Syntax conformed-threshold { percent *MinThresholdPercent* *MaxThresholdPercent* | *MinThresholdBytes* *MaxThresholdBytes* } *MaxDropProbability*

no conformed-threshold

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the conformed queue thresholds and maximum drop probability. The **no** version removes conformed threshold.

- Options**
- percent—Specifies conformed queue thresholds as percentages
 - *MinThresholdPercent*—Minimum queue threshold as a percentage of queue length
 - *MaxThresholdPercent*—Maximum queue threshold as a percentage of queue length
 - *MinThresholdBytes*—Minimum queue threshold in bytes
 - *MaxThresholdBytes*—Maximum queue threshold in bytes
 - *MaxDropProbability*—Maximum drop probability

Mode Drop Profile Configuration

- Related Topics**
- Configuring RED
 - Configuring WRED

control-plane

Syntax control-plane

Release Information Command introduced in JUNOS Release 8.0.0.

Description Enters Control Plane Configuration mode. There is no **no** version.

Mode Global Configuration

Related Topics ■ Rate-Limiting Traffic Flows

controlled-interface-type

Syntax controlled-interface-type { *controlledInterfaceType* | set | superset }
 no controlled-interface-type { *controlledInterfaceType* | all }

Release Information Command introduced in JUNOS Release 7.1.0.
 set and **superset** keywords added in JUNOS Release 9.2.0.

Description Assigns controlled-interface types to a QoS parameter definition. Controlled-interface types specify the types of logical interfaces whose queues and nodes can be controlled by instances of the parameter definition. You can specify up to four controlled-interface types for each parameter definition. The **no** version removes the controlled-interface type from the parameter definition.

- Options**
- *controlledInterfaceType*—One of the following controlled-interface types: atm, atm-vc, atm-vp, bridge, ethernet, fr-vc, ip, ip-tunnel, ipv6, l2tp-session, l2tp-tunnel, lsp, serial, svlan, server-port, vlan
 - set—Specifies an interface set as a controlled-interface type
 - superset—Specifies an interface superset as a controlled-interface type
 - all—Removes all controlled-interface types

Mode QoS Parameter Definition

- Related Topics**
- Configuring a Basic Parameter Definition for QoS Administrators
 - Creating a QoS Parameter on an Interface Superset or Interface Set

controller e3

Syntax `controller e3 interfaceSpecifier`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Accesses Controller Configuration mode so that you can configure an E3 controller. There is no **no** version.

Options ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Global Configuration

controller sonet

Syntax controller sonet *interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Selects an interface on which you want to configure SONET or SDH. There is no **no** version.

Options ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Global Configuration

controller t3

Syntax `controller t3 interfaceSpecifier`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Accesses Controller Configuration mode so that you can configure a T3 controller. There is no **no** version.

Options ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Global Configuration

convergence-factor

Syntax `convergence-factor convergenceFactor`
 `no convergence-factor`

Release Information Command introduced in JUNOS Release 8.0.0.

Description Specifies the convergence factor for all simple shared shapers on the router. The convergence factor determines how quickly the dynamic shaping rate converges with the calculated dynamic shaping rate, and is expressed as a percentage of the available bandwidth. The **no** version removes the specified convergence factor from all simple shared shapers on the router.

Options ■ *convergenceFactor*—Percentage value in the range 0–99; default value is 50

Mode QoS Shared Shaper Control Configuration

Related Topics ■ [Configuring Simple Shared Shaper Algorithm Variables](#)

copy

Syntax `copy [sourcePath]sourceFilename [destinationPath]destinationFilename [force]`

Release Information Command introduced before JUNOS Release 7.1.0.
hostName and *deviceName* variables added in JUNOS Release 7.2.0.

Description Copies a local or network file. There is no **no** version.



NOTE: You cannot change the extension of a file, for example, from .mac to .scr. You can copy software release (.rel) files only *to* the router (download); you cannot copy them *from* the router (upload). See *Copying and Redirecting Files* in the *JUNOS System Basics Configuration Guide*, for detailed information on file type usage with the **copy** command.

- Options**
- *sourcePath*—Path to the source in the format:
hostName: | *deviceName*: | /incoming/subdirectory/ | /outgoing/subdirectory/
 - *hostName*:—Name of the network host
 - *deviceName*:—Name of the device specifying a flash card slot
 - *disk0*—Specifies flash card slot 0 on the primary SRP module; if no device is specified for the primary SRP module, then *disk0* is used
 - *disk1*—Specifies flash card slot 1 on the primary SRP module; source and destination file types must be .dmp; supported only on the E120 and E320 routers
 - *standby*—Specifies flash card slot 0 on the standby SRP module for backward compatibility
 - *standby-disk0*—Specifies flash card slot 0 on the standby SRP module
 - *standby-disk1*—Specifies flash card slot 1 on the standby SRP module; source and destination file types must be .dmp; supported only on the E120 and E320 routers
 - *incoming*—Specifies the router's incoming FTP directory
 - *subdirectory*—Name of a subdirectory on the router's FTP server. If the subdirectory does not exist, the router creates it.
 - *outgoing*—Specifies the router's outgoing FTP directory
 - *sourceFilename*—Name of the the source file
 - *destinationPath*—Path to the destination in the format:
networkPath | /incoming/subdirectory | /outgoing/subdirectory

- *networkPath*—Path to the network host
- *incoming*—Specifies the incoming router's FTP directory
- *subdirectory*—Name of a subdirectory on the *ERX* router's FTP server. If the subdirectory does not exist, the router creates it.
- *outgoing*—Specifies the router's outgoing FTP directory
- *destinationFilename*—Name of the destination file
- *force*—Forces a copy, even when the destination file already exists; if a file is marked by the file system as in use because it is required for the current operation or configuration, the **force** keyword cannot force a copy of that file

Mode Privileged Exec

copy running-configuration

Syntax copy running-configuration *destination* [force] [include-text-config]

Release Information Command introduced before JUNOS Release 7.1.0.
include-text-config keyword added in JUNOS Release 9.1.0.

Description Saves the configuration currently running on the router to a local or remote (network) router configuration file (.cnf) in compressed format. Available only if the router is in Automatic Commit mode. There is no **no** version.

- Options**
- *destination*—Destination filename (*.cnf)
 - *force*—Creates a copy even when the destination file already exists
 - *include-text-config*—Generates the .cnf file, including the text configuration, in compressed format



NOTE: A Perl script is provided in the Tools folder of the compressed software image bundle, which you downloaded from the Juniper Networks website, that enables you to view the text configuration in a configuration file that contains both binary and text configuration. The Perl script supports multiple platforms. The “Usage and Troubleshooting document for desktop tool” file in PDF format provides an explanation of how to extract the system configuration file, using the extractScrFromCnf.pl script.

Mode Privileged Exec

copy running-configuration startup-configuration

Syntax copy running-configuration startup-configuration

Release Information Command introduced before JUNOS Release 7.1.0.

Description Saves all outstanding (unsaved) configuration changes to nonvolatile storage; an exact alias of the **write memory** command. Available if the router is in either Automatic Commit mode or Manual Commit mode. If you issue this command from Automatic Commit mode, the CLI notifies you that the command is not necessary, but allows you to proceed. This command is prevented during the high availability initialization state. If the command is issued during this state, the CLI notifies you of the state and requests that you try again later. There is no **no** version.

Mode Privileged Exec

copy startup-configuration

Syntax copy startup-configuration *destination* [force]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Copies the previously saved startup configuration to a local or remote (network) router configuration (*.cnf) file. Available only if the router is in Manual Commit mode. If you have made but not saved any configuration changes, those changes are not in the startup configuration. There is no **no** version.

- Options** ■ *destination*—Destination filename (*.cnf)
 ■ *force*—Creates a copy even if the destination file already exists

Mode Privileged Exec

cost

Syntax *cost intfCost*

 no cost

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a cost metric for an OSPF remote-neighbor interface. Used in the calculation of the SPF routing table. The **no** version restores the default value.

Options ■ *intfCost*—Link-state metric cost; a number in the range 1–65535; default value is 10 if there is no route to the remote neighbor; otherwise, the default is calculated based on the bandwidth of the physical interface used to reach the remote neighbor and the OSPF auto-cost reference bandwidth

Mode Remote Neighbor Configuration

country

Syntax [no] country *countryCode*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a country name used to generate certificate requests. The **no** version removes the country name.

Options ■ *countryCode*—Two-character country name

Mode IPSec Identity Configuration

crc

Syntax `crc { 16 | 32 | none }`

 `no crc`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the size of the cyclic redundancy check. CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. 16 and 32 indicate the number of check digits per frame that are used to calculate the FCS. Both the sender and receiver must use the same setting. The default value is 16. The **no** version restores the value to the default.

- Options** ■ 16—Specifies CRC-16, which transmits streams of 8-bit characters and generates 16-bit check bits per frame
- 32—Specifies CRC-32, which transmits longer streams at faster rates and therefore provides better ongoing error detection
- none—Disables CRC checking

Mode Interface Configuration

crl

Syntax crl { ignored | optional | required }
 no crl

Release Information Command introduced before JUNOS Release 7.1.0.

Description Controls how the router checks certificate revocation lists (CRLs) when determining whether to accept a peer's certificates. The **no** version restores the default setting.

- Options**
- ignored—Specifies that the router will not try to find or use CRLs
 - optional—Specifies that the router will try to find a CRL. If a CRL is found, the peer certificate must not appear in the CRL. If no CRL is found, the peer can still authenticate; this is the default.
 - required—Specifies that the router must find a valid CRL; the CRL must be current, and the peer certificate must not appear in the CRL

Mode IPSec CA Identity Configuration

crypto key dss

Syntax crypto key { generate | zeroize } dss

Release Information Command introduced before JUNOS Release 7.1.0.

Description Controls SSH server daemon and creation/deletion of SSH server host key. This command is not displayed by the **show config** command. There is no **no** version.

- Options**
- generate—Creates the SSH server host key and enables the daemon
 - zeroize—Deletes the SSH server host key and stops the SSH daemon if it is running. Issuing this command terminates any active client sessions. The next time the router boots after this command is issued, the SSH server daemon is not started.

Mode Global Configuration

Chapter 5

D Commands

data-character-bits

Syntax data-character bits { 7 | 8 }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the number of data bits available for characters for all sessions on the specified vty lines. There is no **no** version.

- Options**
- 7—Specifies 7 data bits per character; this setting supports only characters in the standard ASCII set
 - 8—Specifies 8 data bits per character; default setting, supports the full set of 8-bit international characters

Mode Line Configuration

dead-interval

Syntax `dead-interval deadInterval`
`no dead-interval`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the time period that the OSPF router waits without seeing hello packets from a remote neighbor before declaring the neighbor to be down. The **no** version restores the default value.

Options ■ *deadInterval*—Number in the range 1–65535 seconds; default value is 40 seconds

Mode Remote Neighbor Configuration

deadtime

Syntax *deadtime recovery*

 no deadtime

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the amount of time, in minutes, that a server is marked as unavailable if a request times out for the configured retry count. If a server fails to answer a request, it is marked “unavailable” by the router. The router does not send requests to the server for the configured time. The **no** version restores the default value, 0, turning off the deadtime mechanism.

Options ■ *recovery*—Number of minutes that a server is marked as unavailable, in the range 0–1440; default value is 0

Mode RADIUS Configuration

debounce

Syntax `debounce [seconds]`

`no debounce`

Release Information Command introduced in JUNOS Release 9.3.0.

Description Enables the debounce timer and sets the time interval that the interface waits before reporting a state change to the upper-layer protocols. The **no** version restores the default behavior, disabling debounce on the interface.

Options ■ *seconds*—Interval for which an interface must maintain a given state before the interface reports the state change to the upper-layer protocols. Number in the range 1–5 seconds; default value is 1 second.

Mode Interface Configuration

debounce-interval

Syntax `debounce-interval seconds`

 `no debounce-interval`

Release Information Command introduced in JUNOS Release 9.3.0.

Description Modifies the minimum time an Ethernet interface must maintain a given state—for example, up or down—before the interface notifies the upper-layer protocols of the state change. The `no` version restores the default value, 1 second.



NOTE: You can configure this command only if you have enabled the debounce timer feature using the **debounce** command.

Options ■ *seconds*—Interval for which an interface must maintain a given state before the interface reports the state change to the upper-layer protocols. Number in the range 1–5 seconds; default value is 1 second.

Mode Interface Configuration

debounce-time

Syntax `debounce-time interval`
`no debounce-time`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the interval to wait before bringing up a RIP interface that was brought down. The **no** version restores the default value, 10.

Options ■ *interval*—Seconds in the range 0–60

Mode Address Family Configuration, Router Configuration

debug ip bgp

Syntax debug ip bgp [in | out] [*peerAddress* [*peerAddressMask*]] [*bgpLog*]
 [router *routerName*] [filtering-router *filteringRouterName*] [*accessClassName*]
 [route-map *mapName*] [severity { *severityValue* | *severityNumber* }]
 [verbosity *verbosityLevel*] [secondary]

no debug ip bgp [in | out] [*peerAddress* [*peerAddressMask*]] [*bgpLog*]
 [router *routerName*] [filtering-router *filteringRouterName*] [*accessClassName*]
 [route-map *mapName*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Shows information about the selected variable. The **no** version disables the display.

- Options**
- in—Displays information for inbound events
 - out—Displays information for outbound events
 - *peerAddress*—IP address of BGP peer for which information is displayed
 - *peerAddressMask*—Network mask of BGP peer for which information is displayed
 - *bgpLog*—BGP log of interest; one of the following options:
 - dampening—BGP dampening event; route is suppressed or no longer suppressed by route-flap dampening
 - events—BGP finite state machine events and transitions
 - keepalives—BGP keepalive message events
 - next-hops—BGP next hop events
 - updates—BGP routing table update events
 - *routerName*—Name of the virtual router that owns the BGP router for which information is being displayed
 - *filteringRouterName*—Name of the virtual router that owns the access class and route map parameters
 - *accessClassName*—Name of an access list to filter output
 - *mapName*—Name of a route map to filter output
 - severity—Specifies the minimum severity of the log messages displayed for the selected category; described either by a descriptive term—*severityValue*—or by a corresponding number—*severityNumber*—in the range 0–7; the lower the number, the higher the priority:
 - emergency or 0—System unusable
 - alert or 1—Immediate action needed
 - critical or 2—Critical condition exists

- *error or 3*—Error condition
- *warning or 4*—Warning condition
- *notice or 5*—Normal but significant condition
- *info or 6*—Informational message
- *debug or 7*—Debug message
- *verbosityLevel*—Verbosity of the log category's messages; can be any of the following:
 - *low*—Terse
 - *medium*—Moderate detail
 - *high*—Verbose
- *secondary*—Indicates that the specified filter conditions for the log are imposed in addition to any that were previously specified; if omitted, the specified filter conditions replace any that were previously specified

Mode Privileged Exec

debug ip mbgp

Syntax debug ip mbgp [in | out] [*peerAddress* [*peerAddressMask*]] [*bgpLog*]
 [router *routerName*] [filtering-router *filteringRouterName*] [*accessClassName*]
 [route-map *mapName*] [severity { *severityValue* | *severityNumber* }]
 [verbosity *verbosityLevel*] [secondary]

no debug ip mbgp [in | out] [*peerAddress* [*peerAddressMask*]] [*bgpLog*]
 [router *routerName*] [filtering-router *filteringRouterName*] [*accessClassName*]
 [route-map *mapName*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Shows information about the selected variable. The **no** version disables the display.

- Options**
- in—Displays information for inbound events
 - out—Displays information for outbound events
 - *peerAddress*—IP address of BGP peer for which information is displayed
 - *peerAddressMask*—Network mask of BGP peer for which information is displayed
 - *bgpLog*—BGP log of interest; one of the following options:
 - dampening—BGP dampening event; route is suppressed or no longer suppressed by route-flap dampening
 - events—BGP finite state machine events and transitions
 - keepalives—BGP keepalive message events
 - next-hops—BGP next hop events
 - updates—BGP routing table update events
 - *routerName*—Name of the virtual router that owns the BGP router for which information is being displayed
 - *filteringRouterName*—Name of the virtual router that owns the access class and route map parameters
 - *accessClassName*—Name of an access list to filter output
 - *mapName* —Name of a route map to filter output
 - severity—Specifies the minimum severity of the log messages displayed for the selected category; described either by a descriptive term—*severityValue*—or by a corresponding number—*severityNumber*—in the range 0–7; the lower the number, the higher the priority:
 - emergency or 0—System unusable
 - alert or 1—Immediate action needed
 - critical or 2—Critical condition exists

- *error or 3*—Error condition
- *warning or 4*—Warning condition
- *notice or 5*—Normal but significant condition
- *info or 6*—Informational message
- *debug or 7*—Debug message
- *verbosityLevel*—Verbosity of the log category's messages; can be any of the following:
 - *low*—Terse
 - *medium*—Moderate detail
 - *high*—Verbose
- *secondary*—Indicates that the specified filter conditions for the log are imposed in addition to any that were previously specified; if omitted, the specified filter conditions replace any that were previously specified

Mode Privileged Exec

debug ip ospf

Syntax debug ip ospf *ospfLog* [severity { *severityValue* | *severityNumber* }]
 [verbosity *verbosityLevel*]

no debug ip ospf *ospfLog*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Shows information about the selected variable. The **no** version disables the display.

- Options**
- *ospfLog*—OSPF log of interest; one of the following options:
 - adj—OSPF adjacency events
 - elect-dr—OSPF designated router election
 - events—OSPF general events
 - lsa—OSPF link-state advertisements events
 - neighbor—OSPF neighbor state machine
 - packets-rcvd—OSPF packets received
 - packets-sent—OSPF packets sent
 - route—OSPF route events
 - spf—All OSPF shortest path first calculation events
 - spf-ext—OSPF shortest path first external route calculation events
 - spf-inter—OSPF shortest path first interarea route calculation events
 - spf-intra—OSPF shortest path first intra-area route calculation events
 - severity—Specifies the minimum severity of the log messages displayed for the selected category; described either by a descriptive term—*severityValue*—or by a corresponding number—*severityNumber*—in the range 0–7; the lower the number, the higher the priority:
 - emergency or 0—System unusable
 - alert or 1—Immediate action needed
 - critical or 2—Critical condition exists
 - error or 3—Error condition
 - warning or 4—Warning condition
 - notice or 5—Normal but significant condition

- `info or 6`—Informational message
- `debug or 7`—Debug message
- *verbosityLevel*—Verbosity of the log category's messages; can be any of the following:
 - `low`—Terse
 - `medium`—Moderate detail
 - `high`—Verbose

Mode Privileged Exec

debug ip pim

Syntax The syntax differs for PIM Dense Mode and PIM Sparse Mode.

PIM Dense Mode:

```
debug ip pim { pimLog [ severity { severityValue | severityNumber } ]
[ verbosity verbosityLevel ] | switchState groupAddress sourceAddress |
dense-mode { on | off } }
```

PIM Sparse Mode:

```
debug ip pim { pimLog [ severity { severityValue | severityNumber } ]
[ verbosity verbosityLevel ] | switchState groupAddress sourceAddress |
sparse-mode { on | off | sg-state [ group groupAddress
[ source sourceAddress ] | rp rpAddress ] [ count ] } }
```

```
no debug ip pim pimLog
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description Shows information about the selected variable. The **no** version disables the display.

- Options**
- *pimLog*—PIM log of interest; one of the following options:
 - *autoRp-rcvd*—Auto-RP packets received
 - *autoRP-sent*—Auto-RP packets sent
 - *engineering*—PIM engineering
 - *hellos-rcvd*—PIM hello messages received
 - *hellos-sent*—PIM hello messages sent
 - *packets*—PIM packets received and sent
 - *packets-rcvd*—PIM packets received
 - *packets-sent*—PIM packets sent
 - *severity*—Specifies the minimum severity of the log messages displayed for the selected category; described either by a descriptive term—*severityValue*—or by a corresponding number—*severityNumber*—in the range 0–7; the lower the number, the higher the priority:
 - *emergency* or 0—System unusable
 - *alert* or 1—Immediate action needed
 - *critical* or 2—Critical condition exists
 - *error* or 3—Error condition

- warning or 4—Warning condition
- notice or 5—Normal but significant condition
- info or 6—Informational message
- debug or 7—Debug message
- *verbosityLevel*—Verbosity of the log category's messages; can be any of the following:
 - low—Terse
 - medium—Moderate detail
 - high—Verbose
- *switchState*—Switches from one type of tree to another
 - rpt-switch—Switch from a shortest-path tree to a shared path tree
 - spt-switch—Switch from a shared-path tree to a shortest path tree
- *groupAddress*—IP address of the multicast group
- *sourceAddress*—IP address of the multicast source
- on—Turns on the specified PIM mode on all virtual routers
- off—Turns off the specified PIM mode on all virtual routers
- sg-state—Displays information about the relationship between a source, multicast group, and RP router
- rp—Displays information about the relationships between sources, groups, and the specified RP router
- *rpAddress*—Address of the RP router
- count—Displays one of the following
 - (with no optional keywords) number of relationships between a source, multicast group, and RP router
 - (with the **group** keyword) number of sources associated with the multicast group for PIM sparse mode
 - (with the **source** and **group** keywords) number of source-group pairs for PIM sparse mode
 - (with the **rp** keyword) number of source-group pairs associated with the RP router for PIM sparse mode

Mode Privileged Exec

debug ip rip

Syntax `debug ip rip ripLog [severity { severityValue | severityNumber }]`
`[verbosity verbosityLevel]`

`no debug ip rip ripLog`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Shows information about the selected variable. The **no** version disables the display.

- Options**
- *ripLog*—RIP log of interest; one of the following options:
 - *events*—General RIP events, such as removing RIP from an interface or creating the RIP process
 - *route*—Events associated with two RIP routers exchanging routes
 - *severity*—Specifies the minimum severity of the log messages displayed for the selected category; described either by a descriptive term—*severityValue*—or by a corresponding number—*severityNumber*—in the range 0–7; the lower the number, the higher the priority:
 - *emergency or 0*—System unusable
 - *alert or 1*—Immediate action needed
 - *critical or 2*—Critical condition exists
 - *error or 3*—Error condition
 - *warning or 4*—Warning condition
 - *notice or 5*—Normal but significant condition
 - *info or 6*—Informational message
 - *debug or 7*—Debug message
 - *verbosityLevel*—Verbosity of the log category's messages; can be any of the following:
 - *low*—Terse
 - *medium*—Moderate detail
 - *high*—Verbose

Mode Privileged Exec

debug ipv6 ospf

Syntax `debug ipv6 ospf ospfLog [severity { severityValue | severityNumber }]`
`[verbosity verbosityLevel]`

`no debug ipv6 ospf ospfLog`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Shows information about the selected variable. The **no** version disables the display.

- Options**
- *ospfLog*—OSPF log of interest; one of the following options:
 - *adj*—OSPF adjacency events
 - *elect-dr*—OSPF designated router election
 - *events*—OSPF general events
 - *lsa*—OSPF link-state advertisements events
 - *neighbor*—OSPF neighbor state machine
 - *packets-rcvd*—OSPF packets received
 - *packets-sent*—OSPF packets sent
 - *route*—OSPF route events
 - *spf*—All OSPF shortest path first calculation events
 - *spf-ext*—OSPF shortest path first external route calculation events
 - *spf-inter*—OSPF shortest path first interarea route calculation events
 - *spf-intra*—OSPF shortest path first intra-area route calculation events
 - *severity*—Specifies the minimum severity of the log messages displayed for the selected category; described either by a descriptive term—*severityValue*—or by a corresponding number—*severityNumber*—in the range 0–7; the lower the number, the higher the priority:
 - *emergency or 0*—System unusable
 - *alert or 1*—Immediate action needed
 - *critical or 2*—Critical condition exists
 - *error or 3*—Error condition
 - *warning or 4*—Warning condition
 - *notice or 5*—Normal but significant condition

- `info or 6`—Informational message
- `debug or 7`—Debug message
- *verbosityLevel*—Verbosity of the log category's messages; can be any of the following:
 - `low`—Terse
 - `medium`—Moderate detail
 - `high`—Verbose

Mode Privileged Exec

debug ipv6 pim

Syntax debug ipv6 pim
 { *pimLog* [severity { *severityValue* | *severityNumber* }] [verbosity *verbosityLevel*] |
 switchState *groupAddress* *sourceAddress* |
 dense-mode { on | off } |
 sparse-mode { on | off | sg-state [group *groupAddress*
 [source *sourceAddress*] | rp *rpAddress*] [count] } }

 no debug ipv6 pim *pimLog*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Shows information about the selected variable. The **no** version disables the display.

- Options** ■ *pimLog*—PIM log of interest; one of the following options:
- autoRp-rcvd—Auto-RP packets received
 - autoRP-sent—Auto-RP packets sent
 - engineering—PIM engineering
 - hellos-rcvd—PIM hello messages received
 - hellos-sent—PIM hello messages sent
 - packets—PIM packets received and sent
 - packets-rcvd—PIM packets received
 - packets-sent—PIM packets sent
- severity—Specifies the minimum severity of the log messages displayed for the selected category; described either by a descriptive term—*severityValue*—or by a corresponding number—*severityNumber*—in the range 0–7; the lower the number, the higher the priority:
- emergency or 0—System unusable
 - alert or 1—Immediate action needed
 - critical or 2—Critical condition exists
 - error or 3—Error condition
 - warning or 4—Warning condition
 - notice or 5—Normal but significant condition
 - info or 6—Informational message
 - debug or 7—Debug message

- *verbosityLevel*—Verbosity of the log category's messages; can be any of the following:
 - low—Terse
 - medium—Moderate detail
 - high—Verbose
- *switchState*—Switches from one type of tree to another
 - rpt-switch—Switch from a shortest-path tree to a shared path tree
 - spt-switch—Switch from a shared-path tree to a shortest path tree
- *groupAddress*—IPv6 address of the multicast group
- *sourceAddress*—IPv6 address of the multicast source
- on—Turns on the specified PIM mode on all virtual routers
- off—Turns off the specified PIM mode on all virtual routers
- sg-state—Displays information about the relationship between a source, multicast group, and RP router
- rp—Displays information about the relationships between sources, groups, and the specified RP router
- *rpAddress*—Address of the RP router
- count—Displays one of the following
 - (with no optional keywords) number of relationships between a source, multicast group, and RP router
 - (with the **group** keyword) number of sources associated with the multicast group for PIM sparse mode
 - (with the **source** and **group** keywords) number of source-group pairs for PIM sparse mode
 - (with the **rp** keyword) number of source-group pairs associated with the RP router for PIM sparse mode

Mode Privileged Exec

debug isis

Syntax `debug isis isisLog [severity { severityValue | severityNumber }]`
 `[verbosity verbosityLevel]`

`no debug isis isisLog`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Displays debug-related information about selected IS-IS log parameters. This command manipulates the same log as the Global Configuration **log** commands. The **no** version disables debugging display.

- Options** ■ *isisLog*—IS-IS log of interest; one of the following options:
- *adj-packets*—IS-IS adjacency-related packets, such as hello packets sent and IS-IS received adjacencies going up and down
 - *mpls traffic-eng advertisements*—MPLS traffic-engineering agent advertisements
 - *mpls traffic-eng agents*—MPLS traffic-engineering agents
 - *snp-packets*—IS-IS CSNPs/PSNPs
 - *spf-events*—Shortest path first events
 - *spf-statistics*—SPF timing and statistic data
 - *spf-triggers*—SPF triggering events
 - *update-packets*—Update-related packets
- *severity*—Specifies the minimum severity of the log messages displayed for the selected category; described either by a descriptive term—*severityValue*—or by a corresponding number—*severityNumber*—in the range 0–7; the lower the number, the higher the priority:
- *emergency or 0*—System unusable
 - *alert or 1*—Immediate action needed
 - *critical or 2*—Critical condition exists
 - *error or 3*—Error condition
 - *warning or 4*—Warning condition
 - *notice or 5*—Normal but significant condition
 - *info or 6*—Informational message
 - *debug or 7*—Debug message

- *verbosityLevel*—Verbosity of the log category's messages; can be any of the following:
 - low—Terse
 - medium—Moderate detail
 - high—Verbose

Mode Privileged Exec

default-fields peer

Syntax [no] default-fields peer *fieldOptions*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the fields that will appear by default in the output of subsequently issued `show ip bgp summary` and `show bgp ipv6 summary` commands. The **no** version removes the fields from the output.

- Options**
- *fieldOptions*—Field(s) to be displayed, in the format
all | [dynamic | intro | last-reset-reason | messages-received | messages-sent |
more-in-queue | peer-type | prefixes-received | remote-as | rib-version |
send-queue-length | state | times-up | up-down-time | updates-received |
updates-sent]*
 - all—All available information; not recommended, because this information for each network does not fit on a single line and is difficult to read
 - dynamic—Nature of peer, dynamic or not
 - intro—Introductory information about the state of various BGP attributes; this information is displayed only if you specify this keyword
 - last-reset-reason —Reason for most recent reset
 - messages-received—Total number of messages received from the peer
 - messages-sent—Total number of messages sent to the peer
 - more-in-queue—Status indicating whether any messages are waiting to be sent to this peer
 - peer-type—Type of BGP peer: internal, external, or confederation
 - prefixes-received—Number of unique prefixes received from the peer
 - remote-as—Remote AS number of the peer
 - rib-version—Last RIB version queued to be sent to this peer
 - send-queue-length—Number of messages queued to be sent to this peer
 - state—State of the BGP session
 - times-up—Number of times the session has been established
 - up-down-time—How long the session has been up or down
 - updates-received—Number of update messages received from the peer

- updates-sent—Number of update messages sent to the peer
- *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Router Configuration

default-fields route

Syntax [no] default-fields route *fieldOptions*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the fields that will appear by default in the output of any subsequently issued **show ip bgp** or **show bgp ipv6** command that displays routes (except for the **show ip bgp summary** or **show bgp ipv6 summary** commands). The **no** version removes the fields from the output.

- Options**
- *fieldOptions*—Field(s) to be displayed, in the format
all | [afi | aggregator | as-path | atomic-aggregate | best | clusters | communities | extended-communities | imported | intro | in-label | loc-pref | med | next-hop | next-hop-cost | origin | originator-id | out-label | peer | peer-type | rd | safi | stale | unknown-types | weight]*
 - all—All available information; not recommended, because this information for each network does not fit on a single line and is difficult to read
 - afi—Address family identifier
 - aggregator—AS number and IP address of aggregator
 - as-path—AS path through which this route has been advertised
 - atomic-aggregate—Whether the atomic aggregate attribute is present
 - best—Whether this is the best route for the prefix
 - clusters—List of cluster IDs through which the route has been advertised
 - communities—Community number associated with the route
 - extended-communities—Extended community
 - imported—Whether the route was imported
 - intro—Introductory information about the state of various BGP attributes; this information is displayed only if you specify this keyword
 - in-label—MPLS label for the route; the label received with incoming MPLS frames
 - loc-pref—Local preference for the route
 - med—Multiexit discriminator for the route
 - next-hop—IP address of the next router that is used when forwarding a packet to the destination network
 - next-hop-cost—Whether the indirect next hop of the route is unreachable, if not, displays IGP cost to the indirect next hop

- out-label—MPLS label for the route; the label with outgoing MPLS frames
- peer—IP address of BGP peer from which route was learned
- peer-type—Type of BGP peer: internal, external, or confederation
- origin—Origin of the route
- originator-id—Router ID of the router in the local AS that originated the route
- rd—Route distinguisher
- safi—Subsequent address family identifier
- stale—Route that has gone stale due to peer restart
- unknown-types—Attribute codes for unknown path attributes
- weight—Weight of the route
- *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Router Configuration

default-information originate

Syntax For BGP:

```
default-information originate [ route-map mapTag ]
```

```
no default-information originate [ route-map [ mapTag ] ]
```

For IS-IS:

```
[ no ] default-information originate [ route-map mapTag ]
```

For RIP:

```
[ no ] default-information originate [ route-map mapTag ]
```

```
default-information originate always
```

For OSPF:

```
[ no ] default-information originate [ always | metric metricValue | metric-type 1 |  
metric-type 2 | route-map mapTag ]*
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables BGP to advertise a default route (0.0.0.0/0) if the default route exists in the IP routing table. If the default route does not exist, you must configure it using the **ip route** command.

When you issue this command in the route-target address family, BGP advertises the Default-RT-MEM-NLRI route (0:0:0/0)

For IS-IS, OSPF, and RIP, configures a default route for the distribution of default information into the respective routing domain. IS-IS creates the default route (0.0.0.0/0) if it does not exist in the IP routing table. OSPF and RIP do not create the default route unless you use the **always** option.

For all protocols, the **no** version disables advertisement of the default route. The syntax varies with the protocol.

- Options**
- *mapTag*—Name of route map used to import the default route; string of up to 32 characters
 - **always**—Creates the default route, so that it is always advertised
 - *metricValue*—Sets the metric for the default route; in the range 0–4294967295
 - **metric-type 1**—Sets the default route's metric type to OSPF external type 1

- `metric-type 2`—Sets the default route's metric type to OSPF external type 2
- `*`—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Address Family Configuration, Router Configuration

default-metric

Syntax [no] default-metric *metricValue* [*interfaceType* *interfaceSpecifier*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures RIP to use this metric on redistributed routes on all subsequently created interfaces. The **no** version restores the default value, 0.

- Options**
- *metricValue*—Metric to apply to routes; in the range 1–16
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Address Family Configuration, Router Configuration

default-router

Syntax `default-router ipAddressPrimary [ipAddressSecondary]`
 `no default-router`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the IP address of the router that the subscriber's computer will use for traffic destined for locations beyond the local subnet. The default router must be on the same subnet as the local server pool addresses configured with the **network** command. The **no** version removes the association between the address pool and the router.

- Options** ■ *ipAddressPrimary*—IP address of preferred router
 ■ *ipAddressSecondary*—IP address of secondary router

Mode DHCP Local Pool Configuration

default-upper-type mlppp

Syntax default-upper-type mlppp
 no default-upper-type

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that L2TP creates an MLPPP interface for the current LNS session when full LCP proxy data is not available. The **no** version deletes the MLPPP specification.

Mode L2TP Destination Profile Host Configuration

delete

Syntax delete { *filename* | directory *directoryName*[:*fileName*] } [force]

Release Information Command introduced before JUNOS Release 7.1.0.
fileName variable added for **directory** keyword in JUNOS Release 9.1.0.

Description Deletes a directory or file in nonvolatile storage. There is no **no** version.



NOTE: For detailed information on file type usage with the **delete** command, see *Deleting Files* in the *JUNOS System Basics Configuration Guide*.

- Options**
- *fileName*—Name of the local file you are deleting (for example, `system1.cnf`); in User Exec and Privileged Exec mode only, an asterisk (*) in any position in the filename substitutes for zero or more characters; using an asterisk causes the CLI to prompt you for confirmation before the file or directory is deleted. You cannot delete `reboot.hty` or `system.log` files when you use an asterisk.
 - *directoryName*—Path of a directory. To delete a file in user space, specify the incoming or outgoing directory on the FTP server; you can specify the name of a subdirectory in the incoming or outgoing directory. You cannot use an asterisk in a directory name.
 - **force**—Forces deletion of directory or file even when it is not empty; however, if a file in the specified directory, or a specified file, is marked by the file system as in use because it is required for the current operation or configuration, the **force** keyword cannot force a deletion of the directory.

The **force** keyword is ignored when you attempt to delete any `.dmp` or `.tsa` file (unless the deletion is issued from a `.mac` or `.scr` file); this means that the CLI always prompts for confirmation for these file types.

Mode Boot, Privileged Exec, User Exec

delta-sampling

Syntax delta-sampling [discontinuity-id *mibId*
 | discontinuity-id-type { timeStamp | timeTicks }]
 no delta-sampling [discontinuity-id]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies delta sampling for the trigger you are configuring. The **no** version returns the trigger to the default sampling method—absolute-value sampling.

- Options**
- discontinuity-id—Specifies a discontinuity MIB ID for the sample. The discontinuity MIB ID monitors the sample for any discontinuity errors during the sample frequency. If a discontinuity error occurs, the router removes the sampling for that interval.
 - *mibId*—Object ID of the discontinuity MIB attribute that you want to use for this trigger
 - discontinuity-id-type—Specifies a discontinuity ID type (either timeStamp or timeTicks). The discontinuity ID type indicates the time value that you expect for a specific sample.

Mode SNMP Trigger Configuration

deny

Syntax [no] deny *domainName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the domain name(s) that are to be denied access to AAA authentication. The **no** version negates the command.

Options ■ *domainName*—Name of the domain; maximum of 64 characters

Mode AAA Profile Configuration

description

Syntax `description name`
 `no description`

Release Information Command introduced before JUNOS Release 7.1.0.

Description In Controller Configuration mode, assigns a text description or an alias to a CT3, E3, T3, or SONET/SDH interface. Use the `show controllers e3`, `show controllers sonet`, `show controllers t1`, or `mpls rsvp disable` command to display the description. The **no** version removes the description or alias.

In VRF Configuration mode, assigns a text description or an alias to the VRF. The **no** version removes the description or alias.



NOTE: In Interface Configuration mode, this command has been replaced by the `ip description` command for assigning a description to a static IP interface. This command may be removed completely from Interface Configuration mode in a future release.

Options ■ *name*—Text string or alias of up to 256 characters (in Interface Configuration mode) or up to 80 characters (in Controller Configuration mode and VRF Configuration mode)

Mode Controller Configuration, Interface Configuration, VRF Configuration

dhcp delete-binding

Syntax To delete the DHCP client with the specified binding ID:

```
dhcp delete-binding bindingId
```

To delete all DHCP client bindings or all DHCP client bindings of a particular type on the specified subnet:

```
dhcp delete-binding { all | all-local | all-external | all-relay-proxy } [ subnetAddress ]
```

To delete DHCP client bindings of a particular type on the specified subnet:

```
dhcp delete-binding { local | external | relay-proxy } [ subnetAddress ]
```

To delete DHCP client bindings for the specified IP prefix:

```
dhcp delete-binding [ local | external | relay-proxy ] [ subnetAddress ] ip-prefix ipPrefix
```

To delete DHCP client bindings for the specified interface string:

```
dhcp delete-binding [ local | external | relay-proxy ] [ subnetAddress ] interface string
```

To delete DHCP client bindings without a lower-layer interface:

```
dhcp delete-binding [ local | external | relay-proxy ] [ subnetAddress ] no-interface
```

To delete DHCP client bindings for the specified agent-circuit-id suboption (suboption 1) string of the DHCP relay agent information option (option 82):

```
dhcp delete-binding [ local | external | relay-proxy ] [ subnetAddress ] circuit-id string
```

To delete DHCP client bindings for the specified agent-remote-id suboption (suboption 2) string of the DHCP relay agent information option (option 82):

```
dhcp delete-binding [ local | external | relay-proxy ] [ subnetAddress ] remote-id string
```

Release Information Command introduced in JUNOS Release 8.1.0.
local, **external**, **relay-proxy**, **interface**, **no-interface**, **ip-prefix**, **circuit-id**, and **remote-id** keywords and *subnetAddress*, *ipAddress*, and *string* variables added in JUNOS Release 9.3.0.

Description Deletes the specified DHCP client bindings. There is no **no** version.



NOTE: This command replaces the deprecated **clear ip dhcp-local binding** and **dhcp-external delete-binding** commands, which may be removed completely in a future release.

- Options**
- *bindingId*—DHCP binding ID for a specific client
 - *all*—Specifies all DHCP local server, DHCP external server, and DHCP relay proxy client bindings
 - *all-local*—Specifies all DHCP local server client bindings
 - *all-external*—Specifies all DHCP external server client bindings
 - *all-relay-proxy*—Specifies all DHCP relay proxy client bindings
 - *local*—Specifies DHCP local server client bindings that meet the deletion criteria
 - *external*—Specifies DHCP external server client bindings that meet the deletion criteria
 - *relay-proxy*—Specifies DHCP relay proxy client bindings that meet the deletion criteria
 - *subnetAddress*—IP address of the subnet on which the DHCP clients reside
 - *ipPrefix*—IP prefix (address and subnetwork mask) of the DHCP clients; for example, 10.10.10.0/24
 - *no-interface*—Specifies DHCP clients without a lower-layer interface; use this keyword to delete DHCP client bindings configured over dynamic interfaces for which the lower-layer interface has been shut down
 - *string*—Regular expression string that represents the interface, circuit ID, or remote ID to be matched; you must enclose elements containing a space within double quotes (“*one element*”)

Each element is either a literal string, a metacharacter, or a combination. You can remove the special meaning of a metacharacter by preceding it with a backslash (\). Regular expressions support the following metacharacters:

- *^* Matches the beginning of the input string. Alternatively, when used as the first character within brackets—*[^]*—matches any number except the ones specified within the brackets.
- *\$* Matches the end of the input string
- *.* (period) Matches any single character, including white space
- *** Matches 0 or more sequences of the immediately previous character or pattern.
- *+* Matches 1 or more sequences of the immediately previous character or pattern
- *?* Matches 0 or 1 sequence of the immediately previous character or pattern
- *()* Specifies patterns for multiple use when followed by one of the multiplier metacharacters: asterisk ***, plus sign *+*, or question mark *?*
- *[]* Matches any enclosed character; specifies a range of single characters
- *-* (hyphen) Used within brackets to specify a range of AS or community numbers
- *_* (underscore) Matches a *^*, a *\$*, a comma, a space, a *{*, or a *}*. Placed on either side of a string to specify a literal and disallow substring matching.

Numerals enclosed by underscores can be preceded or followed by any of the characters listed above

- | Matches characters on either side of the metacharacter; logical OR

You must specify the interface string as a regular expression without spaces; for example, `fastEthernet1.1/100` or `fastEthernet.*100`

The following rules apply for representing nonprintable character sequences in the circuit ID string or the remote ID string:

- To represent the binary sequence 0d 0a (hex), use the string `'\r\n'`. This consists of four ASCII characters: 5c for `\`, 72 for `r`, 5c for `\`, and 6e for `n`.
For example, to match the sequence 74 65 73 74 0d 0a 6f 6e 65 (hex), use the string `'test\r\none'`. In this string, 74 is represented by `t`, 65 is represented by `e`, 73 is represented by `s`, 74 is represented by `t`, 0d 0a is represented by `\r\n`, 6f is represented by `o`, 6e is represented by `n`, and 65 is represented by `e`.
- To represent the binary sequence 0d 00 (hex), use the string `'\r'`. This consists of two ASCII characters: 5c for `\`, and 72 for `r`.
- To represent the binary sequence 0a 00 (hex), use the string `'\n'`. This consists of two ASCII characters: 5c for `\`, and 6e for `n`.
For example, to match the sequence 74 65 73 74 0a 00 6f 6e 65 (hex), use the string `'test\none'`. In this string, 74 is represented by `t`, 65 is represented by `e`, 73 is represented by `s`, 74 is represented by `t`, 0a 00 is represented by `\n`, 0a is represented by `\n`, 6f is represented by `o`, 6e is represented by `n`, and 65 is represented by `e`.
- To represent all other cases, use the string `'\xab'`, where `ab` is a hex code of the byte. For example, to represent byte 3A, use `'\x3a'`. This consists of four ASCII characters: 5c for `\`, 78 for `x`, 33 for `3`, and 61 for `a`.
As another example, to match the sequence 74 65 73 74 f3 6f 6e 65 (hex), use the string `'test\xf3one'`. In this string, 74 is represented by `t`, 65 is represented by `e`, 73 is represented by `s`, 74 is represented by `t`, byte F3 is represented by `\xf3`, 6f is represented by `o`, 6e is represented by `n`, and 65 is represented by `e`.

Mode Privileged Exec

dhcp-external delete-binding

Syntax dhcp-external delete-binding [binding-id *bindingId* | all]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Deletes a specific client binding or all bindings from the virtual router's DHCP binding table. There is no **no** version.



NOTE: This command is deprecated and might be removed completely in a future release. The function provided by this command has been replaced by the **dhcp delete-binding** command.

- Options**
- *bindingId*—DHCP binding ID associated with the user.
 - *all*—Specifies all bindings

Mode Privileged Exec

dhcp-external duplicate-mac-address

Syntax [no] dhcp-external duplicate-mac-address

Release Information Command introduced in JUNOS Release 9.3.0.

Description Configures the DHCP external server application to use a combination of the MAC address and the gateway IP address (giaddr) to uniquely identify DHCP clients attached to the router. This behavior is also referred to as *duplicate MAC mode*. The **no** version restores the default behavior, also known as *unique MAC mode*, which uses only the MAC address to uniquely identify DHCP clients.

Mode Global Configuration

- Related Topics**
- DHCP External Server Identification of Clients with Duplicate MAC Addresses Overview
 - Configuring DHCP External Server to Uniquely Identify Clients with Duplicate MAC Addresses

dhcpv6 delete-binding

Syntax `dhcpv6 delete-binding { all | ipv6Prefix | string }`

Release Information Command introduced in JUNOS Release 11.0.0.

Description Deletes the specified DHCPv6 client bindings. There is no **no** version.

- Options**
- *all*—Specifies all DHCPv6 client bindings.
 - *ipv6Prefix*—IPv6 prefix (address and subnetwork mask) of the DHCPv6 clients; for example, 2002:2:4:1::/64
 - *string*—Local address pool name in the range 1–16 characters; for example, server4pool

Mode Privileged Exec

- Related Topics**
- Deleting DHCPv6 Client Bindings
 - Monitoring DHCPv6 Local Server Binding Information

diag

Syntax `diag slotNumber [subsystem] [force]`

Release Information Command introduced in JUNOS Release 7.3.0.

Description Reboots the SRP module or line module in the specified slot on all E Series routers and performs diagnostic tests. There is no **no** version.

- Options**
- *slotNumber*—Number of the chassis slot that contains the SRP module or line module
 - *subsystem*—Type of subsystem on the E120 router or the E320 router; use when the specified *slotNumber* is a slot that contains an SRP module
 - *srp*—Indicates the system controller (SC) on one or both SRP modules; specify this keyword to restart only the portion of the SC on the individual SRP module
 - *fabric*—Indicates the portion of the switch fabric on the SRP modules; specify this keyword to restart only an individual fabric slice
 - *force*—Specifies that the system manually confirm conflicting conditions when the slot of the active SRP module is specified

Mode Privileged Exec

diag-level

Syntax diag-level [normal] [bypass]

Release Information Command introduced in JUNOS Release 9.2.0.

Description Sets the diagnostics level on the active or standby SRP module to reduce boot time during a cold and a warm boot. The default diagnostics level is normal. There is no **no** version.

Options ■ normal—executes full diagnostics on the boot of the line card
 bypass—skips diagnostic tests on the boot of the line card

Mode Global Configuration

dir

Syntax dir [*word*] [short]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Displays information about the files in nonvolatile storage, including name, size, date created, and whether they are in use. There is no **no** version.



NOTE: When high availability is enabled on the router, it is possible that files or file attributes may appear to be unsynchronized when they are not. When enabled, high availability mirrors configuration changes instantly from the active SRP module to the standby SRP module. However, although these changes are reflected immediately in memory, NVS on the standby SRP module is updated at 5-minute intervals.

- Options**
- *word*—Path to a specific directory, or a filename; an asterisk (*) in any position in a filename substitutes for zero or more characters; you cannot use a wildcard in a path
 - *short*—Limits display to file name and creation date

Mode Privileged Exec, User Exec

disable

Syntax To return to User Exec mode:

disable [*level*]

For DVMRP, RIP:

[no] disable

Release Information Command introduced before JUNOS Release 7.1.0.

Description When used from Privileged Exec mode, exits Privileged Exec mode and returns to User Exec mode.

When used from Router Configuration or Interface Configuration mode in the context of a DVMRP configuration, disables DVMRP on the virtual router or interface. The **no** version reenables DVMRP on the virtual router or interface.

When used from Router Configuration mode in the context of a RIP configuration, disables RIP on the virtual router. The **no** version enables RIP processing on the virtual router.

- Options**
- *level*—One of the following privilege levels; default value is 1
 - 0—Allows the user to execute the **help**, **enable**, **disable**, and **exit** commands
 - 1—Allows the user to execute commands in User Exec mode plus commands at level 0
 - 5—Allows the user to execute Privileged Exec show commands plus the commands at levels 1 and 0
 - 10—Allows the user to execute all commands except support commands, which may be provided by Juniper Networks Customer Service
 - 15—Allows the user to execute support commands

Mode Address Family Configuration (RIP), Interface Configuration (DVMRP only), Privileged Exec, Router Configuration (DVMRP or RIP)

disable-autosync

Syntax [no] disable-autosync

Release Information Command introduced before JUNOS Release 7.1.0.

Description Halts automatic synchronization between the primary and standby SRP modules. When high availability is enabled (that is, the high availability state is initializing, active, or pending) this command affects only changes to nonconfiguration files. With high availability enabled, configuration changes are always mirrored to the standby SRP module. The **no** version restores the default situation, in which automatic synchronization runs as a background process every 5 minutes.

Mode Global Configuration

disable-dynamic-redistribute

Syntax [no] disable-dynamic-redistribute

Release Information Command introduced before JUNOS Release 7.1.0.

Description Halts the dynamic redistribution of routes that are initiated by changes to a route map. Supported by DVMRP, BGP, IS-IS, OSPF, and RIP. The **no** version reenables dynamic redistribution of routes.

Mode Address Family Configuration, Router Configuration

disable-incremental-external-spf

Syntax [no] disable-incremental-external-spf

Release Information Command introduced before JUNOS Release 7.1.0.

Description Disables incremental external SPF on the router; results in a full SPF when an event occurs to trigger an external SPF. The **no** version reenables incremental external SPF.

Mode Router Configuration

disable proxy lcp

Syntax [no] disable proxy lcp

Release Information Command introduced before JUNOS Release 7.1.0.

Description Disables the proxy LCP parameter for the remote host. The **no** version enables the proxy LCP parameter for the remote host.

Mode L2TP Destination Profile Host Configuration

disable-switch-on-error

Syntax [no] disable-switch-on-error

Release Information Command introduced before JUNOS Release 7.1.0.

Description Prevents the redundant SRP module from taking over if the primary SRP module experiences a software failure or if you push the reset button on the primary SRP module. Issue the **sync** command immediately before you issue this command. The **no** version restores the default situation, in which the redundant SRP module takes over if the primary SRP module experiences a failure.

Mode Global Configuration

disconnect-cause

Syntax [no] disconnect-cause

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables an E Series LNS to generate, for the L2TP session to which the L2TP host profile applies, a PPP Disconnect Cause Code attribute value pair (AVP) and include it in all L2TP Call-Disconnect-Notify (CDN) messages that it sends to an LAC. This action provides a mechanism for the LAC to obtain information about the cause of a session disconnection. The **no** version disables generation of the PPP Disconnect Cause Code AVP, which is the default setting.

Mode L2TP Destination Profile Host Configuration

disconnect ssh

Syntax `disconnect ssh { vty vtYId | sessionId }`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Terminates an active SSH session. Use the **show ip ssh** command to determine the session identifier for the session to terminate. There is no **no** version.

- Options**
- *vtYId*—Virtual terminal identifier for VTY where the SSH session resides; use the **show users** command to determine the identifier
 - *sessionId*—Integer in the range 0–4294967295 that identifies the session to be terminated

Mode Privileged Exec

discovery-mode

Syntax [no] discovery-mode

Release Information Command introduced in JUNOS Release 7.2.0.

Description Enables ANCP discovery mode. This mode allows RADIUS software to obtain loop parameter information from a connected access node. If discovery mode is disabled, it does not accept topology discovery messages and stops advertising topology discovery capability. It does not affect any other neighbors. The **no** version disables ANCP discovery mode.

Mode L2C Neighbor Configuration

distance

Syntax The options available vary depending on your routing protocol context; that is, on whether you are configuring OSPF or RIP.

For OSPF:

```
[ no ] distance { ospfWeight | ospf { external distExt | inter-area disInter | intra-area disIntra } [ external distExt | inter-area distInter | intra-area distIntra ]* }
```

For RIP:

```
[ no ] distance ripWeight
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines an administrative distance for RIP or OSPF routes. A distance of 255 prevents the route from being installed in the routing table. The **no** version either negates a command or restores the command's defaults.

- Options**
- *distance*—Weight applied to OSPF routes
 - *ospfWeight*—Value assigned to OSPF routes that are added to the IP routing table; a number in the range 1–255
 - *ospf*—OSPF routes
 - *distExt*—Distance for external type 5 and type 7 routes; a number in the range 1–255
 - *disInter*—Distance for interarea routes; a number in the range 1–255
 - *disIntra*—Distance for intra-area routes; a number in the range 1–255
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line
 - *ripWeight*—Administrative distance assigned to RIP routes added to the IP routing table in the range 0–255; default value is 120

Mode Address Family Configuration (RIP), Router Configuration (OSPF or RIP)

distance bgp

Syntax distance bgp *externalDistance internalDistance localDistance*
 no distance bgp [*externalDistance* [*internalDistance* [*localDistance*]]]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the administrative distances for BGP routes. A distance of 255 prevents the route from being installed in the routing table. The **no** version restores the default values.

- Options**
- *externalDistance*—Administrative distance for routes external to the AS in the range 1–255; default value is 20
 - *internalDistance*—Administrative distance for routes internal to the AS in the range 1–255; default value is 200
 - *localDistance*—Administrative distance for local (redistributed) routes in the range 1–255; default value is 200

Mode Address Family Configuration, Router Configuration

distance ip

Syntax [no] distance *weight* ip

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the administrative distance for IS-IS routes that are inserted into the IP routing table. A distance of 255 prevents the route from being installed in the routing table. The **no** version restores the default value, 115.

Options ■ *weight*—Administrative distance assigned to IS-IS routes added to the IP routing table in the range 1–255

Mode Router Configuration

distribute-domain-wide

Syntax [no] distribute-domain-wide

Release Information Command introduced before JUNOS Release 7.1.0.

Description Increases the granularity of routing information within an IS-IS domain by allowing routes to be distributed from level 2 to level 1. This results in more accurate routing between level 1 areas. The **no** version disables the command.

Mode Router Configuration

distribute-list

Syntax In Router Configuration mode:

```
[ no ] distribute-list accessListName { in | out } [ interfaceType interfaceSpecifier ]
```

In Remote Neighbor Configuration mode:

```
[ no ] distribute-list accessListName { in | out }
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the distribute list, an access list applied to incoming or outgoing RIP route updates. In Remote Neighbor Configuration mode, applies only to a RIP remote-neighbor interface. The **no** version removes the distribute list. An IP access list acts as a filter; refer to the **access-list** command for details.

- Options**
- *accessListName*—Name of the access list; string of up to 32 alphanumeric characters
 - in—Applies the access list to incoming route updates
 - out—Applies the access list to outgoing route updates
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Address Family Configuration, Remote Neighbor Configuration, Router Configuration

dns-domain-search

Syntax [no] dns-domain-search *domainName*

Release Information Command introduced in JUNOS Release 10.1.0.

Description Specifies a list of domain names in the IPv6 local address pool to be returned to clients in DHCPv6 responses as part of the Domain Search List option. The **no** version removes the configured domain name.



NOTE: You can configure one domain name per line. Enter the command on separate lines to configure additional domain names.

Options ■ *domainName*—Domain name that the DHCPv6 client uses when it resolves hostnames with the DNS server. You can specify a maximum of four DNS domains for the search list of an IPv6 local pool; maximum of 32 characters

Mode IPv6 Local Pool Configuration

dns-server

Syntax `dns-server ipAddressPrimary [ipAddressSecondary]`
 `no dns-server`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns a DNS server to an address pool. The **no** version removes the association between the address pool and the DNS server.

- Options** ■ *ipAddressPrimary*—IP address of preferred DNS server
 ■ *ipAddressSecondary*—IP address of secondary DNS server

Mode DHCP Local Pool Configuration

dns-server (for IPv6)

Syntax `dns-server ipv6AddressPrimary [ipv6AddressSecondary]`
`no dns-server`

Release Information Command introduced in JUNOS Release 10.1.0.

Description Configures the primary and secondary IPv6 DNS server addresses in the IPv6 local address pool. The DNS server addresses are returned to the client in DHCPv6 responses as part of the DNS Recursive Name Server option. The **no** version removes the configured DNS server addresses.

- Options** ■ *ipv6AddressPrimary*—IPv6 address of the primary DNS server.
 ■ *ipv6AddressSecondary*—IPv6 address of the secondary DNS server.

Mode IPv6 Local Pool Configuration

do

Syntax `do execCommand`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Allows you to issue an Exec mode command from any configuration command mode. This command functions the same as the **run** command. There is no **no** version.

Options ■ *execCommand*—CLI command that you can issue from User Exec or Privileged Exec mode

Mode All configuration command modes

domain

Syntax domain *domainName*

no domain

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the domain to an automatically generated username in an IP service profile. The **no** version removes the domain.

Options ■ *domainName* —Name of the domain; maximum of 32 characters

Mode IP Service Profile Configuration

domain-authentication

Syntax [no] domain-authentication { csnp | psnp }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables or disables simple text authentication or HMAC MD5 authentication of IS-IS level 2 CSNP packets or PSNP packets. The **no** version restores the default behavior, in which authentication of IS-IS level 2 CSNPs and PSNPs is disabled.

- Options**
- csnp—Enables authentication of IS-IS level 2 complete sequence number PDUs (CSNPs)
 - psnp—Enables authentication of IS-IS level 2 partial sequence number PDUs (PSNPs)

Mode Router Configuration

domain-authentication-key

Syntax domain-authentication-key [0 | 8] *authKey*
 no domain-authentication-key

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns a password for authentication of IS-IS level 2 LSPs, CSNPs, and PSNPs. The **no** version deletes the password.



NOTE: Issuing this command enables simple authentication of level 2 LSPs only. To enable authentication of level 2 CSNPs or PSNPs, use the **domain-authentication** command.

- Options**
- 0—indicates the *authKey* is entered in unencrypted form (plaintext); this is the default option
 - 8—indicates the *authKey* is entered in encrypted form (ciphertext)
 - *authKey*—password; string of up to 8 characters

Mode Router Configuration

domain-id

Syntax domain-id *domainIdAddress* | *domainId*
 no domain-id

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the OSPF domain ID for an OSPF VRF on a PE. The **no** version restores the default value.

- Options**
- *domainIdAddress*—OSPF domain ID in IP address format; default value is the IP address of the OSPF router configured in the VRF
 - *domainId*—OSPF domain ID as an integer value in the range 0–4294967295; default value is 0

Mode Router Configuration

domain-message-digest-key

Syntax domain-message-digest-key *keyId* hmac-md5 [0 | 8] *key*
 [start-accept *startAcceptTime* [{ *startAcceptMonth* *startAcceptDay* | *startAcceptDay* *startAcceptMonth* } *startAcceptYear*]]
 [start-generate *startGenTime* [{ *startGenMonth* *startGenDay* | *startGenDay* *startGenMonth* } *startGenYear*]]
 [stop-accept { never | *stopAcceptTime* [{ *stopAcceptMonth* *stopAcceptDay* | *stopAcceptDay* *stopAcceptMonth* } *stopAcceptYear*] }]
 [stop-generate { never | *stopGenTime* [{ *stopGenMonth* *stopGenDay* | *stopGenDay* *stopGenMonth* } *stopGenYear*] }]
 no domain-message-digest-key *keyId*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies an HMAC MD5 key that the router uses to create a secure, encrypted message digest of each IS-IS level 2 packet (LSPs, CSNPs, and PSNPs). The digest is inserted into the packet from which it is created. Using this algorithm for domain routers protects against unauthorized routers injecting false routing information into your network. You can specify when the router will start (default is the current time) and stop (default is never) accepting packets that include a digest made with this key. You can specify when the router will start (default is the current time plus 2 minutes) and stop (default is never) generating packets that include a digest made with this key. The **no** version deletes the key specified by the *keyId*.



NOTE: Issuing this command enables MD5 authentication of level 2 LSPs only. To enable authentication of level 2 CSNPs or PSNPs, use the **domain-authentication** command.

- Options**
- *keyId*—Integer from 1 to 255 that is a unique identifier for the secret key, sent with the message digest in the packet.
 - 0—Indicates the *key* is entered in unencrypted form (plaintext); this is the default option
 - 8—Indicates the *key* is entered in encrypted form (ciphertext)
 - *key*—String of up to 20 alphanumeric characters; secret key used by the HMAC MD5 algorithm to generate the message digest.
 - *startAcceptTime*, *startAcceptMonth*, *startAcceptDay*, *startAcceptYear* – time, month, day, year that the router will start accepting packets created with this password. Use military time format *HH : MM[: SS]*.
 - *startGenTime*, *startGenMonth*, *startGenDay*, *startGenYear*—Time, month, day, year that the router will start inserting this password into packets. Use military time format *HH : MM[: SS]*.

- *never*—Specifies that the router never stops accepting or generating packets; overrides previously specified stop times.
- *stopAcceptTime, stopAcceptMonth, stopAcceptDay, stopAcceptYear*—Time, month, day, year that the router will stop accepting packets created with this password. Use military time format *HH : MM[: SS]*.
- *stopGenTime, stopGenMonth, stopGenDay, stopGenYear*—Time, month, day, year that the router will stop inserting this password into packets. Use military time format *HH : MM[: SS]*.

Mode Router Configuration

domain-name

Syntax From DHCP Local Pool Configuration mode:

domain-name *domainName*

no domain-name

From IPsec Identity Configuration mode:

[no] domain-name *domainName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description From DHCP Local Pool Configuration mode, specifies a domain name that can be returned to the subscriber of an address pool if requested. The **no** version removes the association between the address pool and the domain name.

From IPsec Identity mode, specifies the domain name that the router uses in IKE authentication messages and to generate certificate requests. The **no** version removes the domain name.

- Options**
- *domainName*—Name of the domain
 - *domainName*—Name used in certificate requests and in IKE authentication messages; up to 60 characters

Mode DHCP Local Pool Configuration, IPsec Identity Configuration

domain-suffix

Syntax domain-suffix *domainSuffix*
 no domain-suffix

Release Information Command introduced in JUNOS Release 7.3.0.

Description Appends a domain suffix to user-provided usernames on this profile. The **no** version restores the default value, no domain suffix, and usernames are passed transparently to AAA.

Options ■ *domainSuffix*—Domain suffix that you want to append to user-provided usernames.

Mode IPSec Tunnel Profile Configuration

domain-tag

Syntax domain-tag *routeTag*
 no domain-tag

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the VPN route tag for an OSPF VRF on a PE to prevent routing loops back into the VPN. The **no** version restores the default value.

Options ■ *routeTag*—Number identifying the VPN route tag in the range 0–4294967295

Mode Router Configuration

dont-install-routes

Syntax [no] dont-install-routes

Release Information Command introduced before JUNOS Release 7.1.0.

Description Prevents OSPF routes that point directly to the OSPF remote neighbor from being installed in the IP routing table of the VR or VRF in which OSPF is running. The **no** version restores the default behavior, which installs the routes in the IP routing table.

Mode Remote Neighbor Configuration

dos-protection-group

Syntax [no] dos-protection-group *groupName*

Release Information Command introduced in JUNOS Release 8.1.0.

Description Creates a denial of service (DoS) protection group and enters DoS Protection Group Configuration mode. The **no** version removes the DoS protection group.

Options ■ *groupName*—Name of the DoS protection group; string of up to 31 alphanumeric characters

Mode Global Configuration

drop-profile

Syntax [no] drop-profile *dropProfileName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates a drop profile. The **no** version removes the drop profile.

Options ■ *dropProfileName*—Name for the drop profile

Mode Global Configuration

Related Topics ■ Configuring RED
■ Configuring WRED

ds3-scramble

Syntax [no] ds3-scramble

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables scrambling of the ATM cell payload on a T3 interface. DS3 scrambling assists clock recovery on the receiving end of the interface. The **no** version disables cell scrambling.

Mode Controller Configuration

dsr-detect

Syntax [no] dsr-detect

Release Information Command introduced before JUNOS Release 7.1.0.

Description Requires that a DSR signal be detected on the line for a user to log into the console. DSR is carried on pin 6 of the SRP module's RS-232 (DB-9) connector. The DSR input must be connected to the DSR output of a modem or the DTR output of another DTE device, such as a terminal server, that supports this signal. If a session is in progress and the DSR signal is lost, the user is logged out automatically. The **no** version restores the default of no DSR required.

Mode Privileged Exec

dsu bandwidth

Syntax dsu bandwidth *bandwidthValue*

 no dsu bandwidth

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the speed for the fractional T3 lines. The **no** version clears the bandwidth. If you issue this command, be sure to issue the **dsu mode** and **scramble** commands. Similarly, if you issue the **no** version, be sure to issue the **no** versions of the **dsu mode** and **scramble** commands; otherwise, the interface may drop packets unexpectedly.

Options ■ *bandwidthValue*—Value of the fractional bandwidth in the range 22–44210 Kbps. The router offers a set of speeds in increments that depend on the DSU mode you specify. The actual speed of the fractional T3 lines will be the value closest to the fractional bandwidth you specify.

Mode Controller Configuration

dsu mode

Syntax dsu mode { 0 | 2 }

 no dsu mode

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the DSU mode for the lines. The **no** version clears the dsu mode. If you issue this command, be sure to issue the **dsu bandwidth** and **scramble** commands. Similarly, if you issue the **no** version, be sure to issue the **no** versions of the **dsu bandwidth** and **scramble** commands; otherwise, the interface may drop packets unexpectedly.

- Options** ■ 0—Sets digital Link mode
 ■ 2—Sets Larscom mode

Mode Controller Configuration

duplex

Syntax duplex *duplexMode*
 no duplex

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the duplex mode for an Ethernet interface. This command works with the **speed** command; if you set or accept the automatically negotiate setting for either duplex mode or speed, the router negotiates both parameters with the remote device. The **no** version specifies the default value, automatically negotiate or full duplex (FE-8 SFP I/O module only). This command is not available for the Ethernet interface on the SRP module.

- Options** ■ *duplexMode*—One of the following duplex options
- automatically negotiate—Specifies that the router negotiates duplex mode with the remote device; not valid for the FE-8 SFP I/O module
 - full—Specifies that the router uses full duplex on a Fast Ethernet or Gigabit Ethernet interface
 - half—Specifies that the router uses half duplex on a Fast Ethernet interface; this value is not valid for Gigabit Ethernet interfaces

Mode Interface Configuration

dvmrp destination profile

Syntax dvmrp destination profile *profileName* { [any-virtual-router] |
[virtual-router *virtualRouterName*] }

no dvmrp destination profile *profileName*

Release Information Command introduced in JUNOS Release 8.2.0.

Description	Configures a destination profile for dynamic DVMRP tunnels and enters IP Tunnel Destination Profile Configuration mode. There is no no version.
--------------------	--

Options

- *profileName*—Name of the destination profile
- *any-virtual-router*—Specifies a default destination profile for all virtual routers; only one default destination profile can be defined in the system
- *virtualRouterName*—Name of the transport virtual router

Mode Global Configuration

Chapter 6

E Commands

e3-scramble

Syntax [no] e3-scramble

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables scrambling of the ATM cell payload on an E3 interface. E3 scrambling assists clock recovery on the receiving end of the interface. The **no** version disables scrambling.

Mode Controller Configuration

enable

Syntax To access Privileged Exec mode:

```
enable [ level ]
```

To enable event or trigger configuration:

```
[ no ] enable
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description From User Exec mode, enters Privileged Exec mode at the specified privilege level. There is no **no** version for this use.

From SNMP Event Configuration or SNMP Trigger Configuration modes, enables the configuration for the event or trigger, respectively. The **no** version disables the event or trigger.

- Options**
- *level*—level at which you want to access the Privileged Exec mode; default value is 10; commands generally fall into one of the following security/privilege levels:
 - 0—allows the user to execute the **help**, **enable**, **disable**, and **exit** commands
 - 1—Allows the user to execute commands in User Exec mode plus commands at level 0
 - 5—Allows the user to execute Privileged Exec **show** commands plus the commands at levels 1 and 0
 - 10—Allows the user to execute all commands except support commands, which may be provided by Juniper Networks Customer Service, or the ability to assign privileges to commands
 - 15—Allows the user to execute support commands and assign privileges to commands

Mode SNMP Event Configuration, SNMP Trigger Configuration, User Exec

enabled

Syntax [no] enabled

Release Information Command introduced in JUNOS Release 8.1.0.

Description Enables the aggregation cache to start accumulating information from the flow cache. The **no** version stops the information flow from the flow cache.

Mode Flow Cache Configuration

enable ipsec-transport

Syntax [no] enable ipsec-transport

Release Information Command introduced before JUNOS Release 7.1.0.
IP Tunnel Destination Profile Configuration mode added in JUNOS Release 8.2.0.

Description In IP Tunnel Destination Profile Configuration mode, specifies that the router accepts only dynamic IP tunnels protected by an IPsec transport connection. The **no** version disables IPsec transport mode.

In L2TP Destination Profile Host Configuration mode, specifies that the router accepts only L2TP tunnels protected by an IPsec transport connection. The **no** version disables IPsec transport mode.

Mode IP Tunnel Destination Profile Configuration, L2TP Destination Profile Host Configuration

enable password

Syntax enable password [level *securityLevel*] [*passwordType*] *passwordText*
 no enable password [level *securityLevel*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a password to control access to certain types of commands. The **no** version removes the password requirement.



NOTE: On the E Series router, all passwords are stored as encrypted passwords.

- Options**
- *securityLevel*—Security level for which you want to set the password; default value is 5; commands generally fall into one of the following security/privilege levels:
 - 0—Allows the user to execute the **help**, **enable**, **disable**, and **exit** commands
 - 1—Allows the user to execute commands in User Exec mode plus commands at level 0
 - 5—Allows the user to execute Privileged Exec show commands plus the commands at levels 1 and 0; this is the default level
 - 10—Allows the user to execute all commands except support commands, which may be provided by Juniper Networks Customer Service
 - 15—Allows the user to execute privilege setting and support commands
 - *passwordType*:
 - 0—Specifies that an unencrypted password follows; this is the default
 - 7—Specifies that an encrypted password follows
 - *passwordText*—Password, either encrypted or unencrypted, depending on the password type

Mode Global Configuration

enable proxy authenticate

Syntax [no] enable proxy authenticate

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures proxy authenticate for a remote host. The **no** version removes proxy authenticate configuration from the remote host.

Mode L2TP Destination Profile Host Configuration

enable secret

Syntax `enable secret [level securityLevel] [secretType] secretText`
 `no enable secret [securityLevel]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a secret to control access to certain types of commands. The **no** version removes the secret requirement.



NOTE: On the E Series router, all secrets are stored as encrypted secrets.

- Options**
- *securityLevel*—Security level for which you want to set the secret; default value is 5
 - 0—Allows the user to execute the **help**, **enable**, **disable**, and **exit** commands
 - 1—Allows the user to execute commands in User Exec mode plus commands at level 0
 - 5—Allows the user to execute Privileged Exec **show** commands plus the commands at levels 1 and 0; this is the default level
 - 10—Allows the user to execute all commands except support commands, which may be provided by Juniper Networks Customer Service
 - 15—Allows the user to execute support commands
 - *secretType*—One of the following:
 - 0—Indicates that the secret is unencrypted; this is the default
 - 7—Indicates that the secret is encrypted
 - *secretText*—Secret, either encrypted or unencrypted, depending on the secret type

Mode Global Configuration

encapsulation

Syntax `encapsulation encapsulationType`
 `no encapsulation`

Release Information Command introduced in JUNOS Release 7.1.0.
 ATM VC Class Configuration mode added in JUNOS Release 7.3.0.

Description In ATM VC Configuration mode, configures the encapsulation method on an ATM PVC. The encapsulation method represents the format of the data units that traverse the PVC. The **encapsulation** command is valid only for data PVCs; you cannot use this command for control (ILMI or signaling) PVCs. The **no** version restores the default encapsulation method, **aal5snap**.

In ATM VC Class Configuration mode, configures the encapsulation method as part of a VC class definition that you assign to an ATM data PVC. The **no** version restores the default encapsulation method, **aal5snap**, in the VC class.

- Options** ■ *encapsulationType*—One of the following encapsulation methods for data PVCs:
- **aal0**—Causes the router to receive raw ATM cells on this PVC and forward the cells without performing AAL5 packet reassembly
 - **aal5all**—Configures ATM over MPLS passthrough connections; the router passes through all ATM AAL5 traffic without interpreting it
 - **aal5autoconfig**—Enables autodetection of the 1483 encapsulation (LLC/SNAP or VC multiplexed)
 - **aal5mux ip**—Configures a VC-based multiplexed circuit used for IP only
 - **aal5snap**—Configures an LLC encapsulated circuit; an LLC/SNAP header precedes the protocol datagram

Mode ATM VC Configuration, ATM VC Class Configuration

encapsulation bridge1483

Syntax encapsulation bridge1483 [mac-address *macAddress*]
 no encapsulation bridge1483

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures bridged Ethernet as the encapsulation method on an interface and optionally assigns a MAC address to the interface. The **no** version removes bridged Ethernet as the encapsulation method on the interface.

Options ■ *macAddress*—User-configured MAC address for the interface. The MAC address format is a dotted triple of four-digit hexadecimal numbers; for example, 0090.1a40.4c7c. Multicast MAC address cannot be configured on bridged Ethernet interfaces.

Mode Subinterface Configuration

encapsulation frame-relay ietf

Syntax encapsulation frame-relay ietf
 no encapsulation frame-relay

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables Frame Relay encapsulation. The **no** version removes Frame Relay configuration from an interface.

Mode Interface Configuration

Related Topics ■ *Configuring Frame Relay Layer 2 Services in the JUNOS BGP and MPLS Configuration Guide*

encapsulation hdlc

Syntax [no] encapsulation hdlc

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables Cisco HDLC encapsulation. The **no** version disables Cisco HDLC on an interface.

Mode Interface Configuration, Subinterface Configuration

encapsulation mlframe-relay ietf

Syntax encapsulation mlframe-relay ietf
 no encapsulation mlframe-relay

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables Multilink Frame Relay encapsulation. The **no** version removes Multilink Frame Relay configuration from an interface.

Mode Interface Configuration

encapsulation mlppp

Syntax [no] encapsulation mlppp

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures MLPPP as the encapsulation method on an individual interface. Creates an MLPPP link interface, which can be configured as a member of an MLPPP bundle. The **no** version disables MLPPP on an interface.

Mode Interface Configuration, Subinterface Configuration

encapsulation ppp

Syntax [no] encapsulation ppp

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures PPP as the encapsulation method for the interface. The **no** version disables PPP on an interface.

Mode Interface Configuration, Subinterface Configuration

encapsulation pppoe

Syntax [no] encapsulation pppoe

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures PPPoE as the encapsulation method for the interface. The **no** version removes PPPoE encapsulation from the interface.

Mode Interface Configuration, Subinterface Configuration

encapsulation vlan

Syntax [no] encapsulation vlan

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures VLAN as the encapsulation method for the interface. The **no** version removes VLAN encapsulation from the interface.

Mode Interface Configuration, Subinterface Configuration

Related Topics ■ *Configuring Ethernet/VLAN Layer 2 Services, Configuring Local Cross-Connects Between Ethernet/VLAN Interfaces, and Configuring S-VLAN Tunnels for Layer 2 Services in the JUNOS BGP and MPLS Configuration Guide*

encryption

Syntax encryption { des | 3des }
 no encryption

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the encryption algorithm to use in the IKE policy. The **no** version restores the default, 3DES.

- Options** ■ des—Specifies 56-bit DES-CBC as the encryption algorithm
 ■ 3des—Specifies 168-bit 3DES-CBC as the encryption algorithm

Mode IKE Policy Configuration

end

Syntax end

Release Information Command introduced before JUNOS Release 7.1.0.

Description Exits Global Configuration mode or any of the Configuration submodes and returns to the User Exec mode. There is no **no** version.

Mode Global Configuration

enrollment retry-limit

Syntax enrollment retry-limit *minutes*
 no enrollment retry-limit

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the number of minutes during which the router continues to send a certificate request to the CA. The **no** version restores the default.

Options ■ *minutes*—Number of minutes, from 0 (infinite time period) to 480; default value is 60

Mode IPSec CA Identity Configuration

enrollment retry-period

Syntax enrollment retry-period *minutes*
 no enrollment retry-period

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the number of minutes that the router waits after receiving no response before resending a certificate request to the CA. The **no** version restores the default.

Options ■ *minutes*—Number of minutes in the range 0–60 minutes; default value is 1

Mode IPSec CA Identity Configuration

enrollment url

Syntax `enrollment url url`
`no enrollment url`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the URL of the simple certificate enrollment protocol (SCEP) server to which the router sends CA certificate requests (using the **ipsec ca authenticate** command) and public certificate requests (using the **ipsec ca enroll** command). The **no** version deletes the URL specification.

Options ■ *url*—URL of SCEP server; in the format `http://server_ipaddress`; a maximum of 200 characters

Mode IPsec CA Identity Configuration

equipment loopback

Syntax equipment { customer | network } loopback
 no equipment

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables or disables the router's ability to be placed in loopback by a remote device connected on a CT3 or T3 interface. The **no** version disables the router's ability to be placed in loopback by the remote device.

- Options**
- customer—Enables the router to enter into loopback when it receives an appropriate signal from the remote interface
 - network—Disables the router's ability to enter into loopback when it receives an appropriate signal from the remote interface

Mode Controller Configuration

erase secrets

Syntax `erase secrets seconds`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Removes all CLI passwords or secrets. Execute before pressing the NMI button on the SRP module. There is no **no** version.



NOTE: If you enter the **service unattended password-recovery** command, the behavior of the **erase secrets** command changes. The **erase secrets** command will not take any parameters and will not be available through a vty session until you enter **no service unattended password-recovery**.

Options ■ *seconds*—Number of seconds in the range 1–60 to allow for the operation

Mode User Exec

ethernet description

Syntax ethernet description *name*
 no ethernet description

Release Information Command introduced before JUNOS Release 7.1.0.

Description Adds a text description to a non-SRP Fast Ethernet or Gigabit Ethernet interface. The **no** version removes the description from the interface.

Options ■ *name*—String of up to 64 characters

Mode Interface Configuration

ethernet dos-protection-group

Syntax ethernet dos-protection-group *groupName*
 no ethernet dos-protection-group

Release Information Command introduced in JUNOS Release 8.1.0.

Description Attaches an Ethernet denial of service (DoS) protection group to an interface. The **no** version removes the attachment of the DoS protection group from the interface.

Options ■ *groupName*—Name of the DoS protection group; string of up to 31 alphanumeric characters

Mode Interface Configuration

ethernet oam lfm

Syntax [no] ethernet oam lfm

Release Information Command introduced in JUNOS Release 11.1.0.

Description Enables 802.3ah Ethernet Operation, Administration, and Maintenance (OAM) link-fault management on an interface. Enabling IEEE 802.3ah OAM functionality on a physical interface automatically triggers the discovery process. The default discovery mode of the OAM entity is active. The **no** version disables OAM link-fault management on the interface.



NOTE: If you enable OAM on an interface without specifying other parameters for the local OAM entity, such as the discovery mode for the OAM entity and the interval at which OAM protocol data units (PDUs) are sent to the remote peer, default values are assigned to all the attributes that are not manually configured.

Mode Interface Configuration

- Related Topics**
- ethernet oam lfm mode on page 589
 - Guidelines for Configuring 802.3ah OAM Link-Fault Management
 - Configuring 802.3ah OAM Link-Fault Management

ethernet oam lfm high-threshold

Syntax [no] ethernet oam lfm high-threshold { disable-interface | failover }

Release Information Command introduced in JUNOS Release 11.1.0.

Description Configures a specific action to occur when a high threshold for an error is exceeded on an Ethernet OAM interface. The **no** version removes the high-threshold action from the interface of the local OAM client and causes no action to be performed when local errors occur on the interface.

- Options**
- disable-interface—Sets the OAM functionality to unconditionally attempt to influence the operational state of the interface to down. If the interface is a member link of a LAG bundle and at least one other viable link (redundant member or another active/up link) is present, OAM attempts to influence the operational state of the link to down. Otherwise, no action is taken
 - failover—On GE-2 and GE-HDE line modules with GE-2 SFP I/O modules with physical link redundancy, causes the link to transition from active to redundant

Mode Interface Configuration

- Related Topics**
- OAM Link Monitoring Feature
 - Configuring 802.3ah OAM Link-Fault Management
 - Example: Configuring 802.3ah OAM Link-Fault Management and Enabling Remote Failure Monitoring on an Interface

ethernet oam lfm link-monitor frame-seconds

Syntax [no] ethernet oam lfm link-monitor frame-seconds { threshold { high { *highFrames* | none } | low *lowFrames* } | window *period* }

Release Information Command introduced in JUNOS Release 11.1.0.

Description Configures a threshold value for sending frame error events that triggers an action or causes an Errored Frame Event TLV to be sent to the OAM entity, or a period of time in which error frames are counted. The **no** version disables monitoring of received frame error events.



NOTE: You can configure this command multiple times to configure combinations of high and low threshold values or a window period for frame error events.

- Options**
- **link-monitor**—Configures link monitoring parameters. Link monitoring operations start automatically when Ethernet OAM is enabled on an interface. When link monitoring operations are disabled, the interface does not actively send or receive Event Notification OAM PDUs
 - **frame-seconds**—Configures the threshold value or window for frame error events
 - **threshold**—Configures a period or a value at, above, or below which an action is triggered
 - ***highFrames***—Integer in the range 1–65535 that is the high threshold in number of frames, which when exceeded causes an action to be triggered. The action that the local OAM entity performs when the high threshold value is exceeded depends on the value configured using the **ethernet oam lfm high-threshold** command. There is no default value. If you specify a high threshold option for error frames, you must also enter the number of frames, which when exceeded causes the configured action to be taken
 - **none**—Removes the high threshold value for error frames
 - ***lowFrames***—Integer in the range 0–65535 that is the low threshold in number of frames; default value is 0 frames. When this value is exceeded, an Errored Frame Event TLV is sent to the peer. If you do not configure a low threshold for frame error events, the Errored Frame Event TLV is not sent to the peer
 - ***period***—A window and period of time during which error frames are counted. Integer in the range 10–600 that represents a number of milliseconds in a multiple of 100; default value is 1000 milliseconds, which is denoted by specifying 10 units for the *period* variable in the CLI interface

Mode Interface Configuration

- Related Topics**
- OAM Link Monitoring Feature
 - Configuring 802.3ah OAM Link-Fault Management
 - `ethernet oam lfm link-monitor symbol-period` on page 587
 - `ethernet oam lfm link-monitor frame-seconds-summary` on page 585
 - Example: Configuring 802.3ah OAM Link-Fault Management and Enabling Remote Failure Monitoring on an Interface

ethernet oam lfm link-monitor frame-seconds-summary

Syntax [no] ethernet oam lfm link-monitor frame-seconds-summary { threshold { high { *highSummary* | none } | low *lowSummary* } | window *period* }

Release Information Command introduced in JUNOS Release 11.1.0.

Description Configures a threshold value for frame period summary error events that triggers an action or causes an Errored Frame Seconds Summary Event TLV to be sent to the OAM entity, or a period of time in which frame period summary error events are counted. The **no** version disables monitoring of received frame period summary error events.



NOTE: You can configure this command multiple times to configure combinations of high and low threshold values or a window period for frame error events.

- Options**
- **link-monitor**—Configures link monitoring parameters. Link monitoring operations start automatically when Ethernet OAM is enabled on an interface. When link monitoring operations are disabled, the interface does not actively send or receive Event Notification OAM PDUs
 - **frame-seconds-summary**—Configures the threshold value or window for frame period summary error events
 - **threshold**—Configures a period or a value at, above, or below which an action is triggered
 - **highSummary**—Integer in the range 1–65535 that is the high threshold in number of error frame seconds, which when exceeded causes an action to be triggered. The action that the local OAM entity performs when the high threshold value is exceeded depends on the value configured using the **ethernet oam lfm high-threshold** command. There is no default value. If you specify a high threshold option for frame period summary error events, you must also enter the number of frames, which when exceeded causes the configured action to be taken
 - **none**—Removes the high threshold value for frame period summary error events
 - **lowSummary**—Integer in the range 0–65535 that is the low threshold in number of error frame seconds, which when exceeded causes an Errored Frame Seconds Summary Event TLV to be sent to the peer; default value is 0 frames. If you do not configure a low threshold for framed symbol errors, the Link Fault critical event PDU is not sent to the peer
 - **period**—A window and period of time during which framed period summary seconds are counted. Integer in the range 10–900 seconds that is the monitoring period for framed symbol errors; default value is 60 seconds

Mode Interface Configuration

- Related Topics**
- OAM Link Monitoring Feature
 - Configuring 802.3ah OAM Link-Fault Management
 - `ethernet oam lfm link-monitor symbol-period` on page 587
 - `ethernet oam lfm link-monitor frame-seconds` on page 583
 - Example: Configuring 802.3ah OAM Link-Fault Management and Enabling Remote Failure Monitoring on an Interface

ethernet oam lfm link-monitor symbol-period

Syntax [no] ethernet oam lfm link-monitor symbol-period { threshold { high { *highFrames* | none } | low *lowFrames* } | window *period* }

Release Information Command introduced in JUNOS Release 11.1.0.

Description Configures a threshold value for symbol error events that triggers an action or causes an Error Symbol Period TLV to be sent to the OAM entity, or a period of time in which symbol error events are counted. The **no** version disables monitoring of received symbol error events.



NOTE: You can configure this command multiple times to configure combinations of high and low threshold values or a window period for frame error events.

- Options**
- **link-monitor**—Configures link monitoring parameters. Link monitoring operations start automatically when Ethernet OAM is enabled on an interface. When link monitoring operations are disabled, the interface does not actively send or receive Event Notification OAM PDUs
 - **symbol-period**—Configures the threshold value or window for symbol error events
 - **threshold**—Configures a period or a value at, above, or below which an action is triggered
 - **highSymbols**—Integer in the range 1–65535 that is the high threshold in number of symbol error seconds, which when exceeded causes an action to be triggered. The action that the local OAM entity performs when the high threshold value is exceeded depends on the value configured using the **ethernet oam lfm high-threshold** command. There is no default value. If you specify a high threshold option for frame period summary error events, you must also enter the number of frames, which when exceeded causes the configured action to be taken
 - **none**—Removes the high threshold value for symbol error events
 - **lowSymbols**—Integer in the range 0–65535 that is the low threshold in number of symbol error seconds, which when exceeded causes an Error Symbol Period TLV to be sent to the peer; default value is 0 symbol error seconds. If you do not configure a low threshold for symbol error events, the Link Fault critical event PDU is not sent to the peer
 - **period**—A window and period of time during which symbol error events are counted. Integer in the range 1–60 seconds that is the monitoring period for symbol errors; there is no default value

Mode Interface Configuration

- Related Topics**
- OAM Link Monitoring Feature
 - Configuring 802.3ah OAM Link-Fault Management
 - `ethernet oam lfm link-monitor symbol-period` on page 587
 - `ethernet oam lfm link-monitor frame-seconds` on page 583
 - Example: Configuring 802.3ah OAM Link-Fault Management and Enabling Remote Failure Monitoring on an Interface

ethernet oam lfm mode

Syntax [no] ethernet oam lfm mode { active | passive } [pdu-lost-threshold *pduLostPackets*]

Release Information Command introduced in JUNOS Release 11.1.0.

Description Configures the discovery mode to be used for IEEE 802.3ah OAM link-fault management support on an interface as active or passive. Also, configures the number of OAM packet data units (PDUs) from the remote peer that an interface on the local client can miss before the link between the two entities is considered down. The default mode of the interface on the OAM client is active. The **no** version disables discovery, deactivating link-fault management functionality on the interface.

- Options**
- **mode**—Configures the OAM client mode for the discovery process
 - **active**—Sets the discovery mode of the local OAM client as active. In active mode, the interface discovers and monitors the peer on the link if the peer also supports IEEE 802.3ah OAM functionality. This is the default discovery mode of the OAM client
 - **passive**—Sets the discovery mode of the local OAM client as passive. In passive mode, an OAM entity does not initiate the discovery process. You cannot perform link-fault management if you configure both the local client and the remote peer for passive mode operation
 - ***pduLostPackets***—The window for which the local client waits to receive OAM packets from the remote peer before it generates a link fault event. Number of expected OAM packets from the remote peer that the local OAM client can miss before a link-fault event is triggered; a number in the range 3–10; default value is 5

Mode Interface Configuration

- Related Topics**
- OAM Discovery Feature
 - Guidelines for Configuring 802.3ah OAM Link-Fault Management
 - Configuring 802.3ah OAM Link-Fault Management

ethernet oam lfm pdu-lost-threshold

Syntax [no] ethernet oam lfm pdu-lost-threshold *pduLostPackets*

Release Information Command introduced in JUNOS Release 11.1.0.

Description Configures the number of OAM protocol data units (PDUs) that a local OAM client can fail to receive from a remote peer before a link-fault event is triggered. The **no** version removes the configured threshold for PDUs that can be missed from a remote peer before the generation of a link-fault event.

Options ■ *pduLostPackets*—Number of expected OAM packets from the remote peer that the local OAM client can miss before a link-fault event is triggered; a number in the range 3–10; default value is 5

Mode Interface Configuration

Related Topics ■ OAM Discovery Feature
 ■ Configuring 802.3ah OAM Link-Fault Management
 ■ ethernet oam lfm mode on page 589

ethernet oam lfm pdu-transmit-interval

Syntax [no] ethernet oam lfm pdu-transmit-interval *period* [mode { active | passive } | pdu-lost-threshold *pduLostPackets*]

Release Information Command introduced in JUNOS Release 11.1.0.

Description Configures the minimum rate at which OAM protocol data units (PDUs) are transmitted in milliseconds. Also, specifies the discovery mode of the OAM client and the number of OAM packet data units (PDUs) from the remote peer that an interface on the local client can miss before the link between the two entities is considered down. The **no** version removes the frequency values configured on the interface for transmission of OAM PDUs to the remote peer. The **no** version with the **mode** keyword deactivates link-fault management on the interface.

- Options**
- *period*—Interval at which OAM PDUs are sent from the local OAM entity to the remote peer to maintain the OAM association in an active state. Number in the range 100-1000 milliseconds; default value is 1000 milliseconds
 - *mode*—Configures the OAM client mode for the discovery process
 - *active*—Sets the discovery mode of the local OAM client as active. In active mode, the interface discovers and monitors the peer on the link if the peer also supports IEEE 802.3ah OAM functionality. This is the default discovery mode of the OAM client
 - *passive*—Sets the discovery mode of the local OAM client as passive. In passive mode, an OAM entity does not initiate the discovery process. You cannot perform link-fault management if you configure both the local client and the remote peer for passive mode operation
 - *pduLostPackets*—The window for which the local client waits to receive OAM packets from the remote peer before it generates a link fault event. Number of expected OAM packets from the remote peer that the local OAM client can miss before a link-fault event is triggered; a number in the range 3–10; default value is 5

Mode Interface Configuration

- Related Topics**
- OAM Discovery Feature
 - Configuring 802.3ah OAM Link-Fault Management
 - ethernet oam lfm mode on page 589

ethernet oam lfm remote-failure

Syntax [no] ethernet oam lfm remote-failure { critical-event | dying-gasp | link-fault } action { disable-interface | failover }

Release Information Command introduced in JUNOS Release 11.1.0.

Description Configures the Ethernet OAM link-fault management functionality to detect failure conditions that occurred in the receive path of the link, and to influence the state of the link based on an Event Notification PDU received from the remote peer. Also, specifies the action to be taken by the system when the configured link-fault event occurs, such as disabling the interface or causing a failover to another member link of a LAG bundle. The **no** version disables detection of remote faults and causes no action to be taken when a link-fault event occurs.

- Options**
- remote-failure—Enables detection of faults that occur in the receive path of an OAM link
 - critical-event—Enables detection of unspecified critical event conditions that occurred in the receive path of the link and influences the state of the link based on an Event Notification PDU received from the remote peer. This type of condition is vendor-specific
 - dying-gasp—Enables detection of unrecoverable error conditions that occurred in the receive path of the link and influences the state of the link based on an Event Notification PDU received from the remote peer. This type of condition is vendor-specific
 - link-fault—Enables detection of loss-of-signal conditions that occurred in the receive path of the link and influences the state of the link based on an Event Notification PDU received from the remote peer
 - action—Sets the action to be performed on an interface when an OAM PDU is received from the remote peer by the local OAM entity to signal a fault condition in the receive path of the link
 - disable-interface—Sets the OAM functionality to unconditionally attempt to influence the operational state of the interface to down
 - failover—Causes a failover to another member interface in the LAG bundle when the high threshold for an error is exceeded that trigger the sending of link event TLVs. On GE-2 and GE-HDE line modules that are paired with GE-2 SFP I/O modules with physical link redundancy, causes the link to transition from active to redundant

Mode Interface Configuration

- Related Topics**
- OAM Remote Fault Detection Feature
 - Configuring 802.3ah OAM Link-Fault Management

- Example: Configuring 802.3ah OAM Link-Fault Management and Enabling Remote Failure Monitoring on an Interface

ethernet oam lfm remote-loopback

Syntax ethernet oam lfm remote-loopback { start | stop } *interfaceType interfaceSpecifier*

Release Information Command introduced in JUNOS Release 11.1.0.

Description Enables or disables remote loopback functionality on the remote OAM entity. Also causes the remote peer to commence or halt sending of all received frames from the local entity to the specified interface, except OAM PDUs, without any changes made to the frames. OAM PDUs continue to be processed. By default, the remote peer does not loop back the non-OAM PDUs that it receives from the local entity. There is no **no** version.

This configuration setting is not preserved across a reboot.

- Options**
- start—Commences the remote loopback operation on the remote OAM entity
 - stop—Halts the remote loopback operation on the remote OAM entity; this is the default behavior
 - *interfaceType*—One of the following interface types listed in “Interface Types and Specifiers” on page 5
 - fastEthernet
 - gigabitEthernet
 - tenGigabitEthernet
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec

- Related Topics**
- OAM Remote and Local Loopback Feature
 - ethernet oam lfm remote-loopback supported on page 595
 - Configuring 802.3ah OAM Link-Fault Management
 - Example: Enabling Remote Loopback Support on the Local Interface

ethernet oam lfm remote-loopback supported

Syntax [no] ethernet oam lfm remote-loopback supported

Release Information Command introduced in JUNOS Release 11.1.0.

Description Configures Ethernet OAM remote loopback functionality on an interface and causes the interface to receive and respond to remote loopback requests from peers. The **no** version disables the remote loopback behavior on the interface, which is the default behavior.

- Options**
- remote-loopback—Configures a local interface to be placed into remote loopback mode and enables the local interface to respond to remote loopback requests that it receives from a peer OAM entity
 - supported—Enables the Ethernet OAM configuration on the interface to initiate remote loopback or respond to a remote loopback request it receives from a peer

Mode Interface Configuration

- Related Topics**
- OAM Remote and Local Loopback Feature
 - ethernet oam lfm remote-loopback on page 594
 - Configuring 802.3ah OAM Link-Fault Management
 - Example: Enabling Remote Loopback Support on the Local Interface

event

Syntax [no] event *eventOwner eventName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates an event and launches the event configuration mode in the SNMP server event manager. The **no** version removes the event.

- Options**
- *eventOwner*—Owner associated with this event; string of up to 32 alphanumeric characters
 - *eventName*—Name associated with this event; string of up to 32 alphanumeric characters

Mode SNMP Event Manager Configuration

exceeded-action

Syntax For IP and IPv6 rate-limit profiles:

```
[ no ] exceeded-action { drop | transmit | mark markVal }
```

For L2TP rate-limit profiles:

```
[ no ] exceeded-action { drop | transmit }
```

For MPLS rate-limit profiles:

```
[ no ] exceeded-action { drop | transmit | mark-exp expValue }
```

For hierarchical rate-limit profiles:

```
[ no ] exceeded-action { drop | transmit [ conditional | final ] }
```

Release Information Command introduced before JUNOS Release 7.1.0.
conditional and **final** keywords added in JUNOS Release 7.2.0.

Description Sets the action for packets not conforming to the committed rate and committed burst size, and not conforming to the peak rate and peak burst size. The **no** version restores the default, drop.

- Options**
- drop—Drops the packet
 - transmit—Transmits the packet; for hierarchical rate limits:
 - conditional—Packets must pass the next rate limit
 - final—Packets exit the hierarchy at rate limit
 - *markVal*—Marks value in the range 0–255; mark actions are not supported on hierarchical rate limits
 - *expValue*—EXP bit value in the range 0–7

Mode Rate Limit Profile Configuration

Related Topics

- Creating a Two-Rate Rate-Limit Profile

exceeded-drop-threshold

Syntax `exceeded-drop-threshold exceededDropThreshold`
 `no exceeded-drop-threshold`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the threshold above which exceeded-drop-events are logged. The **no** version removes the threshold.

Options ■ *exceededDropThreshold*—Bits per second in the range 0–1073741824

Mode Statistics Profile Configuration

Related Topics ■ [Configuring Event Statistics](#)

exceeded-fraction

Syntax `exceeded-fraction exceededFraction`
`no exceeded-fraction`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the percentage of the total queue length that can be occupied before dropping exceeded packets. The **no** version returns the exceeded fraction to its default setting.

Options ■ *exceededFraction*—Percentage range 0–100; default value is 25

Mode Queue Profile Configuration

Related Topics ■ Configuring Queue Profiles to Manage Buffers and Thresholds

exceeded-length

Syntax `exceeded-length minimumExceededLength [maximumExceededLength]`
`no exceeded-length`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets minimum and maximum constraints for the queue's exceeded lengths. The **no** version removes constraints on the queue's exceeded length.

- Options** ■ *minimumExceededLength*—Range 0–1073741824
 ■ *maximumExceededLength*—Range 0–1073741824

Mode Queue Profile Configuration

- Related Topics** ■ Configuring Queue Profiles to Manage Buffers and Thresholds

exceeded-threshold

Syntax `exceeded-threshold { percent MinThresholdPercent MaxThresholdPercent |
 MinThresholdBytes MaxThresholdBytes } MaxDropProbability`
 `no exceeded-threshold`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the exceeded queue thresholds and maximum drop probability. The **no** version removes exceeded threshold.

- Options**
- `percent`—Specifies *exceeded* queue thresholds as percentages
 - `MinThresholdPercent`—Minimum queue threshold as a percentage of queue length
 - `MaxThresholdPercent`—Maximum queue threshold as a percentage of queue length
 - `MinThresholdBytes`—Minimum queue threshold in bytes
 - `MaxThresholdBytes`—Maximum queue threshold in bytes
 - `MaxDropProbability`—Maximum drop probability

Mode Drop Profile Configuration

- Related Topics**
- Configuring RED
 - Configuring WRED

exception dump

Syntax exception dump { except-srp | srp-only } { local | *ipAddress* [*directoryName*] }
no exception dump

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the location from and to which the router should transfer a core dump file. Core dumps are enabled and stored in local NVS by default. The **no** version disables the command.

- Options**
- except-srp—Generates core dump for all non-SRP modules
 - srp-only—Generates core dump for only the SRP modules
 - local—Nonvolatile storage memory
 - *ipAddress*—IP address of the server to which the router will transfer the core dump file
 - *directoryName*—Name of the directory on the server to which the router will transfer the core dump file

Mode Global Configuration

exception gateway

Syntax exception gateway *ipAddress*
 no exception gateway

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the gateway through which the router sends the core dump file to the remote FTP server. The **no** version returns the value to its default (null).

Options ■ *ipAddress*—IP address of the gateway

Mode Global Configuration

exception http-redirect

Syntax [no] exception http-redirect

Release Information Command introduced in JUNOS Release 7.2.0.

Description Creates the exception rule within an IPv4 or IPv6 policy classifier group so the application can perform an application-dependent action on the content of the packet. HTTP redirect is the only application that is available as a destination of the exception rule. The **no** version removes the exception rule.

This command is not supported for the ES2 10G Uplink LM.

Mode Classifier Group Configuration

- Related Topics**
- Assigning Values to the ATM CLP Bit
 - Creating an Exception Rule within a Policy Classifier Group

exception monitor

Syntax exception monitor *ipAddress* [*directoryName*]
 no exception monitor

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the core dump monitor and specifies the location to which the router transfers core dump files. The **no** version disables the core dump monitor.

- Options** ■ *ipAddress*—IP address of the server to which you want the router to transfer core dump files
- *directoryName*—Name of the directory on the server to which you want the router to transfer core dump files

Mode Global Configuration

exception monitor interval

Syntax exception monitor interval *interval*
 no exception monitor interval

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the interval at which you want the router to check NVS for core dump files. The **no** version disables the core dump monitor.

Options ■ *interval*—Number of minutes between NVS checks; in the range 1–1440

Mode Global Configuration

exception protocol ftp

Syntax exception protocol ftp [[*algorithmType*] *userName* [[*algorithmType*] *password*]]
no exception protocol

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the username and password for FTP access to a host where you transferred a core dump file. The **no** version restores the defaults.

- Options**
- *algorithmType*—Type of user name or password
 - 0—Indicates the *password* is unencrypted; the default
 - 8—Indicates the *password* is encrypted
 - *userName*—Username required to access the FTP server; the default username is anonymous
 - *password*—Password required to access the FTP server; default value is no password

Mode Global Configuration

exception source

Syntax exception source *ipAddress ipAddressMask*
 no exception source

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the IP address and mask of the router interface over which you want to send the core dump file to the remote FTP server. The **no** version returns the value to its default (null).

- Options** ■ *ipAddress*—IP address of the interface
 ■ *ipAddressMask*—Optionally add the IP address mask of the interface

Mode Global Configuration

excess-burst

Syntax `excess-burst { size | millisecond milliseconds }`
 `no excess-burst`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets amount of bandwidth allocated to accommodate a packet in progress when the rate is in excess of the burst. The **no** version restores the default value, 0.

- Options** ■ *size*—Amount of bandwidth allocated; in the range 0–4294967295
 ■ *milliseconds*—Milliseconds in the range 1–10000

Mode Rate Limit Profile Configuration

- Related Topics** ■ Creating a Two-Rate Rate-Limit Profile

exclude-prefix

Syntax [no] exclude-prefix *Ipv6Prefix* [*endIpv6prefix*]

Release Information Command introduced in JUNOS Release 10.1.0.

Description Specifies the IPv6 prefix or range of prefixes to exclude from being allocated to the requesting router. You can exclude those prefixes that have been assigned to local interfaces from being delegated to the DHCPv6 clients. The **no** version removes the IPv6 prefix or prefix range from the exclusion set and makes it available again for delegation to clients.



NOTE: If you attempt to exclude a prefix range that overlaps with another prefix range that has been already excluded from delegation to clients in the IPv6 local address pool, an error message is displayed and the configuration fails.

- Options**
- *Ipv6Prefix*—IPv6 prefix or the starting IPv6 prefix of the range of prefixes to be excluded from being delegated to the requesting router.
 - *endIpv6Prefix*—Ending prefix of the range of IPv6 prefixes to be excluded from being delegated to the requesting router. If you specify this value, all prefixes from the starting IPv6 prefix up to this prefix are excluded from allocation.

Mode IPv6 Local Pool Configuration

exclude-subsystem

Syntax `exclude-subsystem subsystemName`
 `no exclude-subsystem [subsystemName]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Excludes subsystem files from being copied when you copy a software release to the router. The **no** version removes the exclusion for a specified subsystem file or all subsystem files.

Options ■ *subsystemName*—Name of the subsystem file to be excluded

Mode Global Configuration

exec-banner

Syntax [no | default] exec-banner

Release Information Command introduced before JUNOS Release 7.1.0.

Description Controls display of an exec banner (configured with the **banner** command) on a particular line after user authentication (if any) and before the first prompt of a CLI session. The **no** version disables the exec banner and the motd banner on the line. The **default** version restores the default setting, in which the banner is enabled on all lines.

Mode Line Configuration

exec-timeout

Syntax `exec-timeout minutes [seconds]`

`no exec-timeout`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the time interval that the console or vty line waits for expected user input. The **no** version restores the default value, which is no time limit.

- Options**
- *minutes*—Number of minutes for the time limit; in the range from 0 to 35791
 - *seconds*—Number of seconds in addition to the minutes for the time limit; in the range from 0 to 2147483

Mode Line Configuration

existence-test

Syntax `existence-test { event eventOwner eventName |
startup { absent | present } | test-type { absent | changed | present } }`

`no existence-test [event | startup | test-type]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines existence test values for the trigger that you are configuring, including binding an event to the existence-test trigger, specifying a startup condition, and defining an existence-test type. The **no** version deletes the existence-test values for this trigger or removes either the startup condition or event binding.

- Options**
- *eventOwner*—Name of event owner that partially specifies event to trigger the existence test; string of up to 32 alphanumeric characters
 - *eventName*—Name of event that partially specifies event to trigger the existence test; string of up to 32 alphanumeric characters
 - *startup*—Specifies startup existence condition that you predict the sample to follow; absent or present; you can specify both conditions in the same command
 - *test-type*—Specifies type of existence test to perform; absent, changed, or present; you can specify one, two, or all three conditions in the same command

Mode SNMP Trigger Configuration

exit

Syntax exit

Release Information Command introduced before JUNOS Release 7.1.0.

Description Exits the current command mode. In User Exec and Privileged Exec modes, logs out of the CLI. There is no **no** version.

Mode All modes

exit-address-family

Syntax exit-address-family

Release Information Command introduced before JUNOS Release 7.1.0.

Description Exits from Address Family Configuration mode and returns to Router Configuration mode. There is no **no** version.

Mode Address Family Configuration

Related Topics ■ *Configuring BGP Signaling for L2VPNs and Configuring BGP Signaling for VPLS in the JUNOS BGP and MPLS Configuration Guide*

exit-remote-neighbor

Syntax exit-remote-neighbor

Release Information Command introduced before JUNOS Release 7.1.0.

Description Exits from Remote Neighbor Configuration mode and returns to Router Configuration mode. There is no **no** version.

Mode Remote Neighbor Configuration

exp-mask

Syntax [no] exp-mask *maskValue*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the EXP mask to be applied with the mark values. The **no** version restores the default mask of 7.

Options ■ *maskValue*—EXP mask value in the range 0–7

Mode Rate Limit Profile Configuration

Related Topics ■ Creating a Two-Rate Rate-Limit Profile

export destination

Syntax [no] export destination { *hostName* | *ipAddress* } udp-port

Release Information Command introduced in JUNOS Release 8.1.0.

Description Configures an export destination for the aggregation cache. The **no** version removes the destination.

- Options**
- *hostName*—Name of the destination host
 - *ipAddress*—Address of IP interface
 - udp-port—Specifies UDP port as the destination

Mode Flow Cache Configuration

export map

Syntax export map [ipv4 | ipv6] *routeMap* [filter]
 no export map [ipv4 | ipv6]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Associates a route map with a VRF to modify or filter routes exported by the VRF to the global BGP VPN RIB in the parent VR. Both IPv4 and IPv6 routes are exported unless you issue the appropriate keyword to restrict exportation. The **no** version restores the default behavior, which is to export all routes without applying a route map.

- Options**
- *ipv4*—Specifies that only IPv4 routes are exported to the global BGP VPN RIB
 - *ipv6*—Specifies that only IPv6 routes are exported to the global BGP VPN RIB
 - *routeMap*—Name of a route map; string of up to 32 alphanumeric characters
 - *filter*—Prevents routes that do not match the route map from being exported; if absent, such routes are exported but their attributes are not modified by the route map

Mode VRF Configuration

export source

Syntax [no] export source interface *interface*

Release Information Command introduced in JUNOS Release 8.1.0.

Description Sets the source IP address for datagrams containing information from the cache. The **no** version removes the setting of the IP address.

Options ■ *interface*—Name of the interface

Mode Flow Cache Configuration

extended-authentication

Syntax extended-authentication { none | pap | chap } [re-authenticate]
 [skip-peer-config]

no extended-authentication

Release Information Command introduced in JUNOS Release 7.3.0.

Description Specifies the extended user authentication protocol for use during the extended user authentication protocol exchange. The **re-authenticate** keyword enables the reauthentication option (a second authentication procedure). The **skip-peer-config** keyword disables the router from configuring peer IP characteristics. The **no** version restores the default protocol, pap.

- Options**
- none—Specifies that no extended authentication is performed
 - pap—Specifies the use of PAP protocol for extended authentication
 - chap—Specifies the use of CHAP protocol for extended authentication
 - re-authenticate—Enables reauthentication when IKE SA rekeying occurs
 - skip-peer-config—Disables configuration of peer IP characteristics

Mode IPSec Tunnel Profile Configuration

external-paths

Syntax external-paths *limit*
 no external-paths

Release Information Command introduced in JUNOS Release 8.2.0.

Description Configures the maximum number of received external BGP best paths allowed for route-target signaling. The **no** version restores the default value, 1.

Options ■ *limit*—Number of paths, in the range 1–255

Mode Address Family Configuration, Router Configuration

Chapter 7

F Commands

fabric-strict-priority

Syntax [no] fabric-strict-priority

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies strict priority scheduling for queues in the traffic class in the fabric. The **no** version deletes the strict priority setting.

Mode Traffic Class Configuration

fabric-weight

Syntax fabric-weight *weight*
 no fabric-weight

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the relative weight for queues in the traffic class in the fabric. The **no** version sets the fabric weight to the default value.

Options ■ *weight*—Range 1–63; default value is 8

Mode Traffic Class Configuration

fabric weights

Syntax fabric weights multicast *multicastValue* unicast *unicastValue*
no fabric weights

Release Information Command introduced in JUNOS Release 7.2.0.

Description Defines the multicast-to-unicast traffic ratio for the ERX1440, ERX310, E120, or E320 router switch fabric. The **no** version returns the switch fabric to its default multicast:unicast ratio (15:2).

- Options**
- *multicastValue*—Ratio value of multicast bandwidth in the range 1–15
 - *unicastValue*—Ratio value of unicast bandwidth in the range 1–15

Mode Global Configuration

failover-resync

Syntax failover-resync { failover-protocol | failover-protocol-fallback-to-silent-failover |
silent-failover | disable | not-configured }

no failover-resync

Release Information Command introduced in JUNOS Release 7.3.0.

Description Configures the L2TP peer resynchronization method that an L2TP failed endpoint uses to resynchronize with its peer non-failed endpoint. This command configures peer resynchronization for a host profile or a domain map tunnel, and overrides a global peer resynchronization method that is specified in Global Configuration mode. The **no** version restores the default setting, not-configured.

- Options**
- failover-protocol—Specifies the L2TP failover protocol method
 - failover-protocol-fallback-to-silent-failover—Specifies the L2TP failover protocol method; however, if the peer does not support this method, the silent failover method is used
 - silent-failover—Specifies the silent failover method
 - disable—Disables peer resynchronization
 - not-configured—Specifies that peer resynchronization is not configured for L2TP host profiles and AAA domain map tunnels. L2TP uses the global failover method; the default setting

Mode Domain Map Tunnel Configuration, L2TP Destination Profile Host Configuration

filter

Syntax [no] [suspend] filter

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a policy rule that drops all packets conforming to the current classifier control list and can be used while the policy list is referenced by interfaces. The **no** version removes the filter rule from the policy list; the **suspend** version temporarily suspends the policy rule; the **no suspend** version resumes application of a suspended rule.



NOTE: This command replaces the Policy List Configuration version of the **filter** command, which may be removed completely in a future release.

Mode Classifier Group Configuration

Related Topics ■ Policy Rule Precedence

flash-disk compare

Syntax flash-disk compare { all | configuration }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Performs a checksum validation that compares the contents of the NVS file system on the primary SRP module with the contents of the NVS file system on the redundant SRP module, and detects any differences. The command validates only those files that are synchronized between the primary and redundant SRP modules; it does not validate log files, core dump files, and other files that are excluded from the system synchronization process. There is no **no** version.

- Options**
- all—Compares all files in NVS; this option can take several minutes to complete
 - configuration—Compares only configuration files; this option takes less time to complete because it compares only a subset of the files in the NVS file system

Mode Privileged Exec

flash-disk duplicate

Syntax flash-disk duplicate

Release Information Command introduced before JUNOS Release 7.1.0.

Description Copies the contents of NVS on the primary SRP module to another NVS card. There is no **no** version.

Mode Boot

flash-disk initialize

Syntax flash-disk initialize [no-format] [disk0 | disk1]

Release Information Command introduced before JUNOS Release 7.1.0.
disk0 and **disk1** keywords added in JUNOS Release 7.2.0.
Privileged Exec mode added in JUNOS Release 8.0.0.

Description Performs a low-level format of unmounted flash cards. There is no **no** version.

- Options**
- no-format—Erases all files but does not format the flash card
 - disk0—Specifies flash card in slot 0 of the SRP module; default value is disk0; available only in Boot mode, because disk0 cannot be in an unmounted state in a router outside of Boot mode
 - disk1—Specifies flash card in slot 1 of the SRP module; supported only on the E120 router and the E320 router

Mode Boot, Privileged Exec

flash-disk scan

Syntax flash-disk scan [repair] [disk0 | disk1]

Release Information Command introduced before JUNOS Release 7.1.0.
disk0 and **disk1** keywords added in JUNOS Release 7.2.0.
Privileged Exec mode added in JUNOS Release 8.0.0.

Description Scans the flash card on the primary SRP module to detect corrupt sectors, deletes files and directories that contain corrupt sectors, and fixes nonfatal errors. There is no **no** version.

- Options**
- repair—Repairs nonfatal errors detected on flash disk
 - disk0—Specifies flash card in slot 0 of the SRP module; default value is disk0; available only in Boot mode, because disk0 cannot be in an unmounted state in a router outside of Boot mode
 - disk1—Specifies flash card in slot 1 of the SRP module; supported only on the E120 router and the E320 router

Mode Boot, Privileged Exec

forward

Syntax [no] [suspend] forward
 [interface *interfaceType* *interfaceSpecifier* [next-hop *nextHop*
 [ignore-default-route]]
 [order *orderValue*]] | [next-hop *nextHop* [virtual-router *vrName*]
 [ignore-default-route] [order *orderValue*]] |
 [order *orderValue*] | classifier-group *claclName*] [precedence *precValue*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a rule to forward all packets that match the specified classifier control list. If you do not specify a classifier control list using the **classifier-group** keyword, the router will select all packets from the interface in the direction of the attached policy list. The **no** version removes the rule from the policy list; the **suspend** version temporarily suspends the forward rule; the **no suspend** version resumes application of a suspended rule.

See the **forward interface** and **forward next-hop** commands for descriptions of the Classifier Group Configuration mode versions of this command.

- Options**
- *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5 (IP policy lists only)
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see “Interface Types and Specifiers” on page 5 (IP policy lists only)
 - *nextHop*—Next-hop IP address (IP policy lists only)
 - ignore-default-route—Ignores the default route as a consideration for the next hop (IP policy lists only)
 - *vrName*—Name of the virtual router (IP policy lists only)
 - *orderValue*—Order of this forward rule within the single classifier; in the range 1–32767; default value is 100 (IP policy lists only)
 - *claclName*—Classifier control list used to classify packets for this policy
 - *precValue*—Precedence of this rule in relation to other rules within this set: in the range 0–32768; default value is 100

Mode Policy List Configuration

Related Topics ■ Assigning Values to the ATM CLP Bit

forward interface

Syntax [no] [suspend] forward [interface *interfaceType* *interfaceSpecifier*
[next-hop *nextHop* [ignore-default-route]] [order *orderValue*]]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a rule to forward all packets that match the current classifier control list. The **no** version removes the rule from the policy list; the **suspend** version temporarily suspends the forward rule; the **no suspend** version resumes application of a suspended rule.



NOTE: The **forward interface** command replaces the **next-interface** command, which may be removed completely in a future release.

- Options**
- *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *nextHop*—Next-hop IP address
 - ignore-default-route—Ignores the default route as a consideration for the next hop
 - *orderValue*—Order of this forward rule within the single classifier; in the range 1–32767; default value is 100

Mode Classifier Group Configuration

Related Topics ■ Assigning Values to the ATM CLP Bit

forward next-hop

Syntax [no] [suspend] forward next-hop *nextHop* [virtual-router *vrName*]
[ignore-default-route] [order *orderValue*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a rule to forward all packets that match the current classifier control list. The **no** version removes the rule from the policy list; the **suspend** version temporarily suspends the forward rule; the **no suspend** version resumes application of a suspended rule.



NOTE: The **forward next-hop** command replaces the **next-hop** command, which may be removed completely in a future release.

- Options**
- *nextHop*—Next-hop IP address
 - *vrName*—Name of the virtual router
 - ignore-default-route—Ignores the default route as a consideration for the next hop
 - *orderValue*—Order of this forward rule within the single classifier; in the range 1–32767; default value is 100

Mode Classifier Group Configuration

Related Topics ■ Assigning Values to the ATM CLP Bit

forwarding-rate-threshold

Syntax forwarding-rate-threshold *forwardingRateThreshold*
no forwarding-rate-threshold

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the threshold above which forwarded-rate-exceeded events are logged. The **no** version removes the threshold.

Options ■ *forwardingRateThreshold*—Bits per second in the range 0–1073741824

Mode Statistics Profile Configuration

Related Topics ■ [Configuring Event Statistics](#)

forwarding-table route-holddown

Syntax forwarding-table route-holddown *timerValue*
no forwarding-table route-holddown

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the number of seconds allowed after a routing table change for the accumulation of additional updates and subsequent distribution of the set of routing table changes to the line modules. The **no** version sets the hold-down time to the default value (3 seconds).

Options ■ *timerValue*—Number of seconds allowed for the accumulation and subsequent distribution of routing table updates to the line modules; a range of 0-30 seconds, where 0 specifies an update following each routing table change

Mode Global Configuration

frame-relay class

Syntax [no] frame-relay class *mapName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Associates a map class with a subinterface. The **no** version removes the association between the map class and the subinterface.

Options ■ *mapName*—Name of the map class; use up to 64 characters

Mode Subinterface Configuration

frame-relay classifier-list

Syntax frame-relay classifier-list *classifierName* [traffic-class *trafficClassName*]
 [color { green | yellow | red }] [user-packet-class *userPacketClassValue*]
 [de-bit *deValue*]

no frame-relay classifier-list *classifierName* [*classifierNumber*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates or modifies a Frame Relay classifier control list. The **no** version removes the classifier control list.

- Options**
- *classifierName*—Name of the classifier control list entry
 - *trafficClassName*—Name of the traffic class to match
 - green—Matches packet color to green, indicating a low drop preference
 - yellow—Matches packet color to yellow, indicating a medium drop preference
 - red—Matches packet color to red, indicating a high drop preference
 - *userPacketClassValue*—User packet value to match in the range 0–15
 - *deValue*—Value of the DE bit to match; 0 or 1

Mode Global Configuration

Related Topics

- Creating or Modifying Classifier Control Lists for Frame-Relay Policy Lists

frame-relay description

Syntax frame-relay description *name*
 no frame-relay description

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns a text description or an alias to a Frame Relay interface or subinterface. Use the show frame-relay interface or show frame-relay subinterface command to display the text description. The **no** version removes the description or alias.

Options ■ *name*—Text string or alias of up to 80 characters for the Frame Relay interface or subinterface

Mode Interface Configuration, Subinterface Configuration

frame-relay dos-protection-group

Syntax frame-relay dos-protection-group *groupName*
 no frame-relay dos-protection-group

Release Information Command introduced in JUNOS Release 8.1.0.

Description Attaches a Frame Relay denial of service (DoS) protection group to an interface. The **no** version removes the attachment of the DoS protection group from the interface.

Options ■ *groupName*—Name of the DoS protection group; string of up to 31 alphanumeric characters

Mode Interface Configuration

frame-relay fragment

Syntax frame-relay fragment [[*fragmentSize*] [fragmentation-only] | reassembly-only]
no frame-relay fragment

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures fragmentation and reassembly for the map class created with the **map-class frame-relay** command. The **no** version stops fragmentation and/or reassembly on the subinterface.

- Options**
- *fragmentSize*—Maximum payload size of a fragment in bytes; a number in the range 16–8188; default value is 52
 - fragmentation-only—Specifies fragmentation only
 - reassembly-only—Specifies reassembly only

Mode Map Class Configuration

frame-relay interface-dlci ietf

Syntax frame-relay interface-dlci *dlci* ietf
 no frame-relay interface-dlci *dlci*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns a data-link connection identifier to a specified Frame Relay subinterface on the router or access server. The DLCI number identifies a virtual circuit. The **no** version removes this assignment.

Options ■ *dlci*—DLCI number to be used on the specified subinterface to identify a virtual circuit in the range 16–1007

Mode Subinterface Configuration

Related Topics ■ *Configuring Frame Relay Layer 2 Services* in the *JUNOS BGP and MPLS Configuration Guide*

frame-relay intf-type

Syntax frame-relay intf-type *type*
 no frame-relay intf-type

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures a Frame Relay interface type. The **no** version restores the default value, DTE.

- Options** ■ *type*—One of the following interface types:
- dce—Router is connected to user DTE equipment
 - dte—Router is connected to a Frame Relay network; the default
 - nni—Router connects two Frame Relay networks

Mode Interface Configuration

Related Topics ■ *Configuring Frame Relay Layer 2 Services* in the *JUNOS BGP and MPLS Configuration Guide*

frame-relay keepalive

Syntax frame-relay keepalive [*seconds*]
 no frame-relay keepalive

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the LMI mechanism for serial lines using Frame Relay encapsulation. The **no** version disables this capability. The keepalive command is similar to the **frame-relay lmi-t391dte** command.

Options ■ *seconds*—Number in the range 5–30; default value is 10 seconds; defines the keepalive interval; the interval must be set, and the value on the DTE should be less than the value set on the DCE

Mode Interface Configuration

frame-relay lmi-n391dte

Syntax frame-relay lmi-n391dte *keepExchanges*
 no frame-relay lmi-n391dte

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the full-status polling counter (N391) on a DTE interface. The **no** version restores the default value, assuming an LMI has been configured.

Options ■ *keepExchanges*—Number in the range 1 – 255; default value is 6; number of keep exchanges to be done before requesting a full-status message. If you specify a value of 1, you receive full-status messages only.

Mode Interface Configuration

frame-relay lmi-n392dce

Syntax frame-relay lmi-n392dce *threshold*
 no frame-relay lmi-n392dce

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the error threshold counter (N392) on a DCE interface. The **no** version removes current setting and sets the default.

Options ■ *threshold*—Positive number in the range 1–10; number of errors that will place the interface in an operationally down state; default value is 2 errors

Mode Interface Configuration

frame-relay lmi-n392dte

Syntax frame-relay lmi-n392dte *threshold*
 no frame-relay lmi-n392dte

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the error threshold counter (N392) on a DTE interface. The **no** version removes current setting and sets the default.

Options ■ *threshold*—Positive number in the range 1–10; number of errors that will place the interface in an operationally down state; default value is 3 errors

Mode Interface Configuration

frame-relay lmi-n393dce

Syntax frame-relay lmi-n393dce *events*
 no frame-relay lmi-n393dce

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the monitored events count (N393) on a DCE interface. The **no** version removes current setting and sets the default.

Options ■ *events*—Number in the range 1–10 events; specifies the diagnostic window used to verify link integrity; default value is 2 events (The detection of N392 errors within the window of N393 samples places the interface in an operationally down state.)

Mode Interface Configuration

frame-relay lmi-n393dte

Syntax frame-relay lmi-n393dte *events*
 no frame-relay lmi-n393dte

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the monitored event count (N393) on a DTE interface. The **no** version removes current setting and sets the default.

Options ■ *events*—Number in the range 1–10 events; default value is 4 events; specifies the diagnostic window used to verify link integrity (the detection of N392 errors within the window of N393 samples places the interface in an operationally down state)

Mode Interface Configuration

frame-relay lmi-t391dte

Syntax frame-relay lmi-t391dte *seconds*
 no frame-relay lmi-t391dte

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the link integrity verification polling timer (T391) on a DTE interface. The **no** version removes the current setting and sets the default.

Options ■ *seconds*—Number in the range 5–30 seconds; specifies the interval in seconds between status inquiries issued by the DTE; default value is 10 seconds

Mode Interface Configuration

frame-relay lmi-t392dce

Syntax frame-relay lmi-t392dce *seconds*
 no frame-relay lmi-t392dce

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the polling verification timer (T392) on a DCE interface. The **no** version removes current setting and sets the default.

Options ■ *seconds*—Number in the range 5–30 seconds; specifies the expected interval in seconds between status inquiries issued by the DTE equipment; default value is 15 seconds

Mode Interface Configuration

frame-relay lmi-type

Syntax frame-relay lmi-type *type*
 no frame-relay lmi-type

Release Information Command introduced before JUNOS Release 7.1.0.

Description Selects the LMI type. The **no** version restores the default value.

- Options** ■ *type*—One of the following types:
- ansi—ANSI T1.617 Annex D
 - cisco—Original Group of Four specification developed by DEC, Northern Telecom, Stratacom, and Cisco
 - q933a—ITU-T Q.933 Annex A
 - none—No management interface is used

Mode Interface Configuration

Related Topics ■ *Configuring Frame Relay Layer 2 Services* in the *JUNOS BGP and MPLS Configuration Guide*

frame-relay policy

Syntax frame-relay policy { input | output } *policyName*
 [statistics { enabled [baseline { enabled | disabled }] [preserve | merge] |
 disabled [merge] } | merge]

no frame-relay policy { input | output } [*policyName*]

Release Information Command introduced before JUNOS Release 7.1.0.
merge keyword added in JUNOS Release 7.2.0.

Description Assigns a policy list to the ingress or egress of a Frame Relay interface. If you enter this command when the policy list does not exist, the router will create a policy list with a filter rule as the default. You must specify the **input** or **output** keyword to assign the policy list to the ingress or egress of the interface. The **no** version removes the association between a policy list and an interface.

- Options**
- input—Applies policy to data arriving at this interface
 - output—Applies policy to data leaving this interface
 - *policyName*—Name of the policy; a maximum of 40 characters
 - statistics—Enables or disable collection of policy routing statistics
 - enabled—Enables collection of policy routing statistics
 - baseline enabled—Enables baselining of policy routing statistics
 - baseline disabled—Disables baselining of policy routing statistics
 - preserve—Preserves existing statistics for any classifier-list that is the same for both the new and old policy attachments when you attach a new policy to an interface
 - disabled—Disables collection of policy routing statistics
 - merge—Enables merging of multiple policies to form a single policy

Mode Interface Configuration

Related Topics ■ Setting a Statistics Baseline for Policies

frame-relay policy-list

Syntax [no] frame-relay policy-list *policyName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates or modifies a Frame Relay policy list and accesses Policy List Configuration mode. If you execute a **frame-relay policy-list** command and type **exit**, the router creates a policy list with a filter rule as the default. Attaching this policy list to an interface filters all packets on that interface. The **no** version removes a policy list.

Options ■ *policyName*—Name of the policy list

Mode Global Configuration

Related Topics ■ Creating Policy Lists for Frame Relay

framing

Syntax framing *framingType*
 no framing

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the framing mode used by E3 or T3 interfaces. Available modes vary by the type of interface. The **no** version restores the default for that interface.

- Options** ■ *framingType*—One of the following framing types:
- E3 Frame
 - g751—Default; G.751 compliant frame
 - g832—G.832 compliant frame
 - T3
 - c-bit—Default; specifies c-bit parity framing
 - m23—Specifies M23 multiplexer framing

Mode Controller Configuration

frequency

Syntax *frequency frequencyValue*
 no frequency

Release Information Command introduced before JUNOS Release 7.1.0.

Description In RTR Configuration mode, sets the time interval between RTR operations. In SNMP Event Manager Configuration mode, sets the frequency (in seconds) at which you want MIB sampling to occur. The **no** version restores the default value.

Options ■ *frequencyValue*—Number of seconds between RTR operations or MIB sampling operations, depending on the configuration mode; with RTR operations, for both types (echo and pathEcho), the default value is 60 seconds; with MIB sampling, the default value is 600 seconds.

Mode RTR Configuration, SNMP Event Manager Configuration

ftp-server enable

Syntax [no] ftp-server enable

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the FTP server and monitors the FTP port for attempts to connect to the FTP server. The **no** version terminates the current FTP sessions and disables the FTP server.

Mode Global Configuration

ftp-server flush

Syntax	ftp-server flush
Release Information	Command introduced in JUNOS Release 10.0.0.
Description	Forcibly terminates existing file transfer sessions to enable unified ISSU to proceed successfully. There is no no version.
Mode	Privileged Exec
Related Topics	■ <i>FTP Server File Transfers Behaviors in the JUNOS System Basics Configuration Guide</i>

full-spf-always

Syntax [no] full-spf-always

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables full SPF calculations for ISIS network changes. The **no** version restores partial route calculation (PRC) mode for SPF calculations.

Mode Router Configuration

Chapter 8

G Commands

global export map

Syntax global export map [ipv4 | ipv6] *routeMap*
 no global export map [ipv4 | ipv6]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Associates a route map with a VRF to modify and filter routes exported by the VRF to the global BGP non-VPN RIB in the parent VR. Both IPv4 and IPv6 routes are exported unless you issue the appropriate keyword to restrict exportation. The **no** version disables the exporting of routes to the global BGP non-VPN RIB.

- Options**
- **ipv4**—Specifies that only IPv4 routes are exported to the global BGP non-VPN RIB
 - **ipv6**—Specifies that only IPv6 routes are exported to the global BGP non-VPN RIB
 - ***routeMap***—Name of a route map; string of up to 32 alphanumeric characters

Mode VRF Configuration

global import map

Syntax `global import map [ipv4 | ipv6] routeMap max-routes maxNumber`
 `no global import map [ipv4 | ipv6]`

Release Information Command introduced in JUNOS Release 7.1.0.

Description Associates a route map with a VRF to modify and filter routes imported by the VRF from the global BGP non-VPN RIB in the parent VR. Both IPv4 and IPv6 routes are imported unless you issue the appropriate keyword to restrict importation. The **no** version disables the importing of routes from the global BGP non-VPN RIB to the VRF RIB.

- Options**
- `ipv4`—Specifies that only IPv4 routes are imported from the global BGP non-VPN RIB
 - `ipv6`—Specifies that only IPv6 routes are imported from the global BGP non-VPN RIB
 - `routeMap`—Name of a route map; string of up to 32 alphanumeric characters
 - `maxNumber`—Maximum number of routes that can be imported; integer in the range 1–4294967295

Mode VRF Configuration

graceful-restart

Syntax [no] graceful-restart

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures hitless restart capability for OSPFv2. If high availability is active, the OSPF instance can perform a hitless restart when switching or failing over to the secondary SRP module. The **no** version disables OSPF graceful restart capability on the router.

Mode Router Configuration

graceful-restart helper

Syntax [no] graceful-restart helper

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the router to function as an OSPFv2 or OSPFv3 graceful restart helper router. The **no** version disables OSPF graceful restart helper mode capability on the router.

Mode Router Configuration

graceful-restart helper-abort-topology-change

Syntax graceful-restart helper-abort-topology-change { any | non-externals }
no graceful-restart helper-abort-topology-change

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the OSPFv2 or OSPFv3 helper router to cease help to a restarting router under the specified conditions. However, the router continues to act as helper for subsequent graceful restart requests. The **no** version turns off the graceful restart helper capability.

- Options**
- any—Abandons the helper role when any LSA changes during the restart
 - non-externals—Abandons the helper role only when any nonexternal LSA changes during the restart

Mode Router Configuration

graceful-restart notify-time

Syntax [no] graceful-restart notify-time *notifyTime*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the estimated time for the OSPFv2 router to send purged grace LSAs over all interfaces. The **no** version returns the notify duration timer to its default value, 15 seconds.

Options ■ *notifyTime*—Number of seconds during which the router can send purged grace LSAs over all interfaces; in the range 1–1800

Mode Router Configuration

graceful-restart restart-time

Syntax [no] graceful-restart restart-time *restartTime*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the estimated time for the restarting OSPFv2 router to reacquire OSPF neighbors that were fully functional prior to the restart. When this timer expires, the restarting router exits the restart procedure, originates any LSAs that were suppressed during the restart, removes any self-originated LSAs that it received from helping neighbors, runs SPF, and updates any routes in the routing table. The **no** version returns the restart duration timer to its default value, 180 seconds.

Options ■ *restartTime*—Number of seconds during which the restarting router can reacquire OSPF neighbors that were fully functional prior to the restart; in the range 1–1800

Mode Router Configuration

grace-period

Syntax `grace-period days [hours [minutes [seconds]]]`
 `no grace-period`

Release Information Command introduced in JUNOS Release 8.0.0.

Description Configures the grace period for address leases allocated from the current DHCP local address pool. When the address lease expires, the address enters the grace period, when the address continues to be unavailable to other clients and can only be reassigned to the original client. This command applies only to expired releases—to optionally apply the grace period to addresses that are *explicitly released* by a client, you must enable the **use-release-grace-period** command. The **no** version restores the default, in which no grace period is associated with the local address pool.

- Options**
- *days*—Number of days in the grace period; in the range 0–32767
 - *hours*—Number of hours in the grace period; in the range 0–23
 - *minutes*—Number of minutes in the grace period; in the range 0–59
 - *seconds*—Number of seconds in the grace period; in the range 0–59

Mode DHCP Local Pool Configuration

gre destination profile

Syntax gre destination profile *profileName* { [any-virtual-router] |
[virtual-router *virtualRouterName*] }

no gre destination profile *profileName*

Release Information Command introduced in JUNOS Release 8.2.0.

Description	Configures a destination profile for dynamic GRE tunnels and enters IP Tunnel Destination Profile Configuration mode. The no version deletes the destination profile.
--------------------	--

Options

- *profileName*—Name of the destination profile
- *any-virtual-router*—Specifies a default destination profile for all virtual routers; only one default destination profile can be defined in the system
- *virtualRouterName*—Name of the transport virtual router

Mode Global Configuration

green-mark

Syntax [no] green-mark colorMarkValue

Release Information Command introduced in JUNOS Release 7.2.0.

Description Applies ToS mark value to green packets, which can be from policy actions, earlier policies, or rate-limit hierarchies. The **no** version deletes the ToS mark value.

Options ■ colorMarkValue—Value of the ToS mark to be applied: in the range 0–255

Mode Color Mark Profile Configuration

Related Topics ■ Hierarchical Rate Limits Overview
■ Policy Rule Precedence

gre-tunnel classifier-list

Syntax `gre-tunnel classifier-list classifierName`
 `[traffic-class className] [color { green | yellow | red }]`
 `[user-packet-class userPacketClassValue]`
 `[precedence precNum | dsfield dsfieldNum | tos tosNum]`

 `no gre-tunnel classifier-list classifierName [classifierNumber]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates or modifies a GRE tunnel classifier control list. The **no** version deletes the classifier control list.

- Options**
- *classifierName*—Name of a classifier list entry
 - *className*—Name of a traffic class; the router supports up to eight traffic classes
 - green—Matches packet color to green, indicating a low drop preference
 - yellow—Matches packet color to yellow, indicating a medium drop preference
 - red—Matches packet color to red, indicating a high drop preference
 - *userPacketClassValue*—Value of the user packet class in the range 0–15
 - *precNum*—Upper three bits of the ToS byte; in the range 0–7
 - *dsfieldNum*—Upper six bits of the ToS byte; in the range 0–63
 - *tosNum*—Whole eight bits of the ToS byte; in the range 0–255
 - *classifierNumber*—Index of the classifier control list entry to be deleted; an integer in the range 1–10000

Mode Global Configuration

Related Topics ■ Creating or Modifying Classifier Control Lists for GRE Tunnel Policy Lists

gre-tunnel policy

Syntax gre-tunnel policy { input | output } *policyName*
 [statistics { enabled | disabled | preserve } | merge]
 no gre-tunnel policy { input | output } [*policyName*]

Release Information Command introduced before JUNOS Release 7.1.0.
merge keyword added in JUNOS Release 7.2.0.

Description Assigns a GRE tunnel policy list to an interface. If you enter the **gre-tunnel policy** command and the policy list does not exist, the router creates a policy list with no rules, the default. Attaching this policy list to an interface filters all packets on that interface. You must specify the **input** or **output** keyword to assign the policy list to the ingress or egress of the interface. The **no** version removes the association between a policy list and an interface.

- Options**
- input—Applies policy to data arriving at this interface
 - output—Applies policy to data leaving this interface
 - *policyName*—Name of the policy; a maximum of 40 characters
 - statistics—Enables or disables collection of policy routing statistics
 - enabled—Enables collection of policy routing statistics
 - disabled—Disables collection of policy routing statistics
 - preserve—Preserves existing statistics for any classifier-list that is the same for both the new and old policy attachments when you attach a new policy to an interface
 - merge—Enables merging of multiple policies to form a single policy

Mode Interface Configuration

Related Topics ■ Setting a Statistics Baseline for Policies

gre-tunnel policy-list

Syntax [no] gre-tunnel policy-list *policyName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates the specified policy list and accesses Policy List Configuration mode. If you enter the **gre-tunnel policy-list** command and the policy list does not exist, the router creates a policy list with no rules, the default. Attaching this policy list to an interface filters all packets on that interface. The **no** version deletes the policy list.

Options ■ *policyName*—Name of a policy list; string of up to 40 alphanumeric characters

Mode Global Configuration

Related Topics ■ Creating Policy Lists for GRE Tunnels

group

Syntax To specify a group scheduler node for QoS:

```
[ no ] typeOfInterface group groupName scheduler-profile schedulerProfileName
```

To specify a Diffie-Hellman group:

```
group { 1 | 2 | 5 }
```

```
no group
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description From QoS Profile Configuration mode, specifies that a group scheduler node be configured for each interface of the given interface type. The **no** version removes this rule from the QoS profile.

From IKE Policy Configuration mode, assigns a Diffie-Hellman group to the IKE policy. The **no** version restores the default, 1024-bit Diffie-Hellman group.

- Options**
- *typeOfInterface*—Interface types for group scheduler nodes to be configured: atm, ethernet, serial, server-port
 - *groupName*—Name of the traffic class group
 - *schedulerProfileName*—Name of the scheduler profile
 - 1—Specifies the 768-bit group
 - 2—Specifies the 1024-bit group
 - 5—Specifies the 1536-bit group

Mode IKE Policy Configuration, QoS Profile Configuration

- Related Topics**
- Configuring a QoS Profile
 - Configuring Shadow Nodes
 - Configuring QoS for an L2TP Session
 - Configuring QoS for Tunnel-Server Ports for L2TP LNS Sessions

gsmp-syn-timeout

Syntax [no] gsmp-syn-timeout *timeOutValue*

Release Information Command introduced in JUNOS Release 11.0.0.

Description Defines the ANCP neighbor session connection timeout value (in seconds). The neighbor session connection is established on the TCP session.

The **no** version reverts the session timeout to its default setting (60 seconds).

Options ■ *timeOutValue*— Session timeout in seconds. The timer value cannot be more than the ANCP session timeout value. The default value for the ANCP session timeout is 75 seconds.

Mode L2C Configuration

Chapter 9

H Commands

halt

Syntax The syntax of the command depends on whether you enter it from Boot mode or Privileged Exec mode.

From Boot mode:

halt

From Privileged Exec mode:

halt [force | primary-srp [force] | standby-srp [force]]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Stops operation on both SRP modules or on the specified SRP module. When the high availability state is active or pending, this command ensures that the router configuration, up to when you issued the **halt** command, is mirrored to the standby SRP module. There is no **no** version.



CAUTION: To prevent corruption of NVS, issue this command before you remove or power down an SRP module.

Options

- **force**—Prompts the user to confirm that the router should stop operation if the SRP modules are in certain states, such as writing configuration data to NVS, that could lead to loss of configuration data or corruption of NVS.



CAUTION: When the high availability state is active or pending, issuing the **force** keyword does not guarantee that the configuration has been mirrored; recent configuration changes may be lost if you issue the **force** keyword.

- **primary-srp**—Stops operation on primary SRP module only
- **standby-srp**—Stops operation on standby SRP module only

Mode Boot, Privileged Exec

hash

Syntax hash { sha | md5 }
no hash

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the hash algorithm in an IKE policy. The **no** version restores the default, SHA-1.

- Options**
- sha—Specifies SHA-1 (HMAC variant) as the hash algorithm
 - md5—Specifies MD5 (HMAC variant) as the hash algorithm

Mode IKE Policy Configuration

hdlc dos-protection-group

Syntax hdlc dos-protection-group *groupName*
 no hdlc dos-protection-group

Release Information Command introduced in JUNOS Release 8.1.0.

Description Attaches an HDLC denial of service (DoS) protection group to an interface. The **no** version removes the attachment of the DoS protection group from the interface.

Options ■ *groupName*—Name of the DoS protection group; string of up to 31 alphanumeric characters

Mode Interface Configuration

hdlc down-when-looped

Syntax [no] hdlc down-when-looped

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables loopback detection on a Cisco HDLC interface. Loopback detection is disabled by default. The **no** version disables loopback detection.

Mode Interface Configuration, Subinterface Configuration

hdlc keepalive

Syntax hdlc keepalive [*seconds*]

no hdlc keepalive

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a keepalive value. The keepalive mechanism tracks the health of the connection. The **no** version turns off the keepalive feature.

Options ■ *seconds*—Keepalive timeout period in the range 0–6553 seconds; default value is 10. A value of zero (0) turns off the keepalive feature.

Mode Interface Configuration, Subinterface Configuration

hdlc shutdown

Syntax [no] hdlc shutdown

Release Information Command introduced before JUNOS Release 7.1.0.

Description Stops or restarts a Cisco HDLC session. The **no** version restarts a Cisco HDLC session.

Mode Interface Configuration, Subinterface Configuration

hello hold-time

Syntax hello hold-time *seconds*
 no hello hold-time

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the MPLS hold time, the period that a sending LSR maintains a record of link hello messages from the receiving LSR without receipt of another link hello from that LSR. Each LSR peer sends the hold time in its link hello messages; peers negotiate to use the minimum of the hold times proposed by all LSRs on the same subnet. The hold timer is restarted whenever the LSR receives a link hello from the adjacent peer. The timer expires if no link hello is received from the adjacent peer within the hold time. The LSR deletes the link hello adjacency when the timer expires. If all link hello adjacencies are deleted for an LDP session, then the LSR terminates the LDP session. The **no** version restores the default value, 15 seconds.

Options ■ *seconds*—Number of seconds, in the range 1–65535

Mode LDP Profile Configuration

hello interval

Syntax hello interval *seconds*
 no hello interval

Release Information Command introduced in JUNOS Release 8.1.0.

Description Specifies the interval between link-hello packets sent by LDP. The **no** version restores the default interval, 5 seconds.

Options ■ *seconds*—Number of seconds, in the range 1–65535

Mode LDP Profile Configuration

hello-interval

Syntax hello-interval *helloInterval*
 no hello-interval

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the interval between hello packets that the router sends on the OSPF remote-neighbor interface. The **no** version restores the default value.

Options ■ *helloInterval*—Number in the range 1–65535 seconds; default value is 10 seconds

Mode Remote Neighbor Configuration

help

Syntax help

Release Information Command introduced before JUNOS Release 7.1.0.

Description Displays basic information about the Help system. There is no **no** version.

Mode All modes

hops-of-statistics-kept

Syntax hops-of-statistics-kept [*hopsKeptValue*]
no hops-of-statistics-kept

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the number of hops to keep statistics for an entry. The **no** version restores the default value.

Options ■ *hopsKeptValue*—Number of hops for which statistics are collected for a particular *pathEcho* type; default value is 16 for a *pathEcho* entry and 1 for an *echo* entry; if you omit this option, all hops found are recorded



NOTE: The E Series router supports only the *pathEcho* and *echo* types.

Mode RTR Configuration

host

Syntax `host hostname ipAddress [ftp [[userAlgorithmType] userName [[passwordAlgorithmType] password]]] | [tftp]`

`no host hostname`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Adds or modifies an entry to the host table. The **no** version removes the specified host.

- Options**
- *hostname*—Hostname to add or modify; up to 20 characters
 - *ipAddress*—IPv4 or IPv6 address of the host
 - *ftp*—Specifies that the host is an FTP server; the default protocol if neither *ftp* nor *tftp* is specified
 - *userAlgorithmType*—Type of username
 - 0—Indicates that the *userName* is unencrypted; the default
 - 8—Indicates that the *userName* is an encrypted password
 - *userName*—Username used to access an FTP server (but not an NFS server); defaults to **anonymous**
 - *passwordAlgorithmType*—Type of password
 - 0—Indicates that the *password* is unencrypted; the default
 - 8—Indicates that the *password* is an encrypted password
 - *password*—Password used to access an FTP server (but not an NFS server); defaults to **null**
 - *tftp*—Specifies that the host is a TFTP server

Mode Global Configuration

hostname

Syntax `hostname hostname`
`no hostname`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the name for the router; this hostname subsequently appears in the router CLI prompt. The **no** version removes the hostname from the router.



NOTE: In Domain Map Tunnel Configuration mode, this command has been replaced by the **clear suspicious-control-flow-detection** command and may be removed completely from Domain Map Tunnel Configuration mode in a future release.

Options ■ *hostname*—String of up to 63 characters (no spaces)

Mode Global Configuration

hotfix activate

Syntax hotfix activate *hfixFilename*
no hotfix activate { *hfixFilename* | all }

Release Information Command introduced in JUNOS Release 7.2.0.

Description Activates the specified hotfix present on the local flash card. The **no** version deactivates the specified hotfix or all currently active hotfixes. Deactivating a hotfix restores the router to the state that existed before the hotfix was activated.

- Options**
- *hfixFileName*—Name of a hotfix software file (.hfx) on the local file system
 - all—Specifies that all currently active hotfixes are deactivated

Mode Privileged Exec

Chapter 10

I Commands

id

Syntax [no] id *neighborId*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the ANCP neighbor ID in the L2C Neighbor (config-l2c-neighbor) Configuration mode. The **no** version removes the neighbor ID.

Options ■ *neighborId*—ANCP neighbor ID (MAC address) in the form XXXX.XXXX.XXXX

Mode L2C Neighbor Configuration

identification

Syntax `identification serverId`

`no identification`

Release Information Command introduced before JUNOS Release 7.1.0.

Description From Domain Map Tunnel Configuration or Tunnel Group Tunnel mode, specifies the assignment ID of an L2TP tunnel. The **no** version removes the assignment ID from the tunnel.

Options ■ *serverId*—L2TP tunnel assignment ID up to 32 characters

Mode Domain Map Tunnel Configuration, Tunnel Group Tunnel

idle-character

Syntax idle-character { flags | marks }
 no idle-character

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the HDLC idle character that is transmitted between HDLC packets. The **no** version restores the default value.

- Options**
- flags—Sets the idle character to 0x7E; the default value
 - marks—Sets the idle character to 0xFF

Mode Interface Configuration

igmp disable

Syntax [no] igmp disable

Release Information Command introduced before JUNOS Release 7.1.0.

Description Disables IGMP on a virtual router. The **no** version reenables IGMP on a virtual router.

Mode Router Configuration

igmp promiscuous

Syntax [no] igmp promiscuous

Release Information Command introduced before JUNOS Release 7.1.0.

Description Allows all IGMP interfaces on the router to accept IGMP reports from hosts on any subnet. The **no** version allows IGMP interfaces on the router to accept IGMP reports only from hosts on their associated subnets.

Mode Router Configuration

ignore-lsp-errors

Syntax [no] ignore-lsp-errors

Release Information Command introduced before JUNOS Release 7.1.0.

Description Allows the router to ignore IS-IS link-state packets that are received with internal checksum errors rather than purging the link-state packets. The **no** version disables this function.

Mode Router Configuration

ike crl

Syntax ike crl { ignored | optional | required }
 no ike crl

Release Information Command introduced before JUNOS Release 7.1.0.

Description Controls how the router handles certificate revocation lists (CRLs) during negotiation of IKE phase 1 signature authentication. The **no** version returns the CRL setting to the default, optional.



NOTE: This command has been replaced by the **ipsec crl** command and may be removed completely in a future release.

- Options**
- ignored—Allows negotiations to succeed even if a CRL is invalid or the peer's certificate appears in the CRL; this is the most lenient setting
 - optional—If the router finds a valid CRL, it uses it; this is the default
 - required—Requires a valid CRL; either the certificates belonging to the E Series router or the peer must not appear in the CRL; this is the strictest setting

Mode Global Configuration

ike local-identity

Syntax ike local-identity { ip address *ipAddress* | username *userName* | domain-name *domainName* }

no ike local-identity

Release Information Command introduced in JUNOS Release 7.3.0.

Description Sets the local IKE identity used for IKE security association (SA) negotiations. The **no** version removes the local IKE identity.

- Options**
- *ipAddress*—IP address in 32-bit dotted decimal format (for example, 192.56.32.2)
 - *userName*—Username used as the IKE local identity for IKE SA negotiations
 - *domainName*—Domain name used as the IKE local identity for IKE SA negotiations (string of 1–32 characters)

Mode IPSec Tunnel Profile Configuration

ike peer-identity distinguished-name

Syntax ike peer-identity distinguished-name *dnString*
 no ike peer-identity ip address distinguished-name

Release Information Command introduced in JUNOS Release 7.3.0.

Description Enables this profile to accept logins from users that present an ASN.1-encoded distinguished name as an IKE identity type and the user-provided IKE identity matches each distinguished name field in this profile. The **no** version removes the peer IKE identity.

Options ■ *dnString*—String of 1–32 characters used as the distinguished name

Mode IPSec Tunnel Profile Configuration

ike peer-identity domain-name

Syntax ike peer-identity domain-name *domainName*
 no ike peer-identity ip address domain-name

Release Information Command introduced in JUNOS Release 7.3.0.

Description Enables this profile to accept logins from users that present a userFQDN or FQDN as an IKE identity type and the domain name portion of the IKE identity matches the domain name setting for this profile. The **no** version removes the peer IKE identity.

Options ■ *domainName*—String of 1–32 characters used as the domain name

Mode IPSec Tunnel Profile Configuration

ike peer-identity ip address

Syntax ike peer-identity ip address *ipAddress* [*ipMask*]
 no ike peer-identity ip address ip address

Release Information Command introduced in JUNOS Release 7.3.0.

Description Enables this profile to accept logins from users that present an IP address as an IKE identity type and the IP address resides within the specified network. The **no** version removes the peer IKE identity.

- Options** ■ *ipAddress*—IP address in 32-bit dotted decimal format (for example, 192.56.32.2)
 ■ *ipMask*—Mask for associated IP subnet in dotted decimal or prefix length notation

Mode IPSec Tunnel Profile Configuration

ike peer-identity username

Syntax ike peer-identity username *userName*
 no ike peer-identity ip address username

Release Information Command introduced in JUNOS Release 7.3.0.

Description Enables this profile to accept logins from users that present a userFQDN as an IKE identity type and the username portion of the IKE identity matches the username setting for this profile. The **no** version removes the peer IKE identity.

Options ■ *userName*—String of 1–32 characters used as the user name

Mode IPSec Tunnel Profile Configuration

import map

Syntax `import map [ipv4 | ipv6] routeMap`
`no import map [ipv4 | ipv6]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Associates a route map with a VRF to modify and filter routes imported by the VRF from the global BGP VPN RIB. Both IPv4 and IPv6 routes are imported unless you issue the appropriate keyword to restrict importation. The **no** version enables all routes whose route targets match the import route targets of the VRF to be imported without applying a route map.

- Options**
- `ipv4`—Specifies that only IPv4 routes are imported from the global BGP VPN RIB
 - `ipv6`—Specifies that only IPv6 routes are imported from the global BGP VPN RIB
 - `routeMap`—Name of a route map; string of up to 32 alphanumeric characters

Mode VRF Configuration

inarp

Syntax inarp [*frequency*]
 no inarp

Release Information Command introduced in JUNOS Release 7.1.0.
 ATM VC Class Configuration mode added in JUNOS Release 7.3.0.

Description In ATM VC Configuration mode, enables Inverse ARP (InARP) on an ATM PVC that resides on an ATM 1483 NBMA subinterface. Optionally, you can specify the InARP refresh rate. The **inarp** command is valid only for data PVCs configured with **aal5snap** encapsulation; you cannot use this command for data PVCs with other encapsulation types or for control (ILMI or signaling) PVCs. The **no** version restores the default behavior, which disables InARP.

In ATM VC Class Configuration mode, enables InARP as part of a VC class definition that you assign to an ATM data PVC. The **no** version restores the default behavior, which disables InARP, in the VC class.

Options ■ *frequency*—InARP refresh rate in minutes, in the range 1–60; default value is 15

Mode ATM VC Configuration, ATM VC Class Configuration

include circuit-identifier

Syntax include circuit-identifier *circuitType* [prepend-circuit-type]
 no include circuit-identifier

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that the circuit identifier is included when the router automatically generates a username for an IP service profile. The **no** version disables inclusion of the circuit identifier.

- Options** ■ *circuitType*—Type of circuit; atm or vlan
 ■ prepend-circuit-type—Specifies that the circuit type is included in the username

Mode IP Service Profile Configuration

include dhcp-option 82

Syntax [no] include dhcp-option 82 { agent-circuit-id | agent-remote-id }

Release Information Command introduced in JUNOS Release 7.3.0.

Description Specifies that the agent-circuit-id suboption or the agent-remote-id suboption of the DHCP relay agent information option (option 82) is included when the router automatically generates a username for an IP service profile. The **no** version disables inclusion of the suboption.

Mode IP Service Profile Configuration

include hostname

Syntax [no] include hostname

Release Information Command introduced in JUNOS Release 7.3.0.

Description Specifies that the router's hostname is included when the router automatically generates a username for an IP service profile. The **no** version disables inclusion of the hostname.

Mode IP Service Profile Configuration

include ip-address

Syntax [no] include ip-address

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that the IP address is included when the router automatically generates a username for an IP service profile. The **no** version disables inclusion of the IP address.

Mode IP Service Profile Configuration

include mac-address

Syntax [no] include mac-address

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that the MAC address is included when the router automatically generates a username for an IP service profile. The **no** version disables inclusion of the MAC address.

Mode IP Service Profile Configuration

include virtual-router-name

Syntax [no] include virtual-router-name

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that the virtual router name is included when the router automatically generates a username for an IP service profile. The **no** version disables inclusion of the virtual router name.

Mode IP Service Profile Configuration

index

Syntax `index indexNumber next-address ipAddress [[mask] ipMask] [loose]`
 `no index indexNumber`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a next hop at a particular index in the MPLS explicit path. The **no** version removes the next hop from the index.

- Options**
- *indexNumber*—Number of a node in an ordered set of abstract nodes; in the range 1–255
 - *ipAddress*—Address of the next hop
 - *ipMask*—[not currently used] mask for the next adjacent address
 - *loose*—Node is not necessarily directly connected (adjacent) to the previous node in the path. If *loose* is not configured, the configuration defaults to *strict*. *Strict* indicates that the node is directly connected to the previous node.

Mode Explicit Path Configuration

instance-interface-type

Syntax	<pre>instance-interface-type { <i>instanceInterfaceType</i> set superset }</pre> <pre>no instance-interface-type { <i>instanceInterfaceType</i> all }</pre>
Release Information	<p>Command introduced in JUNOS Release 7.1.0.</p> <p>lag keyword added in JUNOS Release 8.1.0.</p> <p>set and superset keywords added in JUNOS Release 9.2.0.</p>
Description	<p>Assigns an instance-interface type to a QoS parameter definition. Instance-interface types indicate the interfaces for which QoS clients can assign QoS parameter instances. You can specify up to eight instance-interface types for each parameter definition. The no version removes the specified instance-interface type from the parameter definition.</p>
Options	<ul style="list-style-type: none"> ■ <i>instanceInterfaceType</i>—One of the following instance-interface types: atm, atm-vc, atm-vp, bridge, ethernet, fr-vc, ip, ip-tunnel, ipv6, lag, l2tp-session, l2tp-tunnel, lsp, pppoe, serial, server-port, svlan, vlan ■ set—Specifies an interface set as an instance-interface type ■ superset—Specifies an interface superset as an instance-interface type ■ all—Removes all instance-interface types
Mode	QoS Parameter Definition
Related Topics	<ul style="list-style-type: none"> ■ Configuring a Basic Parameter Definition for QoS Administrators ■ Creating a QoS Parameter on an Interface Superset or Interface Set

interface

Syntax [no] interface *interfaceType* *interfaceSpecifier* [*extension*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures an interface. The **no** version removes the subinterface or the logical interface.



NOTE: See the individual **interface** command entries for the syntax for each type of interface.

- Options**
- *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *extension*—Option that depends on the type of interface

Mode Global Configuration

interface atm

Syntax [no] interface atm *interfaceSpecifier* [multipoint | point-to-point]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures an ATM interface or subinterface type. The **no** version removes the interface or subinterface.



NOTE: On the OC3-2 GE APS I/O module, you can configure only OC3/STM1 ATM interfaces in ports 0 and 1. Port 2 is reserved for a Gigabit Ethernet interface.

- Options**
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - multipoint—Specifies an NBMA subinterface
 - point-to-point—Specifies an ATM interface or subinterface; default

Mode Global Configuration, Interface Configuration

Related Topics

- *Configuring an MPLS Pseudowire with VCC Cell Relay Encapsulation, Configuring Local ATM Cross-Connects with AAL5 Encapsulation, and Configuring MPLS LSPs for L2VPNs* in the *JUNOS BGP and MPLS Configuration Guide*

interface-event-disable

Syntax [no] interface-event-disable

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that RIP does not purge the routing table on a RIP interface that has been brought down. The **no** version restores the default condition, wherein RIP does purge the routing table on an interface after a down event.

Mode Address Family Configuration, Router Configuration

interface fastEthernet

Syntax [no] interface fastEthernet *interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a Fast Ethernet interface or subinterface or creates a subinterface over a Fast Ethernet interface. The **no** version removes the interface or subinterface.

Options ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Global Configuration

Related Topics ■ *Configuring Customer-Facing Interfaces in the L2VPN Instance, Configuring Ethernet/VLAN Layer 2 Services, Configuring Local Cross-Connects Between Ethernet/VLAN Interfaces, and Configuring S-VLAN Tunnels for Layer 2 Services in the JUNOS BGP and MPLS Configuration Guide*

interface gigabitEthernet

Syntax [no] interface gigabitEthernet *interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies or creates a Gigabit Ethernet interface or a subinterface over a Gigabit Ethernet interface. The **no** version removes the interface or subinterface.



NOTE: On the GE I/O module, you can configure only the primary port, 0. The router automatically uses the redundant port, 0R, if the primary port fails.

On the GE-2 APS I/O module, you can configure only the primary ports, 0 and 1. The router automatically uses the corresponding redundant port, 0R or 1R, if the primary port fails.

On the OC3-2 GE APS I/O module, you can configure only a Gigabit Ethernet interface in port 2. Ports 0 and 1 are reserved for OC3/STM1 ATM interfaces.

On the ES-2 GE-4 IOA, you can configure all four ports.

Options ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Global Configuration

Related Topics ■ Configuring the QoS Shaping Mode for Ethernet Interfaces
 ■ Creating a QoS Interface Hierarchy for Bulk-Configured VLAN Subinterfaces with RADIUS
 ■ Configuring a Parameter Definition to Shape Ethernet Traffic Using Cell Mode

interface ip

Syntax [no] interface ip *interfaceName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a shared IP interface. The **no** version removes the IP interface.

Options ■ *interfaceName*—String of up to 15 characters

Mode Global Configuration

interface ipv6

Syntax [no] interface ipv6 *interfaceName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a shared IPv6 interface. The **no** version removes the IPv6 interface.

Options ■ *interfaceName*—String of up to 15 characters

Mode Global Configuration

interface lag

Syntax [no] interface lag *interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates an IEEE 802.3ad link aggregation group (LAG) interface, also known as a LAG bundle, or a subinterface in a LAG bundle. Link aggregation enables you to group multiple Ethernet physical interfaces configured on the same module and with the same characteristics into a single logical interface. The individual Ethernet interfaces are referred to as member links of the LAG bundle. The **no** version removes the LAG bundle or subinterface.

Options ■ *interfaceSpecifier*—LAG interface specifier; see Interface Types and Specifiers on page 5

Mode Global Configuration

Related Topics ■ Configuring the Scheduler Hierarchy for Hashed Load Balancing in 802.3ad Link Aggregation Groups

■ Configuring the Scheduler Hierarchy for Subscriber Load Balancing in 802.3ad Link Aggregation Groups

■ Configuring Load Rebalancing for 802.3ad Link Aggregation Groups

interface loopback

Syntax [no] interface loopback *interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a loopback interface, which provides a stable address for protocols (for example, BGP, Telnet, or LDP) to use so that they can avoid any impact if a physical interface goes down. The loopback interface sends packets back to the router or access server for local processing. Any packets routed from the loopback interface, but not destined to the loopback interface, are dropped. The **no** version deletes the loopback interface.



NOTE: Do not confuse loopback with the null 0 interface. Traffic routed to null 0 is discarded on the line module.

You cannot shut down a loopback interface.



BEST PRACTICE: We recommend that you configure a 32-bit subnet mask for the loopback interface. For example, if you configure a loopback interface with the IP address and mask as 1.1.1.1/16, the 1.1.0.0/16 route entry is entered on the line module and if no specific or longer route entry is found, all traffic destined to the 1.1.0.0/16 subnet is forwarded to the SRP module by the line module. Although the SRP module responds only to traffic destined to the 1.1.1.1 subnet and discards traffic to all other host IP addresses within that subnet (1.1.1.1/16), if the SRP module receives too much traffic from subnets other than 1.1.1.1, the CPU utilization on the SRP module reaches the saturation level.

Options ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Global Configuration

Related Topics ■ *Configuring an MPLS Pseudowire with VCC Cell Relay Encapsulation, Configuring Local ATM Cross-Connects with AAL5 Encapsulation, Configuring Local Cross-Connects Between Ethernet/VLAN Interfaces, Configuring the Loopback Interface and Router ID for BGP for L2VPNs, and Configuring the Loopback Interface and Router ID for VPLS in the JUNOS BGP and MPLS Configuration Guide*

interface mlframe-relay

Syntax [no] interface mlframe-relay *interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines an MLFR bundle or a subinterface in a bundle. The **no** version removes the bundle or subinterface.

Options ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Global Configuration

interface mlppp

Syntax [no] interface mlppp *interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates an MLPPP network interface, also known as the MLPPP bundle. The **no** version deletes the MLPPP bundle.

Options ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Interface Configuration, Subinterface Configuration

interface null

Syntax interface null 0

Release Information Command introduced before JUNOS Release 7.1.0.

Description Selects the null interface, which does not forward traffic. The null interface acts as a data sink. Though you can access the null interface, you cannot configure any values for it or delete it. There is no **no** version.

Mode Global Configuration

interface pos

Syntax [no] interface pos *interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures a Packet over SONET interface. The **no** version removes the interface.

Options ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Global Configuration

Related Topics ■ *Configuring HDLC Layer 2 Services in the JUNOS BGP and MPLS Configuration Guide*

interface serial

Syntax [no] interface serial *interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the location of the serial interface on CT3 and COCX-F3 modules. The **no** version disables the interface.

Options ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Global Configuration

Related Topics ■ *Configuring Frame Relay Layer 2 Services* and *Configuring HDLC Layer 2 Services* in the *JUNOS BGP and MPLS Configuration Guide*

interface tenGigabitEthernet

Syntax [no] interface tenGigabitEthernet *interfaceSpecifier*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Specifies or creates a 10-Gigabit Ethernet interface or a subinterface over a 10-Gigabit Ethernet interface. The **no** version removes the interface or subinterface.

Options ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Global Configuration

interface tunnel

Syntax [no] interface tunnel *interfaceSpecifier* [transport-virtual-router *vrName*]
[ipsec-transport]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates a tunnel interface for use by DVMRP, GRE, IPSec, or MPLS. You can specify that the tunnel be established in the routing space of a virtual router other than the current VR. If you specify another VR, all tunnel commands apply to the tunnel in that VR. If you do not specify another VR, tunnel commands apply to the current VR. For DVMRP and GRE tunnels, you can specify that the tunnel be protected with IPSec in transport mode. The **no** version removes the tunnel interface.

- Options**
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *vrName*—Name of virtual router (other than the current VR) in which the tunnel will be established
 - ipsec-transport—Indicates that the tunnel is protected with IPSec in transport mode; used for GRE or DVMRP tunnels only

Mode Global Configuration

invert data

Syntax [no] invert data

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables data stream inversion. Data stream inversion must be turned on by network personnel at the other end of the line. The **no** version disables data stream inversion.

Mode Interface Configuration

ip

Syntax ip { permit | deny }
no ip

Release Information Command introduced before JUNOS Release 7.1.0.

Description Modifies the subscriber policy for IP to define whether the subscriber (client) interfaces that belong to a bridge group or to a VPLS instance forward (permit) or filter (deny) IP packets. The **no** version restores the default value, permit IP packets.

You cannot change the default subscriber policy values for trunk (server) interfaces that belong to a bridge group or to a VPLS instance. You also cannot change the default subscriber policy values for a VPLS virtual core interface, which acts as a trunk interface. The VPLS virtual core interface represents all of the MPLS tunnels from the router to the remote VPLS edge (VE) devices.

- Options**
- permit—Specifies that the subscriber interface associated with the bridge group or VPLS instance forwards IP packets
 - deny—Specifies that the subscriber interface associated with the bridge group or VPLS instance filters IP packets

Mode Subscriber Policy Configuration

ip access-routes

Syntax [no] ip access-routes

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the ability to create host access routes on a PPP interface, which is useful for the B-RAS application. It also enables an access route in a profile. The **no** version disables the feature.

Mode Interface Configuration, Profile Configuration, Subinterface Configuration

ip access-route table-map

Syntax [no] ip access-route table-map *mapName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Filters access routes before an access list adds them to the routing table. The **no** version deletes the table map.

Options ■ *mapName*—Name of the table map that you want the router to use

Mode Global Configuration

ip address

Syntax `ip address ipAddress ipMask [secondary]`
 `no ip address [ipAddress ipMask [secondary]]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a primary or secondary IP address for an interface or subinterface. The **no** version removes an IP address or disables IP processing. You must specify the layer 2 encapsulation before you can set the IP address.

- Options**
- *ipAddress*—IP address in 32-bit dotted decimal format (for example, 192.56.32.2)
 - *ipMask*—mask for associated IP subnet in dotted decimal or prefix length notation
 - *secondary*—Specifies that the configured address is a secondary IP address; if omitted, the configured address is the primary IP address

Mode Interface Configuration, Profile Configuration, Subinterface Configuration

- Related Topics**
- *Configuring Local ATM Cross-Connects with AAL5 Encapsulation, Configuring Local Cross-Connects Between Ethernet/VLAN Interfaces, Configuring the Loopback Interface and Router ID for BGP for L2VPNs, Configuring the Loopback Interface and Router ID for VPLS, and Configuring MPLS LSPs for L2VPNs in the JUNOS BGP and MPLS Configuration Guide*

ip-address

Syntax `ip-address ipAddress`
 `[no] ip-address`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the IP address parameter for a user entry in the local user database. The **no** version deletes the IP address parameter from the user entry.

Options ■ *ipAddress*—IP address in 32-bit dotted decimal format (for example, 192.56.32.2)

Mode Local User Configuration

ip address-pool

Syntax ip address-pool { dhcp | local | none }
no ip address-pool

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies to the router where to get an IP address for the remote user. The **no** version uses the default value, **local**.

- Options**
- dhcp—Enables the use of a DHCP server for address allocations
 - local—Enables the use of local address pool for address allocations
 - none—Does not enable an IP address pool

Mode Global Configuration

ip-address-pool

Syntax `ip-address-pool poolName`
 `no ip-address-pool`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the IP address pool parameter for a user entry in the local user database. The address pool is used to assign an IP address to the subscriber. The **no** version deletes the IP address pool parameter from the user entry in the local user database.

Options ■ *poolName*—Name of IP address pool

Mode Local User Configuration

ip address virtual-router

Syntax [no] ip address *ipAddress* virtual-router *vrName*
no ip address

Release Information Command introduced in JUNOS Release 7.3.0.

Description Limits the scope of the IKE policy rule to the specified local IP address on the specified virtual router. This limitation ensures that this policy rule is evaluated for IKE source address evaluations for only the specified IP address and virtual router. The **no** version removes IP address and virtual router limitation.

- Options**
- *ipAddress*—IP address in 32-bit dotted decimal format (for example, 192.56.32.2) to which you want to limit this policy rule
 - *vrName*—Name of virtual router to which you want to limit this policy rule

Mode IKE Policy Configuration

ip alwaysup

Syntax [no] ip alwaysup

Release Information Command introduced before JUNOS Release 7.1.0.

Description Forces the interface to appear as if it is up, regardless of the state of the lower layers. Use this command to reduce routing protocol topology changes on the router when the network attached to this link is single-homed. This command may be useful when the router is running routing protocols with very large routing tables that may take a long time to converge. The **no** version makes the interface appear in its current state.

Mode Interface Configuration, Subinterface Configuration

ip analyzer

Syntax ip analyzer [default]
no ip analyzer

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures an interface as an analyzer interface, for use in an interface mirroring configuration. The **no** version removes the analyzer interface configuration from the interface.

Options ■ default—Specifies that this interface is the default analyzer interface for the virtual router

Mode Interface Configuration

Related Topics ■ Configuring CLI-Based Mirroring
■ Configuring RADIUS-Based Mirroring

ip as-path access-list

Syntax ip as-path access-list *accessListName* { permit | deny } *pathExpression*
 no ip as-path access-list *accessListName* [{ permit | deny } *pathExpression*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a BGP-related access list. You can specify an access list filter on both inbound and outbound BGP routes. Each filter is an access list based on regular expressions. If the regular expression matches the representation of the AS path of the route as an ASCII string, then the permit or deny condition applies. The AS path does not contain the local AS number. The **no** version removes a single access list entry if **permit** or **deny** and a *pathExpression* are specified. Otherwise, the entire access list is removed.

Options ■ *accessListName*—Name of the access list; a string of up to 32 characters
 ■ permit—Permits access for matching conditions
 ■ deny—Denies access to matching conditions
 ■ *pathExpression*—Regular expression describing the AS paths to be matched
 Use a sequence of one or more elements, each of which is either an AS number or one of the following punctuation characters:

 ^ start of the path

 \$ end of the path

 { start of an AS_SET

 } end of an AS_SET

 (start of an AS_CONFED_SET or AS_CONFED_SEQ

) end of an AS_CONFED_SET or AS_CONFED_SEQ

Use the following regular expression metacharacters to match individual elements:

 . matches any single element

 * matches zero or more occurrences of any element

 + matches one or more occurrences of any element

 [] matches any elements enclosed between brackets ([])

 - hyphen; used within brackets to specify a range of AS numbers

^ matches any AS number except the ones specified when used as a first item within brackets

_ underscore; used in implementations on routers from other vendors on either side of a path to specify a literal and disallow substring matching. Allowed but not required in our CLI.

Mode Global Configuration

ip atm-vc

Syntax `ip ipAddress atm-vc vcd broadcast`
 `no ip ipAddress atm-vc vcd`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Associates a protocol and address to a specific virtual circuit. The **no** version removes the association.

- Options**
- *ipAddress*—IP address to be associated with the virtual circuit
 - *vcd*—Number in the range 1–2147483647; virtual circuit descriptor; an identifier for the VC in other commands
 - **broadcast**—Specifies that the circuit should participate in broadcast operations

Mode Map List Configuration

ip auto-configure ip-subscriber

Syntax [no] ip auto-configure ip-subscriber [include-primary | exclude-primary]

Release Information Command introduced before JUNOS Release 7.1.0.
include-primary and **exclude-primary** keywords added in JUNOS Release 7.1.0.

Description Configures a primary IP interface to support creation of dynamic subscriber interfaces. The **include-primary** and **exclude-primary** keywords specify whether the primary interface can be assigned to a subscriber. The **no** version disables creation of dynamic subscriber interfaces on this primary IP interface.

- Options**
- include-primary—Specifies that the primary interface can be assigned to a subscriber; the **no** version disables the assignment of the primary interface
 - exclude-primary—Specifies that the primary interface cannot be assigned to a subscriber; the **no** version enables the assignment of the primary interface

Mode Interface Configuration, Profile Configuration, Subinterface Configuration

ip auto-detect ip-subscriber

Syntax [no] ip auto-detect ip-subscriber

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the router's packet detect feature, specifying that IP automatically detect packets that do not match any entries in the demultiplexer table. When an unmatched packet is detected, an event is generated that determines whether to create a dynamic subscriber interface or to configure an existing interface. The **no** version disables autodetection.

Mode Interface Configuration, Profile Configuration

ip bgp-community new-format

Syntax [no] ip bgp-community new-format

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that communities must be displayed in *AA:NN* format, where *AA* is a number that identifies the autonomous system and *NN* is a number that identifies the community within the autonomous system. The **no** version restores the default display.

Mode Global Configuration

ip bgp-confed-as-set new-format

Syntax [no] ip bgp-confed-as-set new-format

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that AS-confed-sets must be displayed within square brackets, [], with the ASs delimited by commas. The **no** version restores the default, displaying AS-confed-sets within parentheses, (), with the ASs delimited by spaces.

Mode Global Configuration

ip block-multicast-sources

Syntax [no] ip block-multicast-sources

Release Information Command introduced before JUNOS Release 7.1.0.
Profile Configuration mode added in JUNOS Release 8.1.0.

Description Prevents mroute creation by blocking multicast traffic that has a scope larger than link-local (for example, global). In Profile Configuration mode, blocks multicast sources per user on dynamic IP interfaces. The **no** version restores the default behavior of creating mroutes upon receiving multicast packets.

Mode Interface Configuration, Profile Configuration

ip broadcast-address

Syntax [no] ip broadcast-address [*ipAddress*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a broadcast address for an interface. The **no** version restores the default IP broadcast address.

Options ■ *ipAddress*—Broadcast IP address

Mode Interface Configuration, Subinterface Configuration

ip classifier-list

Syntax `ip classifier-list classifierName [traffic-class trafficClassName]`
`[color { green | yellow | red }] [user-packet-class userPacketClassValue]`
`[source-route-class routeClassValue] [destination-route-class routeClassValue]`
`[local { true | false }] [not] { protocol }`
`[not] { sourceAddress sourceMask | host sourceHostAddress | any }`
`[sourceQualifier]`
`[not] { destinationAddress destinationMask | host destinationHostAddress | any }`
`[destinationQualifier] [tcpQualifier] [ip-flags ipFlags]`
`[ip-frag-offset { eq 0 | eq 1 | gt 1 }]`
`[precedence precNum | dsField dsFieldNum | tos tosNum]`

`no ip classifier-list classifierName [classifierNumber]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates or modifies a classifier control list. Use the **not** keyword to deny traffic for a specific protocol, source address, or destination address. Use the **any** keyword to allow traffic to any source or destination address. The **no** version removes the classifier control list.

- Options**
- *classifierName*—Name of the classifier control list entry
 - *trafficClassName*—Name of the traffic class to match
 - *green*—Matches packet color to green, indicating a low drop preference
 - *yellow*—Matches packet color to yellow, indicating a medium drop preference
 - *red*—Matches packet color to red, indicating a high drop preference
 - *userPacketClassValue*—User packet value to match; in the range 0–15
 - *routeClassValue*—Value of the route-class; in the range 0–255
 - *local*—Specifies traffic destined for this interface
 - *true*—Matches packets that are locally destined
 - *false*—Matches packets that are not locally destined
 - *not*—Matches any except the immediately following protocol or address
 - *protocol*—Protocol name (IGMP, IP, TCP, or UDP) or number (in the range 0–255) to match
 - *sourceAddress*—Source address to match
 - *sourceMask*—Wild-card mask to apply to the source address
 - *host*—Matches source or destination address as a host
 - *sourceHostAddress*—Source host address to match
 - *any*—Matches any source or destination address

- *sourceQualifier*—For UDP or TCP protocols, one of the following protocol-specific classifier parameters. See Creating or Modifying Classifier Control Lists for IP Policy Lists for details.
 - *portOperator*—One of the following Boolean operator keywords: **lt** (less than), **gt** (greater than), **eq** (equal to), **ne** (not equal), or **range** (range of port numbers)
 - *range*—Single port number or a range of port numbers
- *destinationAddress*—Destination address to match
- *destinationMask*—Wild-card mask to apply to the destination address
- *destinationHostAddress*—Destination host address to match
- *destinationQualifier*—One of the following protocol-specific classifier parameters for destination TCP or UDP ports, ICMP code and type, or IGMP type. The *portOperator* and port range are used with TCP and UDP. The *icmpType*, *icmpCode*, and *igmpType* parameters are used with ICMP and IGMP.
 - *portOperator*—one of the following Boolean operator keywords: **lt** (less than), **gt** (greater than), **eq** (equal to), or **ne** (not equal), or **range** (range of port numbers) (TCP and UDP only)
 - *range*—Single port number or a range of port numbers
 - *icmpType*—ICMP message type (ICMP only)
 - *icmpCode*—ICMP message code (ICMP only)
 - *igmpType*—IGMP message type (IGMP only)
- *tcpQualifier*—TCP flags classification parameters
- *tcpFlag*—For TCP only; a logic equation that specifies flag bit values; ! means logical NOT and & means logical AND; use any of the following flag names:
 - *ack*—0x10
 - *fin*—0x01
 - *push*—0x08
 - *rst*—0x04
 - *syn*—0x02
 - *urgent*—0x20
- *ipFlags*—Logic equation that specifies flag bit values; ! means logical NOT and & means logical AND; use any of the following flag names:
 - *dont-fragment*—0x02
 - *more-fragments*—0x01
 - *reserved*—0x04
- *ip-frag-offset*—Matches the specified IP fragmentation offset; use any of the following:

- eq 0—Equals 0
- eq 1—Equals 1
- gt 1—Greater than 1
- *precNum*—Upper three bits of the ToS byte; in the range 0–7
- *dsFieldNum*—Upper six bits of the ToS byte; in the range 0–63
- *tosNum*—Whole eight bits of the ToS byte; in the range 0–255
- *classifierNumber*—Index of the classifier control list entry to be deleted

Mode Global Configuration

Related Topics ■ Creating or Modifying Classifier Control Lists for IP Policy Lists

ip community-list

Syntax Using a regular expression to specify the community:

```
[ no ] ip community-list communityLisName { permit | deny } communityExpression
```

Using some other method to specify the community:

```
ip community-list communityLisName { permit | deny }
{ communityNumber | asCommunityNumber | no-export | no-advertise | local-as |
internet } [ communityNumber | asCommunityNumber | no-export | no-advertise |
local-as | internet ]*
```

```
no ip community-list communityLisName [ { permit | deny }
[ { communityNumber | asCommunityNumber | no-export | no-advertise | local-as |
internet } ] [ communityNumber | asCommunityNumber | no-export | no-advertise |
local-as | internet ]* ]
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates a community list for BGP and controls access to it. The **no** version removes the community list, including all list entries.

- Options**
- *communityLisName*—Name of a community list; a string of up to 32 characters; identifies one or more permit or deny groups of communities; used for standard community lists
 - permit—Permits access for a matching condition
 - deny—Denies access for a matching condition
 - *communityExpression*—Regular expression that matches the community
 - *communityNumber*—Community number in the range 1–4294967295
 - *asCommunityNumber*—Community number in the format *AA:NN*, where *AA* is a number that identifies the autonomous system and *NN* is a number that identifies the community within the autonomous system.
 - no-export—Specifies that BGP does not advertise this route outside a BGP confederation boundary
 - no-advertise—Specifies that BGP does not advertise this route to any peer (internal or external)
 - local-as—Specifies that BGP does not advertise this route to external peers; sometimes known as the no-export-subconfed community
 - internet—Specifies the Internet community
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

ip debounce-time

Syntax ip debounce-time [vrf *vrfName*] *period*
 no ip debounce-time [vrf *vrfName*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines the minimum time an IP interface must be in a given state—for example, up or down—before being reported. The **no** version removes the debounce time.

- Options** ■ *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
 ■ *period*—Interval in the range 0–60000 milliseconds

Mode Global Configuration, Interface Configuration

ip demux-type da-prefix

Syntax [no] ip demux-type da-prefix

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that a subscriber interface will demultiplex traffic using destination addresses. The **no** version restores the default situation, in which the subscriber interface demultiplexes traffic using source addresses.

Mode Interface Configuration

ip description

Syntax ip description *name*
 no ip description

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns a text description or an alias to a static IP interface or subinterface. If no IP interface currently exists, then a static IP interface is automatically created on the current layer 2 interface and the description is applied to that static IP interface. You cannot assign a profile to a layer 2 interface that has a static interface configured above it. Use the show ip interface command to display the text description. The **no** version removes the description or alias.



NOTE: This command is replacing the **description** command to assign a description to a static IP interface. The **description** command may be removed completely from Interface Configuration mode in a future release.

Options ■ *name*—Name for the static IP interface; string of up to 256 characters

Mode Interface Configuration, Subinterface Configuration

ip destination-prefix

Syntax [no] ip destination-prefix *ipAddress* *ipAddressMask* deny

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures a subscriber interface or a primary IP interface that is enabled for dynamic creation of subscriber interfaces to demultiplex traffic with the specified destination address. The **no** version removes the association between the interface and the specified destination address.

- Options**
- *ipAddress*—Destination IP address that the router uses to identify packets for this interface
 - *ipAddressMask*—Network mask for associated IP subnet
 - deny—Filters packets matching this command

Mode Interface Configuration, Subinterface Configuration

ip dhcp-capture

Syntax ip dhcp-capture { all | receive | transmit } [priority { low | high }]
no ip dhcp-capture { all | receive | transmit }

Release Information Command introduced in JUNOS Release 7.3.0.

Description Configures the E Series router to capture and log DHCP packet information for an interface. By default, DHCP packet information is not captured. The **no** version restores the default behavior.

- Options**
- all—Captures received and transmitted packets
 - receive—Captures received packets
 - transmit—Captures transmitted packets
 - low—Captured packets arrive with low priority; the default priority
 - high—Captured packets arrive with high priority

Mode Interface Configuration

ip dhcp-external auto-configure

Syntax [no] ip dhcp-external auto-configure [agent-circuit-identifier]

Release Information Command introduced before JUNOS Release 7.1.0.
agent-circuit-identifier keyword added in JUNOS Release 7.3.0.

Description Configures the E Series router to automatically create the user's DSI. This command is specific to a virtual router. The **no** version disables the autoconfigure feature.

Options ■ agent-circuit-identifier—Creates dynamic subscriber interfaces built over dynamic VLANs that are based on the agent-circuit-id option (suboption 1) of the option 82 field in DHCP messages.

Mode Global Configuration

ip dhcp-external disregard-giaddr-next-hop

Syntax [no] ip dhcp-external disregard-giaddr-next-hop

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the DHCP external application to disregard the giaddr in packets destined for the DHCP server when the next hop for a subscriber's access route is determined. The **no** version returns to the default, in which DHCP external uses the giaddr to determine the next hop.

Mode Global Configuration

ip dhcp-external recreate-subscriber-interface

Syntax [no] ip dhcp-external recreate-subscriber-interface

Release Information Command introduced in JUNOS Release 9.2.0.

Description Configures the DHCP external server application to delete and re-create the existing dynamic subscriber interface after a bound DHCP client extends its IP address lease by restarting the DHCP discovery process on its primary IP interface instead of by initiating the DHCP renewal process on its dynamic subscriber interface. This command is specific to a virtual router. The **no** version restores the default behavior, which preserves the dynamic subscriber interface after a bound client restarts the discovery process on its primary IP interface.

Mode Global Configuration

- Related Topics**
- Preservation of Dynamic Subscriber Interfaces with DHCP External Server Overview
 - Configuring DHCP External Server to Control Preservation of Dynamic Subscriber Interfaces

ip dhcp-external server-address

Syntax [no] ip dhcp-external server-address *ipAddress*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures a DHCP server that is used to determine which DHCP packets are monitored. The **no** version removes the DHCP server.

Options ■ *ipAddress*—IP address of the external DHCP server; you can specify a maximum of four servers

Mode Global Configuration

ip dhcp-external server-sync

Syntax [no] ip dhcp-external server-sync

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates subscriber state information based on lease renewals when the external DHCP server is unsynchronized with the E Series router. The **no** version disables this feature.

Mode Global Configuration

ip dhcp-local auth domain

Syntax [no] ip dhcp-local auth domain *domainName*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Specifies a domain name for a username that is locally configured for a DHCP standalone mode client. In standalone mode, the locally configured username is presented to AAA in an authentication request. The **no** version removes the domain name.

Options ■ *domainName*—String of 1–32 characters used as the domain name

Mode Global Configuration

ip dhcp-local auth include

Syntax [no] ip dhcp-local auth include { circuit-identifier | circuit-type | mac-address | option82 | virtual-router-name }

Release Information Command introduced in JUNOS Release 7.1.0.

Description Includes optional information as part of the locally configured username for a DHCP standalone mode client. In standalone mode, the username is presented to AAA in an authentication request. The **no** version removes the specified optional information.

- Options**
- circuit-identifier—Specifies the circuit identifier of the interface on which the DHCP client's request was received
 - circuit-type—Specifies the circuit type of the interface on which the DHCP client's request was received
 - mac-address—Specifies the DHCP client's MAC address
 - option82—Specifies the DHCP client's Option 82 value
 - virtual-router-name—Specifies the DHCP local server's virtual router name

Mode Global Configuration

ip dhcp-local auth password

Syntax [no] ip dhcp-local auth password *password*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Assigns a password used to authenticate a locally configured DHCP standalone mode client. In DHCP standalone mode, the password is presented to AAA in an authentication request. The **no** version removes the password.

Options ■ *password*—String of 1–32 characters used as the password

Mode Global Configuration

ip dhcp-local auth user-prefix

Syntax [no] ip dhcp-local auth user-prefix *userNamePrefix*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Specifies a user prefix for a username that is locally configured for a DHCP standalone mode client. In DHCP standalone mode, the username is presented to AAA in an authentication request. The **no** version removes the user prefix.

Options ■ *userNamePrefix*—String of 1–32 characters used as the prefix for a locally configured username

Mode Global Configuration

ip dhcp-local auto-configure agent-circuit-identifier

Syntax [no] ip dhcp-local auto-configure agent-circuit-identifier

Release Information Command introduced in JUNOS Release 7.3.0.

Description Configures the DHCP local server to support the creation of dynamic subscriber interfaces built over dynamic VLANs that are based on the agent-circuit-id option (suboption 1) of the option 82 field in DHCP messages. This command is specific to a virtual router. The **no** version disables the autoconfigure feature.

Mode Global Configuration

ip dhcp-local cable-modem

Syntax [no] ip dhcp-local cable-modem dhcp-server *ipAddress*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the IP address of the external DHCP server to which the DHCP local server will relay DHCP messages from cable modems. The **no** version removes the cable modem configuration.



NOTE: This command is deprecated and might be removed completely in a future release. Use the **set dhcp vendor-option** command to configure the vendor class identifier option to match the string used by cable modems to replace the function of this command.

Options ■ *ipAddress*—IP address of the cable modem DHCP server

Mode Global Configuration

ip dhcp-local excluded-address

Syntax [no] ip dhcp-local excluded-address *ipAddressStart* *ipAddressStop*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies IP addresses that the DHCP local server should not supply from the default address pool because those addresses are already used by devices on the subnet. The **no** version allows the DHCP local server to supply the specified IP address.

- Options**
- *ipAddressStart*—Single IP address or start of the range of IP addresses that the DHCP local server should not supply
 - *ipAddressStop*—End of the range of IP addresses that the DHCP local server should not supply

Mode Global Configuration

ip dhcp-local limit

Syntax ip dhcp-local limit
 { atm | ethernet | pos | vlan | interface *InterfaceType InterfaceSpecifier* } *value*
 no ip dhcp-local limit [atm | ethernet | pos | vlan
 | interface *InterfaceType InterfaceSpecifier*]

Release Information Command introduced before JUNOS Release 7.1.0.
interface keyword and *interfaceType* and *interfaceSpecifier* variables added in JUNOS Release 7.1.0.
pos keyword added in JUNOS Release 10.0.0.

Description Specifies the maximum number of IP addresses that the DHCP local server can supply to each VPI/VCI, VLAN, Ethernet subnetwork, or POS access interface, or to a particular interface or subinterface. The **no** version restores the default address limit value, 48000.

- Options**
- atm—Specifies the limit for VPIs and VCIs
 - ethernet—Specifies the limit for Ethernet subnets
 - pos—Specifies the limit for POS access interfaces
 - vlan—Specifies the limit for VLANs
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *value*—Maximum number of leases, in the range 0–96000; default is 48000

Mode Global Configuration

ip dhcp-local pool

Syntax [no] ip dhcp-local pool { *poolName* | default }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Accesses DHCP Local Pool Configuration mode. The **no** version prevents the DHCP local server from supplying IP addresses from the specified pool.

- Options**
- *poolName*—Name of the address pool
 - default—Specifies the default address pool

Mode Global Configuration

ip dhcp-local snmpTraps

Syntax [no] ip dhcp-local snmpTraps

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables DHCP local server SNMP traps. The **no** version disables DHCP local server SNMP traps.

Mode Global Configuration

ip dhcp-local unique-client-ids

Syntax [no] ip dhcp-local unique-client-ids

Release Information Command introduced in JUNOS Release 8.0.0.

Description Configures the method that DHCP local server uses when it receives a DHCP DISCOVER or REQUEST packet from a client ID or hardware address that matches the client ID or hardware address of a currently bound client on another subnet or subinterface.

Use this command to specify that DHCP local server uses a method that considers a request from a client with a duplicate client ID or hardware address to be from a roaming client—the server then terminates the currently bound client's existing lease and assigns a new address to the requesting client.

The **no** version restores the default behavior, in which DHCP local server uses the DHCP client's subnet or subinterface to differentiate between two clients that use the same client ID or hardware address—the DHCP server processes requests in the normal manner.



NOTE: This command replaces the **ip dhcp-local inhibit-roaming** command, which has been removed from the CLI.

Mode Global Configuration

ip dhcp-server

Syntax `ip dhcp-server dhcpServerAddress [adminStatus]`
 `no ip dhcp-server [dhcpServerAddress [adminStatus]]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Adds the IP address of a single DHCP server to the list of DHCP servers from which the router can request addresses to allocate to remote users. A maximum of five DHCP servers can be specified. The **no** version removes the specified DHCP server or removes all DHCP servers from the list.

- Options** ■ *dhcpServerAddress*—IP address of the DHCP server that will allocate addresses for remote users
- *adminStatus*—One of the following options:
- `disable`—Disables the DHCP server
 - `drain`—Drains the DHCP server

Mode Global Configuration

ip directed-broadcast

Syntax [no] ip directed-broadcast

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables translation of directed broadcast to physical broadcasts. The **no** version disables the function.

Mode Interface Configuration, Profile Configuration, Subinterface Configuration

ip disable-forwarding

Syntax [no] ip disable-forwarding

Release Information Command introduced before JUNOS Release 7.1.0.

Description Disables forwarding of packets on the SRP Ethernet interface to maintain router performance. The **no** version enables forwarding of packets on the SRP Ethernet interface. You see an error message if you try to set this command for interfaces other than the SRP Ethernet interface.

Mode Interface Configuration, Subinterface Configuration

ip domain-lookup

Syntax [no] ip domain-lookup [transit-virtual-router *vrName*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Without the **transit-virtual-router** option, enables the router to query the configured DNS name servers when it needs an IP hostname-to-IP address translation. With the **transit-virtual-router** option, configures a virtual router to use the name servers you configured for another virtual router. The **no** version without the **transit-virtual-router** option restores the default situation, in which the router does not query the DNS server. The **no** version with the **transit-virtual-router** option stops a virtual router from using the same name servers you configured for another virtual router.

Options ■ *vrName*—Name of the virtual router that has the DNS configuration you want to use for a second virtual router

Mode Global Configuration

ip domain-name

Syntax [no] ip domain-name *domainName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a default domain name for the clients that a name resolver serves. The **no** version deletes the domain name; that is, the domain name will no longer be appended to hostnames in the static host table.

Options ■ *domainName*—Default domain name for your hosts

Mode Global Configuration

ip dos-protection-group

Syntax ip dos-protection-group *groupName*
 no ip dos-protection-group

Release Information Command introduced in JUNOS Release 8.1.0.

Description Attaches an IP denial of service (DoS) protection group to an interface. The **no** version removes the attachment of the DoS protection group from the interface.

Options ■ *groupName*—Name of the DoS protection group; string of up to 31 alphanumeric characters

Mode Interface Configuration

ip dvmrp

Syntax [no] ip dvmrp

Release Information Command introduced before JUNOS Release 7.1.0.

Description Activates DVMRP on an interface. The **no** version removes DVMRP from an interface.

Mode Interface Configuration

ip dvmrp accept-filter

Syntax [no] ip dvmrp accept-filter *listName1* [*distance*] neighbor-list *listName2*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Filters incoming DVMRP reports in accordance with a standard IP access list. The **no** version disables the filter.

- Options**
- *listName1*—Name of the IP access list. If the name is 0, the interface accepts all destinations. You can specify a simple or extended access list; with an extended access list you can specify an address and a subnet mask.
 - *distance*—Number in the range 0–255; default value is 0; the distance associated with the DVMRP route when the router determines the RPF interface for the source of a multicast packet
 - *listName2*—Name of an access list containing the neighbors from which the router will accept reports. If the name is 0, the interface accepts destinations from all its neighbors.

Mode Interface Configuration

ip dvmrp announce-filter

Syntax ip dvmrp announce-filter *listName*
 no ip dvmrp announce-filter

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a list of DVMRP routes that the router will advertise on an interface. The **no** version restores the default situation, in which the router advertises all known routes on the interface.

Options ■ *listName*—Name of the IP access list that specifies the DVMRP routes that the router will advertise on the interface. You can specify a simple or extended access list; with an extended access list you can specify an address and a subnet mask.

Mode Interface Configuration

ip dvmrp auto-summary

Syntax [no] ip dvmrp auto-summary

Release Information Command introduced before JUNOS Release 7.1.0.

Description Summarizes routes automatically on an interface. By default, automatic summarization is enabled. The **no** version disables automatic summarization.

Mode Interface Configuration

ip dvmrp disable

Syntax [no] ip dvmrp disable

Release Information Command introduced before JUNOS Release 7.1.0.

Description Disables DVMRP on an interface without removing the DVMRP configuration. The **no** version reenables the DVMRP configuration on a disabled interface.

Mode Interface Configuration

ip dvmrp metric-offset

Syntax [no] ip dvmrp metric-offset { in | out } [*increment*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Adjusts the number of hops associated with routes passing through an interface. This action indicates that the route is more efficient or less efficient than an alternative route. The **no** version restores the default values.

- Options**
- **in**—Increments the number of hops for a DVMRP route advertised in incoming DVMRP reports. If you do not specify a key word, this option is the default.
 - **out**—Increments the number of hops for a DVMRP route advertised in outgoing DVMRP reports
 - ***increment***—Number of hops associated with this interface; default value is 1 for incoming reports and 0 for outgoing reports.

Mode Interface Configuration

ip dvmrp route-hog-notification

Syntax [no] ip dvmrp route-hog-notification [*limit*]

limit—Number in the range 0–2147483647

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the number of DVMRP routes that the router can record before it generates a system log warning message. The **no** version restores the default setting, 10,000 routes.

Mode Global Configuration

ip dvmrp route-limit

Syntax [no] ip dvmrp route-limit [*limit*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Limits the number of routes that the router can advertise on each interface. The default value is 7000. The **no** version removes the limit for the number of routes that the router can advertise on each interface.

Options ■ *limit*—Number of routes that the router can advertise

Mode Global Configuration

ip dvmrp summary-address

Syntax [no] ip dvmrp summary-address *ipAddress* *mask* [metric *cost*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Advertises a DVMRP summary address on the interface. The **no** version stops the advertising of a summary address on an interface.

- Options**
- *ipAddress*—Summary address
 - *mask*—Subnet mask
 - *cost*—Cost associated with this summary address

Mode Interface Configuration

ip dvmrp unicast-routing

Syntax [no] ip dvmrp unicast-routing

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the exchange of DVMRP unicast routes on an interface not owned by DVMRP. The **no** version disables the exchange of DVMRP unicast routes on an interface not owned by DVMRP.

Mode Interface Configuration

ip dynamic-interface-prefix

Syntax `ip dynamic-interface-prefix [vrf vrfName] prefix`
`no ip dynamic-interface-prefix [vrf vrfName]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the prefix for the names of dynamic shared IP interfaces created for overlapping BGP/MPLS VPNs. The **no** version restores the default prefix, **dyn**.

- Options** ■ *vrfName*—Name of the VRF in which the shared interface is created; a string of 1–32 alphanumeric characters
- *prefix*—String of 1–10 alphanumeric characters

Mode Global Configuration

ip explicit-path

Syntax

Description Defines an explicit path by name and also enables or disables explicit path routing in implementations on routers from other vendors. See the `mpls explicit-path` command for a complete description and syntax.

Mode Global Configuration

ip extcommunity-list

Syntax ip extcommunity-list *listName* { permit | deny }
extendedCommunity [*extendedCommunity*]*

no ip extcommunity-list *listName* [{ permit | deny }
extendedCommunity [*extendedCommunity*]*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines an extended-community (extcommunity) list to be referenced in a route map. The **no** version deletes the extcommunity.

- Options**
- *listName*—Name of the extended-community list
 - permit—Permits membership in the extended community for matching conditions
 - deny—Denies membership in the extended community for matching conditions
 - *extendedCommunity*—Extended community specified in the format:
{ rt | soo } { *ASN:nn* | *ipAddress:nn* }
 - rt—Specifies a route-target community; consists of one or more routers that can receive a set of routes advertised by BGP that carry the extended-community attribute
 - soo—Specifies a Site-of-Origin community; consists of one or more routers that injects a set of routes into BGP that carry the extended-community attribute
 - *ASN:nn*—Identifies the extended community by a 16-bit autonomous system number followed by a 32-bit integer
 - *ipAddress:nn*—Identifies the extended community identified by an IP address followed by a 16-bit integer
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

ip fallback global

Syntax [no] ip fallback global

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables secondary routing table lookup for an interface in a virtual router forwarding table of the parent (global) virtual router if the initial route lookup on a VRF is unsuccessful. The **no** version discontinues secondary routing table lookup.

Mode VRF Configuration

ip filter-options all

Syntax [no] ip filter-options all

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables filtering of packets with IP options on an interface. IP options filtering is disabled by default. The **no** version disables filtering of packets with IP options.

Mode Interface Configuration, Profile Configuration

Related Topics ■ Enabling IP Options Filtering

ip flow-aggregation cache

Syntax [no] ip flow-aggregation cache [as | destination-prefix | prefix | protocol-port | source-prefix]

Release Information Command introduced in JUNOS Release 8.1.0.

Description Creates an aggregation cache and accesses Flow Cache Configuration mode. The **no** version removes the aggregation cache and its configuration.

- Options**
- as—Specifies autonomous system aggregation
 - destination-prefix—Specifies destination prefix aggregation
 - prefix—Specifies prefix aggregation
 - protocol-port—Specifies protocol port aggregation
 - source-prefix—Specifies source prefix aggregation

Mode Flow Cache Configuration, Global Configuration

ip flow-cache entries

Syntax ip flow-cache entries *cacheEntries*
no ip flow-cache entries

Release Information Command introduced before JUNOS Release 7.1.0.

Description Limits the number of entries in the flow cache (for all line modules in the router). The **no** version sets the number of entries back to its default value.

Options ■ *cacheEntries*—Number of cache entries allowed for all line modules in the router in the range 1024–524288; default value is 65536

Mode Global Configuration

ip flow-cache timeout

Syntax ip flow-cache timeout { active *activeTimer* | inactive *inactiveTimer* }
no ip flow-cache timeout { active | inactive }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines the J-Flow activity or inactivity timers. The **no** version restores the default value of each timer.

- Options**
- *activeTimer*—Value of activity timer in the range 0–60 minutes; default value is 30
 - *inactiveTimer*—Value of inactivity timer in the range 10–600 seconds; default value is 15

Mode Global Configuration

ip flow-export

Syntax [no] ip flow-export { *hostName* | *ipAddress* } *udpPort* version 5
 [peer-as | origin-as]

[no] ip flow-export destination { *hostName* | *ipAddress* } *udpPort*

[no] ip flow-export source *interfaceType* *interfaceSpecifier*

[no] ip flow-export version 5 [peer-as | origin-as]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines J-Flow export values for the IP flow. The **no** version removes the export setting.

- Options**
- *hostName*—Name of the remote host for outgoing export datagrams
 - *ipAddress*—IP address of the export destination host
 - *udpPort*—UDP port number
 - version 5—Specifies version 5 of the J-Flow statistical information
 - peer-as—Exports peer-as information
 - origin-as—Exports origin-as information
 - destination—Specifies destination for outgoing export datagrams
 - source—Specifies source interface for outgoing export datagrams
 - *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Global Configuration

ip flow-sampling-mode packet-interval

Syntax ip flow-sampling-mode packet-interval *intervalValue*
 no ip flow-sampling-mode packet-interval

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines the sampling interval for an interface that is running J-Flow. Even though each flow is sampled, the flow sample is not necessarily cached because of system constraints. The **no** version returns the sampling interval to the default value.



NOTE: For interfaces on the ES2 10G LM with either the ES2-S1 GE-8 IOA or the ES2-S2 10GE PR IOA on E120 routers and E320 routers, J-Flow adjusts the maximum sampling interval to 8,388,608 (decimal equivalent of 0x800000) and changes the sampling interval to the closest integer that is a power of two and that is less than or equal to the configured value.

Options ■ *intervalValue*—Sampling interval, in the range 1–4000000000 packets; default value is 4000000000

Mode Global Configuration

ip flow statistics

Syntax [no] ip flow statistics

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables J-Flow statistics. The **no** version disables J-Flow statistics.

Mode Global Configuration

ip ftp source-address

Syntax ip ftp source-address *sourceAddress*
 no ip ftp source-address [*sourceAddress*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies an operational interface by IP address as the source interface in FTP packets sent via the router's FTP client. The **no** version restores the source address in the FTP packets to that on which the FTP connection is made.

Options ■ *sourceAddress*—Source IP address

Mode Global Configuration

ip ftp source-interface

Syntax ip ftp source-interface *interfaceType interfaceSpecifier*
 no ip ftp source-interface [*interfaceType interfaceSpecifier*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Identifies an interface by type and location as the source interface in FTP packets sent via the router's FTP client. The **no** version restores the source address in the FTP packets to that on which the FTP connection is made.

- Options** ■ *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Global Configuration

ip-hint

Syntax ip-hint { enable | disable }
no ip-hint

Release Information Command introduced before JUNOS Release 7.1.0.

Description When enabled, the E Series router preallocates an IP address for the remote (B-RAS) user before calling authentication. The address is then passed as a hint in the authentication request to the RADIUS server. The **no** version disables the feature.

- Options**
- enable—Specifies the feature
 - disable—Disables the feature; this is the default setting

Mode Domain Map Configuration

ip http

Syntax [no] ip http

Release Information Command introduced in JUNOS Release 7.2.0.

Description Creates the HTTP local server. The **no** version deletes the HTTP local server.

Mode Global Configuration

ip http access-class

Syntax ip http access-class *listName*
 no ip http access-class

Release Information Command introduced in JUNOS Release 7.2.0.

Description Specifies the standard IP access list that identifies the subscribers who are authorized to connect to the HTTP local server. The **no** version removes the association between the access list and the HTTP local server.

Options ■ *listName*—Name of the access list

Mode Global Configuration

ip http max-connection-time

Syntax ip http max-connection-time *seconds*
 no ip http max-connection-time

Release Information Command introduced in JUNOS Release 7.2.0.

Description Specifies the maximum time that the HTTP local server maintains an inactive connection. The **no** version restores the default time.

Options ■ *seconds*—Either 0 (unlimited) or the number of seconds in the range 3–7200; default value is 30 seconds

Mode Global Configuration

ip http port

Syntax ip http port *portNumber*
 no ip http port

Release Information Command introduced in JUNOS Release 7.2.0.

Description Specifies the port on which the HTTP local server receives connection attempts. The **no** version restores the default port number.

Options ■ *portNumber*—Number of the port, in the range 0–65535; the default is port 80

Mode Global Configuration

ip http redirectUrl

Syntax ip http redirectUrl *url*
 no ip http redirectUrl

Release Information Command introduced in JUNOS Release 7.2.0.

Description Specifies the URL to which a subscriber's initial Web browser session is redirected, enabling initial provisioning and service selection for the subscriber. The **no** version removes the redirection action.

Options ■ *url*—Name of the URL; 64 characters maximum

Mode Interface Configuration, Profile Configuration, Subinterface Configuration

ip http same-host-limit

Syntax ip http same-host-limit *maxConnections*
 no ip http same-host-limit

Release Information Command introduced in JUNOS Release 7.2.0.

Description Specifies the maximum number of connections that can exist between one IP address and the HTTP local server. The **no** version restores the default number of allowed connections.

Options ■ *maxConnections*—Maximum number of connections allowed, in the range 0–1000; the default is 3

Mode Global Configuration

ip http server

Syntax [no] ip http server

Release Information Command introduced in JUNOS Release 7.2.0.

Description Enables the HTTP local server. The **no** version disables the HTTP local server.

Mode Global Configuration

ip icmp update-source

Syntax `ip icmp update-source [vrf vrfName] { interfaceType interfaceSpecifier | ipAddress }`
 `no ip icmp update-source [vrf vrfName] [interfaceType interfaceSpecifier`
 `| ipAddress]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a unique source address or interface for any ICMP messages that the E Series router generates. The **no** version removes the unique source specification.

- Options**
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *ipAddress*—IP address of an E Series interface over which you want to send ICMP messages

Mode Global Configuration

ip igmp

Syntax [no] ip igmp

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables IGMP on an interface, and sets the IGMP version to IGMPv2. The **no** version disables IGMP on an interface.

Mode Interface Configuration, Profile Configuration

ip igmp access-group

Syntax ip igmp access-group *accessListName*
 no ip igmp access-group

Release Information Command introduced before JUNOS Release 7.1.0.

Description Restricts hosts on this subnet to joining multicast groups on the specified IP access list. The **no** version removes the association with the specified access list and allows hosts on the subnet to join any multicast group.

Options ■ *accessListName*—Name of the access list; a string of up to 32 characters

Mode Interface Configuration, Profile Configuration

ip igmp access-source-group

Syntax ip igmp access-source-group *accessListName*
 no ip igmp access-source-group

Release Information Command introduced before JUNOS Release 7.1.0.

Description Restricts hosts on this subnet to membership in those source-groups (also known as “channels”) permitted by the specified IP access list. The **no** version removes any access list restriction.

Options ■ *accessListName*—Name of the access list; a string of up to 32 characters

Mode Interface Configuration, Profile Configuration

ip igmp apply-oif-map

Syntax ip igmp apply-oif-map *mapName*
 no ip igmp apply-oif-map

Release Information Command introduced before JUNOS Release 7.1.0.

Description Applies the specified outgoing interface (OIF) map to the current interface. The **no** version removes the outgoing interface map association from the interface.

Options ■ *mapName*—Name of the OIF map

Mode Interface Configuration, Profile Configuration

ip igmp explicit-tracking

Syntax [no] ip igmp explicit-tracking [disable-if-igmp-v2-detected]

Release Information Command introduced in JUNOS Release 8.2.0.

Description Enables explicit host tracking for IGMP interfaces. The **no** version disables explicit host tracking on the interface or with the **disable-if-igmp-v2-detected** keyword reverts to the default explicit host tracking.

Options ■ disable-if-igmp-v2-detected—Disables explicit host tracking if IGMP V2 hosts detected on IGMP V3 interfaces

Mode Interface Configuration, Profile Configuration

ip igmp group limit

Syntax ip igmp group limit *groupLimit*
 no ip igmp group limit

Release Information Command introduced before JUNOS Release 7.1.0.

Description Limits the number of IGMP groups that an interface can accept. The **no** version restores the default situation, in which there is no limit to the number of IGMP groups that the interface accepts.

Options ■ *groupLimit*—Maximum number of IGMP groups that an interface can accept in the range 0–64,000

Mode Interface Configuration, Profile Configuration

ip igmp immediate-leave

Syntax [no] ip igmp immediate-leave

Release Information Command introduced before JUNOS Release 7.1.0.

Description Removes an interface immediately when the router receives an leave group membership message from the host associated with this interface. The **no** version restores the default situation, in which the router issues query messages to multicast groups and removes an interface if the associated host does not return a group membership report within a certain length of time.



CAUTION: Issue this command only on IGMPv2 interfaces to which one IGMP client is connected. Do not issue this command to interfaces to which more than one IGMP client is connected.

Mode Interface Configuration, Profile Configuration

ip igmp last-member-query-interval

Syntax ip igmp last-member-query-interval *tenthsOfaSecond*
 no ip igmp last-member-query-interval

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies in tenths of a second the maximum time the router waits for a response after sending a last member query. The router sends a last member query when it receives an IGMPv2 leave message or an IGMPv3 state change report. The **no** version restores the default value, 10 tenths of a second (1 second).

Options ■ *tenthsOfaSecond*—Time interval between receipt of an IGMP leave message and sending out of a query in the range 1–254 tenths of a second. Using a lower value allows members to leave groups more quickly.

Mode Interface Configuration, Profile Configuration

ip igmp oif-map

Syntax [no] ip igmp oif-map *mapName* { *interfaceType interfaceSpecifier* | self }
[*groupPrefix* [*sourcePrefix*]]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates an outgoing interface (OIF) map. The **no** version removes an outgoing interface map attribute or the entire outgoing interface map.

- Options**
- *mapName*—Name of the OIF map
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - self—Specifies that the multicast outgoing interface is the same as IGMP join interface
 - *groupPrefix*—Group prefix in the form *ipAddress/maskLength*
 - *sourcePrefix*—Source prefix in the form *ipAddress/maskLength*

Mode Global Configuration

ip igmp promiscuous

Syntax ip igmp promiscuous { on | off }
no ip igmp promiscuous

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the specified interface to accept IGMP reports from hosts on any subnet. The **no** version specifies that an IGMP interface should use the Router Configuration mode setting (see the **igmp promiscuous** command) to determine from which subnets it can accept IGMP reports.

- Options**
- on—Enables the interface to accept IGMP reports from hosts on any subnet
 - off—Allows the interface to accept IGMP reports only from hosts on subnets associated with this interface

Mode Interface Configuration, Profile Configuration

ip igmp-proxy

Syntax [no] ip igmp-proxy [version { 2 | 3 }]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables IGMP proxy on an interface and specifies the version. Version 2 is enabled by default. The **no** version disables IGMP proxy for an interface.

- Options**
- 2—Specifies IGMP proxy version 2
 - 3—Specifies IGMP proxy version 3

Mode Interface Configuration

ip igmp-proxy unsolicited-report-interval

Syntax ip igmp-proxy unsolicited-report-interval *tenths-of-a-second*
no ip igmp-proxy unsolicited-report-interval

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies how often the upstream interface should transmit unsolicited reports. This command has no effect on interfaces other than the upstream value. The **no** version transmits unsolicited reports using the default value, 400 tenths of a second.



NOTE: Issue this command only on the upstream interface. Otherwise, this command will have no effect.

Options ■ *tenths-of-a-second*—Time interval at which the interface transmits unsolicited reports

Mode Interface Configuration

ip igmp-proxy V1-router-present-time

Syntax ip igmp-proxy V1-router-present-time *seconds*
no ip igmp-proxy V1-router-present-time

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies how long the router assumes that there is an IGMPv1 querier router on the subnet after the router receives an IGMP V1 query on this interface. The **no** version restores the default value, 10 seconds.

Options ■ *seconds*—Time for which the router assumes that there is an IGMPv1 querier router on the subnet after the router receives an IGMP V1 query on this interface

Mode Interface Configuration

ip igmp querier

Syntax [no] ip igmp querier

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that the interface will act as a querier when you configure IGMPv1 on an interface; this is the default behavior. The **no** version specifies that this interface will not issue query packets.



NOTE: This command is valid only for interfaces on configured with IGMPv1.

Mode Interface Configuration, Profile Configuration

ip igmp querier-timeout

Syntax ip igmp querier-timeout *seconds*
 no ip igmp querier-timeout

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the time that the interface waits before declaring itself as the querier. The **no** version restores the default value, twice the query interval.

Options ■ *seconds*—Time interval between the last query from the previous router and the first query from this interface

Mode Interface Configuration, Profile Configuration

ip igmp query-interval

Syntax ip igmp query-interval *seconds*
 no ip igmp query-interval

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets how often the router sends IGMP host-query packets from this interface. The **no** version restores the default value, 125 seconds.

Options ■ *seconds*—Polling interval in the range 0–65535 seconds

Mode Interface Configuration, Profile Configuration

ip igmp query-max-response-time

Syntax ip igmp query-max-response-time *tenthsOfaSecond*
 no ip igmp query-max-response-time

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the period in tenths of a second during which the host is expected to respond to an IGMP query. IGMP version 2 includes this value in IGMP query messages sent out on the interface. You cannot set this value on interfaces running IGMP version 1. The **no** version restores the default value, 100 tenths of a second (10 seconds).

Options ■ *tenthsOfaSecond*—Time interval between receipt of an IGMP query and the response; in the range 1–254 tenths of a second.

Mode Interface Configuration, Profile Configuration

ip igmp robustness

Syntax ip igmp robustness *numberOfMessages*
 no ip igmp robustness

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the number of times that the router sends IGMP group-specific queries before declaring a group to no longer have any members on an interface. The **no** version restores the default value, 3.

Options ■ *numberOfMessages*—Number of times that the router sends IGMP group-specific queries in the range 1–4

Mode Interface Configuration, Profile Configuration

ip igmp ssm-map enable

Syntax [no] ip igmp ssm-map enable

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables SSM mapping on the router. SSM mapping statically assigns sources to IGMPv1 and IGMPv2 groups. You must use SSM mapping for IGMPv1 and IGMPv2 hosts to interoperate with PIM SSM. SSM mapping allows the router to use a statically configured list to translate (*,G) memberships to (S,G) memberships. The **no** version disables the SSM map.

Mode Privileged Exec, User Exec

ip igmp ssm-map static

Syntax [no] ip igmp ssm-map static *accessListName* *sourceAddress*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies an access list and source address for use in SSM mapping. SSM mapping statically assigns sources to IGMPv1 and IGMPv2 groups. You must use SSM mapping for IGMPv1 and IGMPv2 hosts to interoperate with PIM SSM. SSM mapping allows the router to use a statically configured list to translate (*,G) memberships to (S,G) memberships. The **no** version removes the SSM map association.

- Options**
- *accessListName*—Name of the access control list
 - *sourceAddress*—Address of the source

Mode Privileged Exec, User Exec

ip igmp static-exclude

Syntax [no] ip igmp static-exclude *sourceAddress* *groupAddress*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that an interface not handle multicast traffic for one or more (S,G) combinations. The **no** version removes the (S,G) exclusion from the interface.

- Options**
- *sourceAddress*—Address of the source
 - *groupAddress*—Address of the group

Mode Interface Configuration, Profile Configuration

ip igmp static-group

Syntax [no] ip igmp static-group *groupAddress*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns an interface to handle all multicast traffic for a group. The interface sets no timers for this group. The **no** version removes the group from the interface.

Options ■ *groupAddress*—Address of the group

Mode Interface Configuration, Profile Configuration

ip igmp static-include

Syntax [no] ip igmp static-include *sourceAddress* *groupAddress*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns an interface to handle multicast traffic for one or more (S,G) combinations. The **no** version removes the (S,G) association from the interface.

- Options**
- *sourceAddress*—Address of the source
 - *groupAddress*—Address of the group

Mode Interface Configuration, Profile Configuration

ip igmp version

Syntax ip igmp version { 3 | 2 | 1 | passive }
no ip igmp version

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the IGMP version for the interface. The **no** version restores the default value, IGMPv2.

- Options**
- 3—Specifies IGMP version 3
 - 2—Specifies IGMP version 2
 - 1—Specifies IGMP version 1
 - passive—Configures a mapped OIF as a passive interface with only multicast-data-forwarding capability

Mode Interface Configuration, Profile Configuration

ip ignore-df-bit

Syntax [no] ip ignore-df-bit

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that the router ignores the don't-fragment bit if present in the IP header of packets crossing the configured interface; the router then fragments packets even if the bit is present. The **no** version restores the default behavior, which is to consider the DF bit before fragmenting.

Mode Interface Configuration, Profile Configuration

ip inactivity-timer

Syntax [no] ip inactivity-timer *inactiveTime*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures an inactivity timer. IP polls the dynamic interface at the configured interval to determine whether the interface was active during the interval. Inactive interfaces are deleted only when the period of inactivity is equal to or greater than the configured value. The **no** version disables the timer.

Options ■ *inactiveTime*—Length of time in the range 0–63335 minutes; a value of 0 specifies that dynamically created subscriber interfaces are not deleted

Mode Interface Configuration, Profile Configuration

ip initial-sequence-preference

Syntax ip initial-sequence-preference *preference*
 no ip initial-sequence-preference

Release Information Command introduced in JUNOS Release 8.1.0.

Description Configures the warm restart replay preference for an IP interface after a high availability switchover. The **no** version restores the default value.

Options ■ *preference*—Preference value, 0 or 1; 1 indicates highest preference; default value is 0

Mode Subinterface Configuration

ip interface

Syntax no ip interface

Description This command has only a **no** version. See the no ip interface command for a complete description.

Mode Interface Configuration, Subinterface Configuration

ip irdp

Syntax [no] ip irdp

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables ICMP Router Discovery Protocol processing on an interface. The **no** version disables IRDP routing.

Mode Interface Configuration, Subinterface Configuration

ip local alias

Syntax ip local alias aliasName pool-name *poolName*

[no] ip local alias aliasName

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies an alias for a local address pool. The **no** version deletes the alias name.

- Options**
- *aliasName*—Text string in the range 1–16 characters that defines an alias name for the local address pool
 - *poolName*—Text string in the range 1–16 characters that is the name of the local address pool

Mode Global Configuration

ip local pool

Syntax [no] ip local pool *name* [*startIpAddress* [*endIpAddress*]]
[warning *highUtilization* *abatedUtilization*] [snmpTrap]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the pool name, the starting address, the ending address, group name, the utilization threshold, and the SNMP trap flag. The **no** version deletes a local pool.

- Options**
- *name*—Text string in the range 1–16 characters that defines the name of the local address *pool*
 - *startIpAddress*—Starting IP address in the local address pool
 - *endIpAddress*—Ending IP address in the local address pool
 - warning—Specifies one of the following utilization warnings:
 - *highUtilization*—High utilization value; a number in the range 1–100; default value is 85
 - *abatedUtilization*—Abated utilization value; a number in the range 1–100; default value is 75
 - snmpTrap—Enables SNMP pool utilization traps

Mode Global Configuration

ip local pool snmpTrap

Syntax [no] ip local pool *name* snmpTrap

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables SNMP pool utilization traps. The **no** version disables SNMP pool utilization traps.

Options ■ *name*—Text string in the range 1–16 characters that defines the name of the local address *pool*

Mode Global Configuration

ip local pool warning

Syntax ip local pool *name* warning *highUtilization* *abatedUtilization* [snmpTrap]
 no ip local pool *name* warning [*highUtilization* *abatedUtilization*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Identifies the warning threshold values. The **no** version resets the thresholds to their default values.

- Options**
- *name*—Text string in the range 1–16 characters that defines the name of the local address *pool*
 - *highUtilization*—High utilization value; a number in the range 1–100; default value is 85
 - *abatedUtilization*—Abated utilization value; a number in the range 1–100; default value is 75
 - snmpTrap—Enables snmp pool utilization traps

Mode Global Configuration

ip local shared-pool

Syntax ip local shared-pool *localPoolName dhcpPoolName*
 no ip local shared-pool *localPoolName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures a shared local address pool that shares addresses from the specified DHCP local server address pool in the same virtual router. The **no** version deletes the shared local address pool.

- Options** ■ *localPoolName*—Text string in the range 1–16 characters that defines the name of the shared local address pool that obtains addresses from a DHCP local server address pool.
- *dhcpPoolName*—Text string in the range 1–64 characters that defines the name of the DHCP local address pool that provides addresses to the shared local address pool.

Mode Global Configuration

ip mac-validate

Syntax ip mac-validate [strict | loose]
 no ip mac-validate

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables MAC address validation on a per interface basis. When MAC address validation is enabled, the router checks the entry in the MAC validation table that corresponds to the IP source address of an incoming packet. The MAC source address of the packet must match the MAC source address of the table entry for the router to forward the packet. The **no** version disables the feature.

- Options**
- strict—Prevents transmission of IP packets that do not reside in the validation table
 - loose—Allows IP packets to pass through even though the packets do not have entries in the validation table; only packets that have matching IP–MAC pair entries in the table are validated; this is the default setting

Mode Interface Configuration

ip mask-reply

Syntax [no] ip mask-reply

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables ICMP netmask reply. The **no** version disables the feature.

Mode Interface Configuration, Subinterface Configuration

ip match-policy-list

Syntax [no] ip match-policy-list *policyList* { permit | deny }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates an IP policy list and launches the policy list configuration mode. The **no** version deletes the policy list.

- Options**
- *policyList*—Name of the policy list
 - permit—Defines the policy list as a permit
 - deny—Defines the policy list as a deny

Mode Global Configuration

ip mirror

Syntax `ip mirror mirrorInterfaceType mirrorInterfaceSpecifier`
`[analyzerInterfaceType analyzerInterfaceSpecifier [next-hop nextHop]]`
`no ip mirror mirrorInterfaceType mirrorInterfaceSpecifier`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the specified interface to mirror all IP ingress and egress traffic, and directs the mirrored traffic to an analyzer interface. The **no** version disables mirroring on the interface.



NOTE: This command is deprecated and might be removed completely in a future release. The function provided by this command has been replaced by the updated packet mirroring feature and the **ip policy** command used with the **secure-input** and **secure-output** keywords.

- Options**
- *mirrorInterfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *mirrorInterfaceSpecifier*—Particular interface that performs the interface mirroring function; see Interface Types and Specifiers on page 5
 - *analyzerInterfaceType*—Interface type
 - *analyzerInterfaceSpecifier*—Particular interface used as the analyzer interface; if omitted, the virtual router's default analyzer interface is used
 - *nextHop*—Next-hop IP address to the remote analyzer host; required if the analyzer interface is a shared medium, such as Ethernet

Mode Global Configuration

Related Topics ■ Configuring CLI-Based Mirroring

ip mobile home-agent

Syntax `ip mobile home-agent [care-of-access acl] [lifetime lifetimeSeconds]
[replay replaySeconds] [reverse-tunnel-off]`

`no ip mobile home-agent`

Release Information Command introduced in JUNOS Release 9.0.0.

Description Configures the Mobile IP home agent on a virtual router. Issuing this command does not affect existing parameters such as lifetime, replay value, or care-of-access ACL for any mobile node's existing binding. The new parameters take effect only upon each re-registration or new registration. For example, configuring a shorter lifetime does not cause an existing binding to be removed prematurely, but the new lifetime value is used only upon re-registration by a mobile node so that both the mobile node and the home agent are informed of the newly negotiated value. The **no** version disables the home agent service on the virtual router.



NOTE: The values for lifetime, replay, and care-of access configured per mobile host by using the **ip mobile host** command override the values configured by using the **ip mobile home-agent** command.

- Options**
- *acl*—Name of the access control list applied to the care-of-access, which restricts access for foreign agents or networks. You can override this care-of-access ACL with other ACLs for specific host mobile nodes. By default, the router does not apply a care-of-access ACL
 - *lifetimeSeconds*—Maximum number of seconds, in the range 5–65535, during which registration requests are established; default value is 36,000 seconds. The maximum lifetime configured for specific mobile nodes can override this lifetime value
 - *replaySeconds*—Number of seconds, in the range 1–255, by which a registration request can exceed the home agent configured time value; default value is 7 seconds
 - *reverse-tunnel-off*—Disables reverse tunneling support by the home agent, which denies T bit registration requests. By default, reverse tunneling is enabled on the router. When you modify support for reverse tunnels, the modification takes effect only for subsequently accepted registration requests

Mode Global Configuration

ip mobile host

Syntax ip mobile host { nai { *user@realm* | *@realm* | *@* } | *ipAddress* } [*aaa*]
[*care-of-access acl*] [*lifetime lifetimeSeconds*]

no ip mobile host { nai { *user@realm* | *@realm* | *@* } | *ipAddress* }

Release Information Command introduced in JUNOS Release 9.0.0.

Description Configures the mobile node on a virtual router with an optional host network access identifier (NAI) address or the home address (IP address of the home agent). You can specify either the **nai** keyword or a non-zero home address (IP address of the mobile node). If the AAA server does not provide all configuration information, a local lookup retrieves the configuration information by either matching the NAI registration request or the home address registration request. The **no** version deletes the configuration of the mobile node on the virtual router.

- Options**
- *user@realm*—Name of the user for the mobile node specification when the **nai** keyword is specified, in the format *user@realm*, where *realm* is the domain name
 - *@realm*—Name of the user for the mobile node specification when the **nai** keyword is specified, in the format *@realm*, where *realm* is the domain name
 - *@*—Name of the user for the mobile node specification when the **nai** keyword is specified, in the format *@*
 - *ipAddress*—IP address of the home agent
 - *aaa*—Causes the router to use the AAA server to validate registration requests and to obtain configuration and security association information
 - *acl*—Name of the access control list applied to the care-of-access, which restricts access for foreign agents or networks. You can override this care-of-access ACL with other ACLs for specific host mobile nodes. By default, the router does not apply a care-of-access ACL
 - *lifetimeSeconds*—Maximum number of seconds during which the registration requests are established; default value is 36,000 seconds. The maximum lifetime configured for specific mobile nodes can override this lifetime value

Mode Global Configuration

ip mobile profile

Syntax [no] ip mobile profile *profileName*

Release Information Command introduced in JUNOS Release 9.0.0.

Description Configures or associates a preconfigured interface profile with the home agent in a virtual router. You must configure a mobile profile for every virtual router in which the home agent exists. The profile parameters determine the interface characteristics for Mobile IP signaling. The **no** version removes the profile configuration from the virtual router.

Options ■ *profileName*—Name of the profile associated with the home agent for Mobile IP signaling in a virtual router

Mode Global Configuration

ip mobile secure foreign-agent

Syntax ip mobile secure foreign-agent *ipAddress* spi *spi* key { hex *hexKeyVal* | ascii *asciiKeyVal* } [replay timestamp within *seconds*] [algorithm { hmac-md5 | keyed-md5 }]

no ip mobile secure foreign-agent *ipAddress* spi *spi* key { hex *hexKeyVal* | ascii *asciiKeyVal* }

Release Information Command introduced in JUNOS Release 9.0.0.

Description Configures the security associations for a foreign agent by specifying a security parameter index (SPI) value and an authentication key. You can specify the interval within which a registration request can exceed the home agent configured time value by specifying the **replay timestamp within** keyword. The **no** version deletes the security associations for the specified foreign agent on the virtual router.

- Options**
- *ipAddress*—IP address of the foreign agent
 - *spi*—Security parameter index (SPI) value, a specific 4-octet hexadecimal number, in the range 0x100–0xFFFFFFFF, that authenticates inbound requests and permits authentication for outbound registration requests
 - *hexKeyVal*—128-bit hexadecimal number, in the range 0x0–0xFFFFFFFFE, that specifies the authentication key for a specific security association
 - *asciiKeyVal*—128-bit alphanumeric value, up to a maximum of 16 characters, that specifies the authentication key for a specific security association
 - *seconds*—Number of seconds, in the range 1–255, by which a registration request can exceed the home agent configured time value; default value is 7 seconds
 - hmac-md5—Specifies the authentication algorithm for Mobile IP messages, default value is hmac-md5
 - keyed-md5—Specifies the authentication algorithm for Mobile IP messages

Mode Global Configuration

ip mobile secure host

Syntax ip mobile secure host { nai { *user@realm* | *@realm* | *@* } | *ipAddress* } spi *spi*
key { hex *hexKeyVal* | ascii *asciiKeyVal* } [replay timestamp within *seconds*]
[algorithm { hmac-md5 | keyed-md5 }]

no ip mobile secure host { nai { *user@realm* | *@realm* } | *ipAddress* } spi *spi*
key { hex *hexKeyVal* | ascii *asciiKeyVal* }

Release Information Command introduced in JUNOS Release 9.0.0.

Description Configures the security associations for a mobile node. You can configure the security associations for a mobile node only after configuring a corresponding host configuration for the mobile node, and only if you have not configured the AAA service on the virtual router. You can specify the interval within which a registration request can exceed the home agent configured time value by specifying the **replay timestamp within** keyword. The **no** version deletes the security associations for the specified host on the virtual router.



NOTE: If you delete a mobile node host by using the **no ip mobile host** command, all security associations that you configured for this host are deleted.

- Options**
- *user@realm*—Name of the user for the mobile node specification when the **nai** keyword is specified, in the format *user@realm*, where *realm* is the domain name
 - *@realm*—Name of the user for the mobile node specification when the **nai** keyword is specified, in the format *@realm*, where *realm* is the domain name
 - *@*—Name of the user for the mobile node specification when the **nai** keyword is specified, in the format *@*
 - *ip Address*—IP address of the foreign agent
 - *spi*—Security parameter index (SPI) value, a specific 4-octet hexadecimal number, in the range 0x100–0xFFFFFFFF, that authenticates inbound requests and permits authentication for outbound registration requests
 - *hexKeyVal*—128-bit hexadecimal number, in the range 0x0–0xFFFFFFFFFE, that specifies the authentication key for a specific security association
 - *asciiKeyVal*—128-bit alphanumeric value, up to a maximum of 16 characters, that specifies the authentication key for a specific security association
 - *seconds*—Number of seconds, in the range 1–255, by which a registration request can exceed the home agent configured time value; default value is 7 seconds
 - *hmac-md5*—Specifies the authentication algorithm for Mobile IP messages, default value is *hmac-md5*
 - *keyed-md5*—Specifies the authentication algorithm for Mobile IP messages

Mode Global Configuration

ip mpls forwarding-mode label-switched

Syntax [no] ip mpls forwarding-mode label-switched

Release Information Command introduced before JUNOS Release 7.1.0.

Description Generates a label for each different FEC that a BGP route points to in a BGP/MPLS VPN. The **no** version restores the default, generating a single label for all BGP routes sent from a given VRF.



NOTE: For some types of routes, the router always generates a per-VRF label, regardless of the status of this command. See *Creating labels per FEC* in the *JUNOS BGP and MPLS Configuration Guide*, for details.

Mode VRF Configuration

ip mtu

Syntax [no] ip mtu [*mtuSize*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the maximum transmission unit size of IP packets sent on an interface. The **no** version restores the default value.

Options ■ *mtuSize*—Maximum number of packet transmissions permitted on an interface; in the range 160–10240; default value is 0, which means that the router takes the value from a lower protocol layer

Mode Interface Configuration, Profile Configuration, Subinterface Configuration

ip multicast admission-bandwidth-limit

Syntax [no] ip multicast admission-bandwidth-limit *limitValue*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Specifies multicast admission bandwidth (in kilobits per second) for a given interface. The **no** version removes the admission bandwidth limit.

Options ■ *limitValue*—Maximum admission bandwidth (in kilobits per second) permitted on an interface; default value is 0, which disables the limit

Mode Interface Configuration, Profile Configuration

ip multicast ioa-packet-replication

Syntax ip multicast ioa-packet-replication *interfaceType interfaceSpecifier*
 no ip multicast ioa-packet-replication

Release Information Command introduced in JUNOS Release 7.3.0.

Description Enables IPv4 hardware multicast packet replication on port 8 of a high-density Ethernet I/O module or IOA. The **no** version disables hardware multicast packet replication.

Options ■ *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Interface Configuration

ip multicast-routing

Syntax [no] ip multicast-routing

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables IP multicast routing on the router. The **no** version disables IP multicast routing on the router.

Mode Global Configuration

ip multicast-routing bandwidth-map

Syntax ip multicast-routing bandwidth-map *routeMapName*
 no ip multicast-routing bandwidth-map

Release Information Command introduced in JUNOS Release 7.1.0.

Description Enables the QoS adjust function on the router. The **no** version disables the QoS adjust function on the router.

Options ■ *routeMapName*—Name of the route map you want to use for the bandwidth map

Mode Global Configuration

ip multicast-routing disable-rpf-check

Syntax ip multicast-routing disable-rpf-check *ipAccessList*
 no ip multicast-routing disable-rpf-check

Release Information Command introduced before JUNOS Release 7.1.0.

Description Disables RPF checks for the (S,G) pairs in the specified access list. The **no** version restores the default situation, in which the router performs RPF checks for all (S,G) pairs.

Options ■ *ipAccessList*—Name of the IP access list that specifies the (S,G) pairs

Mode Global Configuration

ip multicast-routing permanent-mroute

Syntax ip multicast-routing permanent-mroute *accessListName*
 no ip multicast-routing permanent-mroute

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that newly created mroutes that match the specified access list do not get timed out. The **no** version of this command prevents any new mroutes from becoming permanent. However, it does not remove any existing permanent mroutes. To remove existing permanent mroutes, use the **clear ip mroute** command.

Options ■ *accessListName*—Name of the IP access list that contains the mroutes

Mode Global Configuration

ip multipath round-robin

Syntax [no] ip multipath round-robin

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies round-robin as the mode for ECMP load sharing on an interface. The **no** version restores the default value, hashed.

Mode Subinterface Configuration

ip name-server

Syntax [no] ip name-server *serverIpAddress* [*serverIpAddress*]*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a DNS name server that the router can query for hostname-to-IP address resolution. The **no** version deletes the name server.

- Options**
- *serverIpAddress*—IP or IPv6 address of a DNS name server
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

ip nat

Syntax [no] ip nat { inside | outside }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Marks interfaces that participate in NAT translation as residing on the inside or the outside network. The **no** version unmarks the interface so that it does not participate in NAT translation.

- Options**
- inside—Specifies that the interface resides on the inside (private) portion of the network. The inside portion of the network uses nonroutable IP addresses.
 - outside—Specifies that the interface resides on the outside (public) portion of the network. The outside portion of the network (for example, the Internet) uses routable legitimate addresses.

Mode Interface Configuration, Profile Configuration

ip nat inside source list

Syntax ip nat inside source list *accessListName* pool *poolName* [overload]
 no ip nat inside source list *accessListName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates dynamic translation rules that are applied to a source address when routing a packet from the inside network to the outside network, and for translating the destination address when a packet returns from the outside network to the inside network. The **no** version removes the dynamic translation rule.



NOTE: This command does not remove any dynamic translations from the translation table.

- Options**
- *accessListName*—Name of the access list that you want to use for this dynamic translation
 - *poolName*—Name of the NAT IP address pool that contains addresses you want to use when translating matched access list addresses
 - **overload**—Specifies that the translation process create extended translation table entries (IP address, protocol, and port values)

Mode Global Configuration

ip nat inside source static

Syntax [no] ip nat inside source static *localIpAddress* *globalIpAddress*

[no] ip nat inside source static { tcp | udp } *localIpAddress* *localPort* *globalIpAddress* *globalPort*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates static translations for a source address when routing a packet from the inside network to the outside network, and “untranslates” the destination address when a packet returns from the outside network to the inside network. The **no** version removes the static translation and purges the associated translations from the translation table.

- Options**
- tcp—Indicates a TCP port
 - udp—Indicates a UDP port
 - *localIpAddress*—Inside local address
 - *localPort*—Inside local TCP or UDP port
 - *globalIpAddress*—Inside global address
 - *globalPort* —Inside global TCP or UDP port

Mode Global Configuration

ip nat outside source list

Syntax ip nat outside source list *accessListName* pool *poolName*
 no ip nat outside source list *accessListName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates dynamic translation rules that are applied to a source address when routing a packet from the outside network to the inside network, and used for translating the destination address when a packet returns to the outside network from the inside network. The **no** version removes the dynamic translation rule.



NOTE: This command does not remove any dynamic translations from the translation table.

- Options**
- *accessListName*—Name of the access list that you want to use for this dynamic translation
 - *poolName*—Name of the NAT IP address pool that contains addresses you want to use when translating matched access list addresses

Mode Global Configuration

ip nat outside source static

Syntax [no] ip nat outside source static *globalIpAddress* *localIpAddress*

[no] ip nat outside source static { tcp | udp } *globalIpAddress* *globalPort* *localIpAddress* *localPort*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Translates the source address when routing a packet from the outside network to the inside network, and “untranslates” the destination address when a packet travels from the inside network to the outside network. The **no** version removes the static translation and purges the associated translations from the translation table.

- Options**
- tcp—Indicates a TCP port
 - udp—Indicates a UDP port
 - *globalIpAddress*—Inside global address
 - *globalPort*—Inside global TCP or UDP port
 - *localIpAddress*—Inside local address
 - *localPort*—Inside local TCP or UDP port

Mode Global Configuration

ip nat pool

Syntax `ip nat pool name [startIpAddress endIpAddress]
{ netmask networkMask | prefix-length length }`

`no ip nat pool name`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates an address pool from which the NAT router obtains an address when performing a dynamic translation. You can create address pools with either a single range or multiple, nonoverlapping ranges. The **no** version removes the NAT pool.



NOTE: The router will not allow you to remove a pool that has allocations outstanding. Before removing this type of pool, you must remove the dynamic translation, clear any outstanding translations, and then remove the pool.



CAUTION: Specifying a range in “single line” mode from the CLI replaces all other ranges. You cannot specify a range in this mode if any existing ranges are in use. To add additional ranges, issue this command to access IP NAT Pool Configuration mode.

- Options**
- *name*—Name of the address pool; 32 alphanumeric characters maximum
 - *startIpAddress*—First IP address (inclusive) in the NAT pool range you are creating; omitting this value in the command (along with *endIpAddress*) launches the IP NAT Pool Configuration mode, in which you can enter multiple, discontinuous ranges
 - *endIpAddress*—Last IP address (inclusive) in the NAT pool range you are creating; omitting this value in the command (along with *startIpAddress*) accesses IP NAT Pool Configuration mode, in which you can enter multiple, discontinuous ranges
 - *ipAddressMask*—Subnet mask for any NAT pool ranges you specify
 - *length*—Length of the network prefix; the number of bits masking the base address that results in the address that you want to match

Mode Global Configuration

ip nat translation

Syntax `ip nat translation { timeout | udp-timeout | dns-timeout | tcp-timeout | finrst-timeout | icmp-timeout | gre-timeout } seconds`

`no ip nat translation { timeout | udp-timeout | dns-timeout | tcp-timeout | finrst-timeout | icmp-timeout | gre-timeout }`

Release Information Command introduced before JUNOS Release 7.1.0.
gre-timeout keyword added in JUNOS Release 7.3.0.

Description Changes or disables translation timeouts, per virtual router, for existing and newly created translations in the translation table. All timeouts for this command support a range of 1–2147483 seconds (about 25 days). The **no** version enables the timer using its default value.



NOTE: GRE translations are used as optimizations to discard GRE traffic. You can use the **gre-timeout** keyword to control GRE aging timeout, even though we do not support NATP for GRE. The GRE aging timer has no effect on any simple translations GRE might use.

- Options**
- **timeout**—Sets aging time for dynamic translations (except for overloaded translations); default value is 86400 seconds (24 hours)
 - **udp-timeout**—Sets aging time for UDP protocol translations; default value is 300 seconds (5 minutes)
 - **dns-timeout**—Sets aging time for DNS protocol translations (port 53 on TCP or UDP); default value is 60 seconds
 - **tcp-timeout**—Sets aging time for TCP protocol translations; default value is 86400 seconds (24 hours)
 - **first-timeout**—Sets aging time for TCP connections terminated with RST or FIN flags; default value is 60 seconds
 - **icmp-timeout**—Sets aging time for ICMP protocol translations; default value is 300 seconds (5 minutes)
 - **gre-timeout**—Sets aging time for GRE protocol translations; default value is 300 seconds (5 minutes)
 - **seconds**—Number of seconds before the router removes an unused NAT table entry

Mode Global Configuration

ip nat translation max-entries

Syntax ip nat translation max-entries *maximumEntryNumber*
 no ip nat translation max-entries

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the maximum number of translation entries per virtual router (that is, address bindings, not translation rules) that the translation table can contain in global configuration mode. The **no** version removes the configured limit.

Options ■ *maximumEntryNumber*—Maximum number of translation entries in the current virtual router; default value is no limit

Mode Global Configuration

ip nfs

Syntax ip nfs { source-address *ipAddress*
 | source-interface *interfaceType interfaceSpecifier* }
 no ip nfs { source-address | source-interface }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the E Series interface that the current virtual router uses to exchange NFS communications with an NFS server. The **no** version prevents this interface from sending or receiving NFS communications for the current virtual router.

- Options**
- *ipAddress*—IP address of an E Series interface that sends and receives NFS communications
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Global Configuration

ip nfs host

Syntax `ip nfs host hostName [user userID [group groupID]]`
 `no ip nfs host hostName`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures a remote host as an NFS server for the current virtual router. The **no** version disassociates the NFS server from the virtual router.

- Options**
- *hostName*—Name of the remote host
 - *userID*—User identity in the range 0–4294967295 that a user must enter to connect to the remote host; default value is 2001
 - *groupID*—Group identity in the range 0–4294967295 that the user must enter to connect to the remote host; default value is 100

Mode Global Configuration

ip ospf authentication-key

Syntax ip ospf authentication-key *authKey*
 no ip ospf authentication-key

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns a password used by neighboring routers that are using OSPF simple password authentication. The **no** version deletes the password.

Options ■ *authKey*—Password; string of up to 8 characters

Mode Interface Configuration, Subinterface Configuration

ip ospf authentication message-digest

Syntax [no] ip ospf authentication message-digest

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that the authentication mode for the interface is MD5. The **no** version sets authentication for the interface to none, but leaves any configured MD5 key intact.

Mode Interface Configuration, Subinterface Configuration

ip ospf authentication-none

Syntax ip ospf authentication-none

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that no authentication is to be used for the interface. The **no** version has no effect.

Mode Interface Configuration, Subinterface Configuration

ip ospf bfd-liveness-detection

Syntax ip ospf bfd-liveness-detection [minimum-interval *minInterval* |
 [minimum-receive-interval *minRecInterval*]
 [minimum-transmit-interval *minTransInterval*]] [multiplier *multValue*]
 no ip ospf bfd-liveness-detection

Release Information Command introduced in JUNOS Release 7.1.0.

Description Enables BFD (bidirectional forwarding detection) on an interface running OSPFv2 and defines BFD values to be negotiated between OSPFv2 neighbors for detection of IP data path failures. The **no** version disables BFD on the OSPFv2 interface.



NOTE: BFD sessions might not be maintained when the multiplier value is 1 and configured intervals are very short. We recommend that you do not use a multiplier value of 1 with very short intervals.

- Options**
- *minInterval*—Minimum proposed transmit interval and required receive interval for BFD control packets; has the same effect as configuring the minimum receive interval and the minimum transmit interval to the same value; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *minRecInterval*—Minimum interval at which the local peer must receive BFD control packets sent by the remote peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *minTransInterval*—Minimum proposed interval between BFD control packets sent by the local peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *multValue*—Detection multiplier value that the remote peer router multiplies by the local peer's negotiated transmit interval to determine the remote peer's BFD liveness detection interval; equal to the number of BFD packets that can be missed before the BFD session is declared down; number in the range 1–255; default value is 3

Mode Interface Configuration, Subinterface Configuration

ip ospf cost

Syntax ip ospf cost *intfCost*
 no ip ospf cost

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a cost metric for an interface. Used in the calculation of the SPF routing table. The **no** version resets the path cost to the default.

Options ■ *intfCost*—Link-state metric cost; number in the range 0–65535; default value is 10

Mode Interface Configuration, Subinterface Configuration

ip ospf dead-interval

Syntax ip ospf dead-interval *deadInterval*
 no ip ospf dead-interval

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the time period during which the router's neighbors do not see hello packets before they declare the router to be down. The **no** version resets the dead interval to its default.

Options ■ *deadInterval*—Number in the range 0–2147483647 seconds; default value is 40 seconds

Mode Interface Configuration, Subinterface Configuration

ip ospf hello-interval

Syntax ip ospf hello-interval *helloInterval*
 no ip ospf hello-interval

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the interval between hello packets that the router sends on the interface. The **no** version resets the hello interval to its default.

Options ■ *helloInterval*—Number in the range 1–65535 seconds; default value is 10 seconds

Mode Interface Configuration, Subinterface Configuration

ip ospf message-digest-key md5

Syntax ip ospf message-digest-key *keyID* md5 [0 | 8] *msgDigestKey*
 no ip ospf message-digest-key *keyID*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables OSPF MD5 authentication and configures the MD5 key. The **no** version deletes an MD5 key.



NOTE: If all the MD5 keys have been deleted, the authentication type is still MD5, but you must configure MD5 keys.

To disable MD5 authentication for the interface, use the **ip ospf authentication-none** command.

To display the password only in encrypted text, use the **service password-encryption** command.

- Options**
- *keyID*—Key identifier in the range 1–255
 - md5—Specifies use of the MD5 algorithm
 - 0—Indicates the *msgDigestKey* is entered in unencrypted form (plaintext); this is the default option
 - 8—Indicates the *msgDigestKey* is entered in encrypted form (ciphertext)
 - *msgDigestKey*—OSPF password; string of up to 16 alphanumeric characters

Mode Interface Configuration, Subinterface Configuration

ip ospf network

Syntax ip ospf network { broadcast | non-broadcast | point-to-point }
no ip ospf network

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the OSPF network type to something other than the default for the network medium. The **no** version restores the default value for the medium.

- Options**
- broadcast—Sets the network type to broadcast
 - non-broadcast—Sets the network type to NBMA
 - point-to-point—Sets the network type to point-to-point

Mode Interface Configuration, Subinterface Configuration

ip ospf priority

Syntax ip ospf priority *intfPriority*
 no ip ospf priority

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the router priority. Used in determining the designated router for the particular network. This designation applies only to multiaccess networks. Every broadcast and nonbroadcast multiaccess network has a designated router. The **no** version restores the default value.

Options ■ *intfPriority*—Priority value, an 8-bit number in the range 1–255; default value is 1

Mode Interface Configuration, Subinterface Configuration

ip ospf retransmit-interval

Syntax ip ospf retransmit-interval *retransInterval*
 no ip ospf retransmit-interval

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the time between LSA retransmissions for the interface when an acknowledgment for the LSA is not received. The **no** version restores the default value.

Options ■ *retransInterval*—Number in the range 0–3600 seconds; default value is 5 seconds

Mode Interface Configuration, Subinterface Configuration

ip ospf shutdown

Syntax [no] ip ospf shutdown

Release Information Command introduced before JUNOS Release 7.1.0.

Description Disables OSPF on an interface. The **no** version enables OSPF on the interface.

Mode Interface Configuration, Subinterface Configuration

ip ospf transmit-delay

Syntax ip ospf transmit-delay *transmDelay*
 no ip ospf transmit-delay

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the estimated time it takes to transmit a link-state update packet on the interface. The **no** version restores the default value.

Options ■ *transmDelay*—Link-state transmit delay, a number in the range 0–3600 seconds; default value is 1 second

Mode Interface Configuration, Subinterface Configuration

ip pim

Syntax In Interface Configuration mode:
[no] ip pim [dense-mode | sparse-mode | sparse-dense-mode]

In Profile Configuration mode:
[no] ip pim [sparse-mode | sparse-dense-mode]

Release Information Command introduced before JUNOS Release 7.1.0.
Profile Configuration mode added in JUNOS Release 8.2.0.

Description In Interface Configuration mode, enables PIM on an interface. In Profile Configuration mode, enables a PIM interface for a dynamic profile. The **no** version disables PIM on an interface.

- Options**
- dense-mode—Enables PIM in dense mode
 - sparse-mode—Enables PIM in sparse mode
 - sparse-dense-mode—Enables PIM in sparse-dense mode

Mode Interface Configuration, Profile Configuration

ip pim bfd-liveness-detection

Syntax ip pim bfd-liveness-detection [minimum-interval *minInterval* |
 [minimum-receive-interval *minRecInterval*]
 [minimum-transmit-interval *minTransInterval*]] [multiplier *multValue*]
 no ip pim bfd-liveness-detection

Release Information Command introduced in JUNOS Release 8.0.0.

Description Enables BFD (bidirectional forwarding detection) on an interface running PIM and defines BFD values to be negotiated between PIM neighbors for detection of IP data path failures. The **no** version disables BFD on the PIM interface.



NOTE: BFD sessions might not be maintained when the multiplier value is 1 and configured intervals are very short. We recommend that you do not use a multiplier value of 1 with very short intervals.

- Options**
- *minInterval*—Minimum proposed transmit interval and required receive interval for BFD control packets; has the same effect as configuring the minimum receive interval and the minimum transmit interval to the same value; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *minRecInterval*—Minimum interval at which the local peer must receive BFD control packets sent by the remote peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *minTransInterval*—Minimum proposed interval between BFD control packets sent by the local peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *multValue*—Detection multiplier value that the remote neighbor multiplies by the local router's negotiated transmit interval to determine the remote neighbor's BFD liveness detection interval; equal to the number of BFD packets that can be missed before the BFD session is declared down; number in the range 1–255; default value is 3

Mode Interface Configuration

ip pim bsr-candidate

Syntax `ip pim bsr-candidate interfaceType interfaceSpecifier`
 `[hashMaskLen [priority priority]] [period bootstrapPeriod]`
 `no ip pim bsr-candidate`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a router as a bootstrap router (BSR) candidate. The **no** version disables the router BSR candidacy.

- Options**
- *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see “Interface Types and Specifiers” on page 5. The autoRP announcement messages will contain the IP address for this interface.
 - *hashMaskLen*—Length (up to 32 bits) of the hash mask length field sent in BSMs that the router originates; default value is 30 bits
 - *priority*—Value in the range 0–255 of the BSR-Priority field of BSMs that the router originates; default value is 0
 - *bootstrapPeriod*—Interval in the range 1–65535 seconds at which the BSR sends bootstrap messages; default value is 60 seconds

Mode Global Configuration

ip pim data-mdt

Syntax [no] ip pim data-mdt

Release Information Command introduced in JUNOS Release 8.2.0.

Description Activates data MDTs and enters IP PIM Data MDT Configuration mode. The **no** version deactivates data MDTs.

Mode Global Configuration

ip pim dr-priority

Syntax ip pim dr-priority *priority*
 no ip pim dr-priority

Release Information Command introduced in JUNOS Release 9.0.0.
 Router Configuration mode added in JUNOS Release 10.0.0.

Description Assigns a priority for the interface to be selected as the designated router. An interface with a higher priority value is preferred as a designated router over an interface with a lower priority value. In Interface Configuration mode, the **no** version restores the value that is specified in Router Configuration mode. If the designated router priority is not specified in Router Configuration mode, then the default value of 1 is restored.



NOTE: You cannot configure the designated router priority on PIM dense mode interfaces.

Options ■ *priority*—Value in the range 1–254; default value is 1.

Mode Interface Configuration, Router Configuration

ip pim group-address-pool

Syntax `ip pim group-address-pool poolName groupAddressMinimum groupAddressMaximum`
 `no ip pim group-address-pool poolName`

Release Information Command introduced in JUNOS Release 8.2.0.

Description Configures PIM group address pools from which data MDT group addresses are allocated. The **no** version removes the group address pool.

- Options**
- *poolName*—Name of the group address pool
 - *groupAddressMinimum*—Minimum value in the group address range
 - *groupAddressMaximum*—Maximum value in the group address range

Mode Global Configuration

ip pim join-filter

Syntax ip pim join-filter *accessListName*
 no ip pim join-filter

Release Information Command introduced before JUNOS Release 7.1.0.
 Profile Configuration mode added in JUNOS Release 8.2.0.

Description Specifies an extended access list that you want this PIM interface to use as a join filter. If an interface-level filter exists, it takes precedence over the global-level filter. The **no** version removes the filter association.

Options ■ *accessListName*—Name of the access list that you want this interface to use as a PIM join filter; a string of up to 32 alphanumeric characters

Mode Global Configuration, Interface Configuration, Profile Configuration

ip pim join-prune-interval

Syntax ip pim join-prune-interval *interval*
 no ip pim join-prune-interval

Release Information Command introduced in JUNOS Release 10.0.0.

Description Specifies the time interval at which the router sends the PIM join/prune message to the upstream RPF neighbor. In Interface Configuration mode, the **no** version restores the value that is specified in Router Configuration mode. If the message interval is not specified in Router Configuration mode, then the default value of 60 seconds is restored.



NOTE: You cannot configure the designated router priority on PIM dense mode interfaces.

Options ■ *interval*—Interval in the range 10–210 seconds at which the router sends the PIM join/prune message; the default value is 60 seconds.

Mode Interface Configuration, Router Configuration

ip pim query-interval

Syntax ip pim query-interval *queryTime*
 no ip pim query-interval

Release Information Command introduced before JUNOS Release 7.1.0.
 Profile Configuration mode added in JUNOS Release 8.2.0.

Description Specifies how often the router sends PIM router query messages from this interface. The **no** version specifies the default time interval, 30 seconds.

Options ■ *queryTime*—Interval in the range 0–210 seconds at which the router sends PIM router query messages from this interface

Mode Interface Configuration, Profile Configuration

ip pim rp-address

Syntax [no] ip pim rp-address *ipAddress* [*ipAccessList*] [override]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a static PIM group-to-RP mapping. The **no** version clears the mapping from this interface.

- Options**
- *ipAddress*—IP address of the router you want to designate as an RP router
 - *ipAccessList*—Name of the IP access list that specifies which multicast groups use this RP
 - **override**—Specifies that this static RP mapping has priority over group-to-RP mappings learned by auto-RP

Mode Global Configuration

ip pim rp-candidate

Syntax `ip pim rp-candidate interfaceType interfaceSpecifier [group-list accessListName] [hold-time holdTime] [priority priority] [interval interval]`

`no ip pim rp-candidate interfaceType interfaceSpecifier`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a router as a rendezvous point (RP) router candidate. The **no** version stops the router from being an RP candidate.

- Options**
- *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see “Interface Types and Specifiers” on page 5. The autoRP announcement messages will contain the IP address for this interface.
 - *accessListName*—Access list containing the set of group prefixes supported by this C-RP. If no group-list is specified, the default value is the entire multicast address range.
 - *holdTime*—Amount of time in the range 1–65535 seconds that the BSR keeps an RP in its C-RP list if the BSR does not receive a C-RP advertisement message; default value is 150 seconds
 - *priority*—Priority field value in the range 0–255 that the C-RP sends to the BSR in C-RP advertisement messages. In the RP election process, the RP with the lower priority value is preferred; default value is 192
 - *interval*—Interval in the range 1–65535 seconds at which the C-RP sends advertisement messages to the BSR; default value is 60 seconds

Mode Global Configuration

ip pim send-rp-announce

Syntax ip pim send-rp-announce *interfaceType interfaceSpecifier* scope *ttl*
 [group-list *ipAccessList*] [interval *seconds*]

no ip pim send-rp-announce *interfaceType interfaceSpecifier* [scope *ttl*]
 [group-list *ipAccessList*] [interval *seconds*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sends autoRP announcement messages from a router you configured as an RP. The **no** version clears the specified filters from this interface.

- Options**
- *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see “Interface Types and Specifiers” on page 5. The autoRP announcement messages will contain the IP address for this interface.
 - *ttl*—Time-to-live value; the number of hops for which the announcement is valid in the range 1–65535; default value is 64 hops
 - *ipAccessList*—Name of the IP access list that specifies which multicast groups use this RP; default value is no access list
 - *seconds*—Time interval in the range 1–65535 seconds at which the router sends the announcements; default value is 60 seconds

Mode Global Configuration

ip pim send-rp-discovery scope

Syntax ip pim send-rp-discovery scope *tvl* [*interfaceType interfaceSpecifier*]
 no ip pim send-rp-discovery

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the router as an RP mapping agent, which records RP-to-group mappings and notifies PIM DRs about the mappings. The **no** version stops the router from acting as an RP mapping agent.

- Options**
- *tvl*—Time-to-live value; number of hops for which the RP discovery message is valid. Specify a value that covers the PIM domain.
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see “Interface Types and Specifiers” on page 5. If you specify an interface, the autoRP discovery messages will contain the IP address for this interface.

Mode Global Configuration

ip pim sparse-mode graceful-restart-duration

Syntax ip pim sparse-mode graceful-restart-duration *seconds*
 no ip pim sparse-mode graceful-restart-duration

Release Information Command introduced in JUNOS Release 8.1.0.

Description Sets duration time for IP PIM sparse-mode graceful restart. The **no** version resets the duration to the default.

- Options** ■ sparse-mode—Enables PIM in sparse mode
 ■ *seconds*—Restart duration in seconds; default value is 30 seconds

Mode Global Configuration

ip pim spt-threshold

Syntax [no] ip pim spt-threshold { 0 | *nonzero_integer* | infinity } [group-list *ipAccessList*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the network configuration that PIM sparse mode uses when a source starts sending multicast messages. The **no** version restores the default value, 0.

- Options**
- 0—Configures PIM sparse mode to switch to an SPT when a source begins to send multicast messages
 - *nonzero_integer*—Integer in the range 1–4294967294; prevents PIM sparse mode from switching from a shared tree to an SPT
 - infinity—Prevents PIM sparse mode from switching from a shared tree to an SPT
 - *ipAccessList*—Name of the IP access list that specifies the groups to which the threshold applies

Mode Global Configuration

ip pim ssm

Syntax ip pim ssm [default | range *ipAccessList*]
no ip pim ssm

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables SSM and defines the SSM range of IP multicast addresses. The **no** version disables SSM on the router.

- Options**
- default—Specifies that SSM use the IANA-specified range of 232/8
 - *ipAccessList*—Name of the IP access list that specifies the range of multicast addresses you want SSM to use

Mode Global Configuration

ip policy

Syntax For standard policy lists in Interface Configuration mode:

```
ip policy { input | output | secondary-input } policyName
[ statistics { enabled [ baseline { enabled | disabled } ] [ preserve | merge ] |
disabled [ merge ] } ] | merge ]
```

```
no ip policy { input | output | secondary-input } [ policyName ]
```

For secure policy lists in Interface Configuration mode:

```
ip policy { secure-input | secure-output } policyName
[ statistics { enabled [ baseline baselineValue ] [ preserve ] | disabled } ]
```

```
no ip policy { secure-input | secure-output }
```

For policy lists in Profile Configuration mode:

```
ip policy { input | output | secondary-input } policyName
[ statistics { enabled | disabled } ] [ merge ]
```

```
no ip policy { input | output | secondary-input } [ policyName ]
```

Release Information Command introduced before JUNOS Release 7.1.0.
merge keyword added in JUNOS Release 7.2.0.
 Profile Configuration mode added in JUNOS Release 7.2.0.

Description Assigns a policy list to the ingress or egress of an interface.

For standard policy lists, specify the **input** or **output** keyword to assign the policy list to the ingress or egress of the interface. If you enter the **ip policy** command and the policy list does not exist, the router inserts a default filter rule. Attaching this policy list to an interface filters all packets on that interface.

For secure policy lists, which are used for packet mirroring, use the **secure-input** or **secure-output** keyword to assign the packet mirroring policy list to the ingress or egress side of the interface. If you use the **ip policy** command and the secure policy list does not exist, the router creates a secure policy list with a default mirror rule that disables mirroring. Attaching this policy list to an interface results in no packet mirroring.

In Profile Configuration mode, assigns the policy list to a profile, which then assigns the policy to an interface.

In Interface Configuration mode, the **no** version removes the association between a policy list and an interface. In Profile Configuration mode, the **no** version removes policy reference from the profile.

- Options**
- **input**—Applies policy to data arriving at this interface before a route lookup
 - **output**—Applies policy to data leaving this interface
 - **secondary-input**—Applies policy to data that arrives at this interface after a route lookup
 - **secure-input**—Applies secure policy to data arriving at this interface
 - **secure-output**—Applies secure policy to data leaving this interface



NOTE: The **ip policy** command used with the **secure-input** and **secure-output** keywords provides packet mirroring support. These keywords are available in Interface Configuration mode and do not support the statistics-related keywords. The **ip policy** command used with these keywords replaces the **ip mirror** command, which has been deprecated.

- *policyName*—Name of the policy; a maximum of 40 characters
- **statistics**—Enables or disables collection of policy routing statistics
 - **enabled**—Enables collection of policy routing statistics
 - **baseline enabled**—Enables baselining of policy routing statistics (Interface Configuration mode only)
 - **baseline disabled**—Disables baselining of policy routing statistics (Interface Configuration mode only)
 - **preserve**—Preserves existing statistics for any classifier list that is the same for both the new and old policy attachments when you attach a new policy to an interface
 - **disabled**—Disable collection of policy routing statistics
- **merge**—Enables merging of multiple policies to form a single policy



NOTE: The **local-input** keyword for the **ip policy** command is deprecated, and might be completely removed in a future release. We recommend that you remove the keyword from scripts.

Mode Interface Configuration, Profile Configuration

- Related Topics**
- Setting a Statistics Baseline for Policies
 - Configuring CLI-Based Mirroring

ip policy-list

Syntax [no] ip policy-list *policyName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates or modifies an IP policy list. If you execute an **ip policy-list** command and type **exit**, the router creates a policy list with no rules, the default. When a policy list does not have rules, the router inserts a default filter rule. Attaching this policy list to an interface filters all packets on that interface. The **no** version removes a policy list.

Options ■ *policyName*—Name of the policy list

Mode Global Configuration

Related Topics ■ Creating Policy Lists for IP

ip policy-parameter hierarchical

Syntax ip policy-parameter hierarchical *parameterName* { *nodeValue* | atm | atm-vc | atm-vp
vpValue | ethernet | fr-vc | forwarding |
 ppp-interface | svlan *svlanValue* | vlan }
 no ip policy-parameter *parameterName*

Release Information Command introduced in JUNOS Release 8.0.0.
ppp-interface keyword added in JUNOS Release 10.3.0.

Description Specifies a parameter value for IP interfaces. The **no** version removes the policy parameter and its contents.

- Options**
- *parameterName*—Name of policy parameter
 - *nodeValue*—Aggregation node number in the range 1–65535
 - *vpValue*—ATM VPI number in the range 0–255
 - *svlanValue*—S-VLAN ID number in the range 0–4095

Mode Interface Configuration, Profile Configuration

Related Topics

- Creating a Classifier Group for a Policy List

ip policy-parameter reference-rate

Syntax In Interface Configuration mode:

ip policy parameter reference-rate *parameterName* [increase] *value*

no ip policy-parameter reference-rate *parameterName* [increase *value*]

In Profile Configuration mode:

ip policy parameter reference-rate *parameterName* [increase] *value*

no ip policy-parameter reference-rate *parameterName*

Release Information Command introduced in JUNOS Release 8.1.0.

Description Creates an IP policy parameter for a reference rate; creates a global parameter if it does not exist. The **no** version removes the policy parameter and its contents; if used with the **increase** keyword, decreases the value.

- Options**
- *parameterName*—Name of policy parameter up to 40 characters
 - increase—Increments the existing reference rate value
 - *value*—Value of the reference rate parameter, in the range 0–4292967295

Mode Interface Configuration, Profile Configuration

Related Topics

- Creating a Classifier Group for a Policy List

ip prefix-list

Syntax ip prefix-list *listName* { description *desc* |
[seq *sequence*] { permit | deny } *ipPrefix* [ge *geNumber*] [le *leNumber*] }

no ip prefix-list *listName* [description |
[seq *sequence*] [{ permit | deny } *ipPrefix* [ge *geNumber*] [le *leNumber*]]]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates a prefix list for route filtering; specifies a list entry—a permit or deny clause for a network address. The **no** version removes the specified prefix list or the specified list entry.

- Options**
- *listName*—Name of the prefix list; a string of up to 32 characters
 - *desc*—Description of the prefix list
 - *sequence*—Number in the range 0–65535 that indicates the position the prefix list entry is to have in the list of entries already configured for the prefix list; if *sequence* is not specified, the value of the last sequence number + 5 is used
 - permit—If the prefix of the route being filtered matches the specified prefix and **permit** is specified, the route is redistributed as controlled by the set actions
 - deny—If the prefix of the route being filtered matches the specified prefix and **deny** is specified, the route is not redistributed
 - *ipPrefix*—Network route to be filtered, in the format *network / length*, where
 - *network*—Base address of the network route to be filtered; for example, 192.168.32.0 or 10.10.0.0
 - *length*—Length of the network prefix; number of bits masking base address to produce address to be matched
 - *geNumber*—Route being filtered matches if its prefix is within the range specified: greater than or equal to *geNumber* and less than or equal to 32
 - *leNumber*—Route being filtered matches if its prefix is within the range specified: greater than or equal to *length* and less than or equal to *leNumber*

Mode Global Configuration

ip prefix-tree

Syntax `ip prefix-tree treeName { description desc | { permit | deny } ipPrefix }`
 `no ip prefix-tree treeName [description | { permit | deny } ipPrefix]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates a prefix tree for best-match route filtering; specifies a tree entry—a deny or permit clause for a network address. The **no** version removes the specified prefix tree or the specified tree entry.

- Options**
- *treeName*—Name of the prefix list; a string of up to 32 characters
 - *desc*—Description of the prefix list
 - deny—If the prefix of the route being filtered matches the specified prefix and **deny** is specified, the route is not redistributed
 - permit—If the prefix of the route being filtered matches the specified prefix and **permit** is specified, the route is redistributed as controlled by the set actions
 - *ipPrefix*—Network route to be filtered, in the format *network / length*, where
 - *network*—Base address of the network route to be filtered; for example, 192.168.32.0 or 10.10.0.0
 - *length*—Length of the network prefix; number of bits masking base address to produce address to be matched

Mode Router Configuration

ip profile

Syntax ip profile *profileName*
 no ip profile

Release Information Command introduced in JUNOS Release 7.3.0.

Description Specifies the IP profile that the IPSec layer passes on to the IP layer upon request for upper-layer instantiation. The **no** version removes the association with this profile.

Options ■ *profileName*—Name of the profile that you want the IPSec layer to pass to the IP layer upon request for upper-layer instantiation

Mode IPSec Tunnel Profile Configuration

ip proxy-arp

Syntax ip proxy-arp [restricted | unrestricted]
no ip proxy-arp

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables proxy ARP on an Ethernet or bridge1483 interface. Proxy ARP is enabled by default. The **no** version disables proxy ARP on an Ethernet or bridge1483 interface.

- Options**
- restricted—Restricts proxy-arp to hosts on the local interface
 - unrestricted—Enables proxy-arp for all reachable hosts

Mode Interface Configuration, Subinterface Configuration

ip re-authenticate-auto-detect ip-subscriber

Syntax ip re-authenticate-auto-detect ip-subscriber
 no ip re-authenticate-auto-detect ip-subscriber

Release Information Command introduced in JUNOS Release 10.0.0.

Description Re-authenticates the auto-detected subscribers (dynamic subscriber interfaces) created on static and dynamic IP subscriber interfaces using the DHCP options **dhcp-options**, **dhcp-gi-address**, and **dhcp-mac-address** when the DHCP external application manages the subscriber addresses following a cold boot. The **no** version negates the command or restores the defaults.

Mode Interface Configuration, Profile Configuration

ip redirects

Syntax [no] ip redirects

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the sending of redirect messages if the software is forced to resend a packet through the same interface on which it was received. The **no** version disables the sending of redirect messages.

Mode Interface Configuration, Profile Configuration, Subinterface Configuration

ip refresh-route

Syntax ip refresh-route [vrf *vrfName*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Reinstalls routes removed from the IP routing table by the **clear ip route** command. There is no **no** version.

Options ■ *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters

Mode Privileged Exec

ip rip

Syntax [no] ip rip

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures RIP to run on the network specified by the **network** command. Uses the default values: send version is RIP version 1, receive version is RIP version 1 and version 2, authentication is not enabled. The **no** version deletes the RIP interface.

Mode Interface Configuration, Subinterface Configuration

ip rip authentication key

Syntax ip rip authentication key [0 | 8] *authkey*
no ip rip authentication key

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the password for text authentication and the key for MD5 authentication. The **no** version clears the key for the interface. Supported only in RIP version 2. Authentication is disabled by default.

- Options**
- 0—Indicates the *authKey* is entered in unencrypted form (plaintext); this is the default option
 - 8—Indicates the *authKey* is entered in encrypted form (ciphertext)
 - *authkey*—Password sent with RIP messages or the key used to encrypt/decrypt RIP messages, depending on the authentication mode set for this interface

Mode Interface Configuration, Subinterface Configuration

ip rip authentication mode

Syntax ip rip authentication mode { text | md5 *keyID* }
no ip rip authentication mode

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the type of authentication used on this interface. The **no** version removes authentication from the interface. Supported only in RIP version 2. Authentication is disabled by default.

- Options**
- text—Sends a simple text password with each RIP message; if the password is not possessed by neighbors, the message is rejected
 - md5—Encrypts and compresses the RIP message with MD5 message-digest algorithms
 - *keyID*—Number identifying the MD5 key; neighbors must share the MD5 key to decrypt the message and encrypt the response

Mode Interface Configuration, Subinterface Configuration

ip rip bfd-liveness-detection

Syntax ip rip bfd-liveness-detection [minimum-interval *minInterval* |
 [minimum-receive-interval *minRecInterval*]
 [minimum-transmit-interval *minTransInterval*]] [multiplier *multValue*]

no ip rip bfd-liveness-detection

Release Information Command introduced in JUNOS Release 8.0.0.

Description Enables BFD (bidirectional forwarding detection) on an interface running RIP and defines BFD values to be negotiated between peers for detection of IP data path failures. The **no** version disables BFD on the RIP interface.



NOTE: BFD sessions might not be maintained when the multiplier value is 1 and configured intervals are very short. We recommend that you do not use a multiplier value of 1 with very short intervals.

- Options**
- *minInterval*—Minimum proposed transmit interval and required receive interval for BFD control packets; has the same effect as configuring the minimum receive interval and the minimum transmit interval to the same value; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *minRecInterval*—Minimum interval at which the local peer must receive BFD control packets sent by the remote peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *minTransInterval*—Minimum proposed interval between BFD control packets sent by the local peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *multValue*—Detection multiplier value that the remote peer router multiplies by the local peer's negotiated transmit interval to determine the remote peer's BFD liveness detection interval; equal to the number of BFD packets that can be missed before the BFD session is declared down; number in the range 1–255; default value is 3

Mode Interface Configuration

ip rip copy-to-dynamic

Syntax [no] ip rip copy-to-dynamic

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables RIP on dynamic, unnumbered IP interfaces. You cannot configure RIP on dynamic interfaces directly. However, this command allows dynamic, unnumbered interfaces (that refer to numbered IP interface for configuration data) to obtain RIP attributes from the numbered IP interface to which they refer. The **no** version disables the feature but does not remove all existing, active RIP interfaces that were created by this command.

Mode Interface Configuration

ip rip receive version

Syntax ip rip receive version { 1 | 2 | 1 2 | 2 1 | off }
no ip rip receive version

Release Information Command introduced before JUNOS Release 7.1.0.

Description Restricts the RIP version that the router can receive on an interface. The **no** version sets the interface back to the default value, receiving both RIP version 1 and version 2.

- Options**
- 1—Specifies RIP version 1 only
 - 2—Specifies RIP version 2 only
 - 1 2—Specifies RIP version 1 and version 2
 - 2 1—Specifies RIP version 2 and version 1
 - off—Turns reception off

Mode Interface Configuration, Subinterface Configuration

ip rip send version

Syntax ip rip send version { 1 | 2 | 1 2 | 2 1 | off }
no ip rip send version

Release Information Command introduced before JUNOS Release 7.1.0.

Description Restricts the RIP version that the router can send on an interface. The **no** version sets the interface back to the default value, sending only RIP version 1.

- Options**
- 1—Specifies RIP version 1 only
 - 2—Specifies RIP version 2 only
 - 1 2—Specifies RIP version 1 and version 2
 - 2 1—Specifies RIP version 2 and version 1
 - off—Turns reception off

Mode Interface Configuration, Subinterface Configuration

ip route

Syntax `ip route [vrf vrfName] { ipAddress ipMask { ipNextHop
 [interfaceType interfaceSpecifier] | interfaceType interfaceSpecifier } }
 [distance] [tag tagVal] [permanent] [verify rtr rtrIndex [last-resort]]
 [verify bfd-liveness-detection [minimum-interval minInterval |
 [minimum-receive-interval minRecInterval]
 [minimum-transmit-interval minTransInterval]]] [multiplier multValue]
 [last-resort]]`

`no ip route [vrf vrfName] ipAddress ipMask [ipNextHop | interfaceType
interfaceSpecifier] [distance]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Establishes static routes and can also enable Bidirectional Forwarding Detection (BFD) for the static route. The **no** version removes static routes or removes BFD from the static route.



NOTE: BFD sessions might not be maintained when the multiplier value is 1 and configured intervals are very short. We recommend that you do not use a multiplier value of 1 with very short intervals.

- Options**
- *vrfName*—Name of the VRF if the static route is being established within a VRF context; available only in Global Configuration mode
 - *ipAddress*—Destination IP address
 - *ipMask*—IP mask for the destination
 - *ipNextHop*—IP address of the next hop that can be used to reach the destination network
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *distance*—Administrative distance for this route in the range 0–254
 - *tagVal*—Number in the range 0–4294967295 that identifies the tag for this route
 - *permanent*—Specifies that the route will not be removed, even if the interface shuts down
 - *verify rtr*—Installs the static route in the routing table only if the next hop to the specified destination address is resolved and if the specified RTR operation is currently reachable
 - *rtrIndex*—Number of the RTR operation to be verified; there is no default value

- **last-resort**—Installs the static route in the routing table even if the specified RTR operation is currently unreachable, provided that no other static route to the same network prefix is available
- **verify bfd-liveness-detection**—Installs the static route in the routing table only if the next hop to the specified destination address is verifiable by means of BFD liveness detection
- **minInterval**—Minimum proposed transmit interval and required receive interval for BFD control packets; has the same effect as configuring the minimum receive interval and the minimum transmit interval to the same value; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
- **minRecInterval**—Minimum interval at which the local peer must receive BFD control packets sent by the remote peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
- **minTransInterval**—Minimum proposed interval between BFD control packets sent by the local peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
- **multValue**—Detection multiplier value that the remote peer router multiplies by the local peer's negotiated transmit interval to determine the remote peer's BFD liveness detection interval; equal to the number of BFD packets that can be missed before the BFD session is declared down; number in the range 1–255; default value is 3

Mode Global Configuration, VRF Configuration

ip route-cache flow sampled

Syntax [no] ip route-cache flow sampled

Release Information Command introduced before JUNOS Release 7.1.0.
Profile Configuration mode added in JUNOS Release 7.2.0.

Description Enables J-Flow statistics on an interface. The **no** version disables J-Flow statistics on the interface.

Mode Interface Configuration, Profile Configuration

ip route-map ip-subscriber

Syntax ip route-map ip-subscriber *routeMapName*
 no ip route-map ip-subscriber

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures an interface for route-map processing and specifies the route map that is applied to the IP interface subscriber. If no route map is specified, then all packets will trigger the creation of a dynamic subscriber interface. The **no** version deletes the route map.

Options ■ *routeMapName*—Name of route map

Mode Interface Configuration, Profile Configuration

ip route-type

Syntax For BGP:

```
ip route-type [ unicast | both ]
```

```
no ip route-type
```

For IS-IS, OSPF, and RIP:

```
ip route-type [ unicast | multicast | both ]
```

```
no ip route-type
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies whether BGP, IS-IS, OSPF, or RIP routes are available only for unicast forwarding, only for multicast reverse path forwarding checks, or for both. The **no** version restores the default value, **unicast** for BGP or **both** for IS-IS, OSPF, and RIP.

- Options**
- **unicast**—Specifies that routes for the protocol are available only for unicast forwarding
 - **multicast**—Specifies that routes for the protocol are available only for multicast route path forwarding checks; this option is not available for BGP
 - **both**—Specifies that routes for the protocol are available for both unicast forwarding and multicast route path forwarding checks

Mode Address Family Configuration (RIP), Router Configuration

ip router-id

Syntax [no] ip router-id [*vrfName*] *ipAddress*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Establishes the IP address of a router. The **no** version removes the IP address assignment.

- Options**
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
 - *ipAddress*—IP address of the router

Mode Global Configuration

- Related Topics**
- *Configuring the Loopback Interface and Router ID for BGP for L2VPNs and Configuring the Loopback Interface and Router ID for VPLS in the JUNOS BGP and MPLS Configuration Guide*

ip router isis

Syntax [no] ip router isis [*tag*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures an IS-IS routing process for IP on an interface. The **no** version disables IS-IS for IP on the interface.

Options ■ *tag*—Meaningful name for a routing process. If not specified, a null tag is assumed. The name must be unique among all IP router processes for a given router. Use the same text for the argument tag as specified in the router isis command.

Mode Interface Configuration, Subinterface Configuration

ip-router-name

Syntax [no] ip-router-name [*vrName*]

Release Information Command introduced in JUNOS Release 9.0.0.

Description Assigns an IPv4 virtual router. The **no** version restores the default router.



NOTE: This command replaces the deprecated **router-name** command, which may be removed completely in a future release.

Options ■ *vrName*—Name of the virtual router; string of 1–32 alphanumeric characters

Mode Domain Map Configuration

ip rpf-route

Syntax `ip rpf-route ipAddress addressMask`
`{ nextHopIpAddress | nextHopInterfaceType nextHopInterfaceSpecifier }`
`[distanceValue] [tag tagValue]`

`[no] ip rpf-route ipAddress addressMask`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Customizes static routes that the router can use to verify source addresses in multicast packets. The **no** version removes the static route.

- Options**
- *ipAddress*—IP address of the destination network
 - *addressMask*—Subnet mask for the destination network
 - *nextHopIpAddress*—IP address of the next hop
 - *nextHopInterfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *nextHopInterfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *distanceValue*—Number in the range 0–255 that indicates the preference for this route
 - *tagValue*—Number in the range 0–4294967295 that identifies the route in the routing table

Mode Global Configuration

ip rsvp authentication

Syntax [no] { ip | mpls } rsvp authentication

Description Enables MD5 authentication on the RSVP interface in implementations on routers from other vendors. See the **mpls rsvp authentication** command for a complete description and syntax.

Mode Interface Configuration

ip rsvp authentication key

Syntax { ip | mpls } rsvp authentication [key *authkey*]
no { ip | mpls } rsvp authentication [key [*authkey*]]

Description Assigns a key for MD5 authentication between RSVP peers in implementations on routers from other vendors. See the **mpls rsvp authentication key** command for a complete description and syntax.

Mode Interface Configuration

ip rsvp bandwidth

Syntax { ip rsvp | mpls } bandwidth *bandwidth*
no { ip rsvp | mpls } bandwidth

Description Specifies the total bandwidth *reservable* on the interface in a non-E Series implementation. See the **mpls bandwidth** command for a complete description and syntax.

Mode Interface Configuration

ip rsvp bfd-liveness-detection

Syntax { ip | mpls } rsvp bfd-liveness-detection [minimum-interval *minInterval* |
[minimum-receive-interval *minRecInterval*]
[minimum-transmit-interval *minTransInterval*]] [multiplier *multValue*]

no { ip | mpls } rsvp bfd-liveness-detection

Description Enables BFD (bidirectional forwarding detection) on an interface running RSVP-TE and defines BFD values to be negotiated between RSVP-TE neighbors for detection of IP data path failures. See the **mpls rsvp bfd-liveness-detection** command for a complete description and syntax.

Mode Interface Configuration

ip rsvp signalling hello

Syntax { ip | mpls } rsvp signalling hello
[refresh { interval *helloInterval* | misses *helloMisses* }]

{ no | default } { ip | mpls } rsvp signalling hello

Description Turns on or configures RSVP-TE hello support. See the `mpls rsvp signalling hello` command for a complete description and syntax.

Mode Global Configuration, Interface Configuration, Subinterface Configuration

ip sa-validate

Syntax [no] ip sa-validate

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables source address validation on an interface. This feature verifies that a packet has been sent from a valid source address. When a packet arrives on an interface, the router performs a routing table lookup using the source address. The result from the routing table lookup is an interface to which packets destined for that address are routed. This interface must match the interface that the packet arrived on. If it does not match, the router drops the packet. The **no** version disables source address validation.

Mode Interface Configuration, Profile Configuration

ip sa-validate trap-enable

Syntax [no] ip sa-validate [vrf *vrfName*] trap-enable

Release Information Command introduced in JUNOS Release 7.1.0.

Description Enables the generation of source address validation failure traps. The **no** version disables the generation of source address validation failure traps.

Options ■ *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters

Mode Global Configuration

ip service-profile

Syntax ip service-profile *profileName*
 no ip service-profile

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a service profile used in the route map and enters Service Profile configuration mode. The **no** version deletes the profile.

Options ■ *profileName*—Name of service profile

Mode Global Configuration

ip share-interface

Syntax ip share-interface *interfaceType interfaceSpecifier*
 no ip share-interface

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the layer 2 interface that an IP interface will share in the current virtual router. The **no** version removes the association between the layer 2 interface and the shared IP interface.

- Options** ■ *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Interface Configuration

ip share-nexthop

Syntax ip share-nexthop *ipAddress* [virtual-router *vrName*]
 no ip share-nexthop

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that the shared IP interface dynamically tracks a next hop for the specified destination. The **no** version halts tracking of the next hop.

- Options** ■ *ipAddress*—IP address of the destination for which the next hop is tracked
 ■ *vrName*—Name of the virtual router for the next hop

Mode Interface Configuration

ip shutdown

Syntax [no] ip shutdown

Release Information Command introduced before JUNOS Release 7.1.0.

Description Shuts down an IP interface. The **no** version restarts the interface.

Mode Interface Configuration, Subinterface Configuration

ip source-prefix

Syntax [no] ip source-prefix *ipAddress* *ipAddressMask* deny

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures a subscriber interface or a primary IP interface that is enabled for dynamic creation of subscriber interfaces to demultiplex traffic with the specified IP address and mask. The **no** version removes the association between the interface and the specified IP address and mask.

- Options**
- *ipAddress*—IP address of the physical interface that receives messages for this subscriber
 - *ipAddressMask*—Network mask for associated IP subnet
 - deny—Filters packets matching this command

Mode Interface Configuration, Subinterface Configuration

ip source-route

Syntax [no] ip source-route [vrf *vrfName*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the forwarding of source-routed packets in a VR or VRF. The **no** version disables forwarding. Forwarding is disabled by default in all VRs.

Options ■ *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters

Mode Global Configuration

ip speed

Syntax [no] ip speed *adminSpeed*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the speed of an IP interface in bits per second. The **no** version restores the default value, 0 bps.

Options ■ *adminSpeed*—Speed of the interface in bps in the range 1–4294967295

Mode Interface Configuration, Subinterface Configuration

ip split-horizon

Syntax [no] ip split-horizon

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables split horizon, preventing the RIP router from advertising routes from the interface originating the route, reducing the possibility of routing loops; this is the default condition. The **no** version disables split horizon.

Mode Interface Configuration, Subinterface Configuration

ip ssh authentication-retries

Syntax ip ssh authentication-retries *retryLimit*
 no ip ssh authentication-retries

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the number of times that a user can retry a failed authentication (such as trying to correct a wrong password) before the server terminates the connection. The **no** version restores the default value, 20 retries.

Options ■ *retryLimit*—Number of times authentication can be retried after the initial failure within a given connection attempt

Mode Global Configuration

ip ssh crypto

Syntax ip ssh crypto [client-to-server | server-to-client] [no | default] *cipherAlgorithm*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Adds an encryption algorithm to the specified list of supported algorithms. The **no** version removes or excludes an algorithm from the specified list. The **default** version restores the default algorithms for the specified list.

- Options**
- client-to-server—Adds the specified algorithm to the SSH server's list of supported inbound algorithms
 - server-to-client—Adds the specified algorithm to the SSH server's list of supported outbound algorithms
 - no—Removes or excludes the specified algorithm from the list
 - default—Restores the specified list to the factory defaults, which includes 3des-cbc, twofish-cbc, and blowfish-cbc
 - *cipherAlgorithm*—Algorithm to add to the list

Mode Global Configuration

ip ssh disable-user-authentication

Syntax [no] ip ssh disable-user-authentication

Release Information Command introduced before JUNOS Release 7.1.0.

Description Disables RADIUS password authentication, resulting in the acceptance of all SSH clients that pass protocol negotiation. The **no** version restores RADIUS authentication.

Mode Global Configuration

ip ssh mac

Syntax ip ssh mac [client-to-server | server-to-client] [no | default] *macAlgorithm*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Adds a MAC algorithm to the specified list of supported algorithms. The **no** version removes or excludes an algorithm from the specified list. The **default** version restores the default algorithms for the specified list.

- Options**
- client-to-server—Adds the specified algorithm to the SSH server's list of supported inbound algorithms
 - server-to-client—Adds the specified algorithm to the SSH server's list of supported outbound algorithms
 - no—Removes or excludes the specified algorithm from the list
 - default—Restores the specified list to the factory defaults, which includes hmac-md5, hmac-sha1, and hmac-sha1-96
 - *macAlgorithm*—Algorithm to add to the list

Mode Global Configuration

ip ssh sleep

Syntax `ip ssh sleep sleepPeriod`
`no ip ssh sleep`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a sleep period in seconds for users that have exceeded the authentication retry limit. Connection attempts from the user at the same host are denied until this period expires. The **no** version restores the default value, 600 seconds.

Options ■ *sleepPeriod*—Period in the range 0–4294967295 seconds

Mode Global Configuration

ip ssh timeout

Syntax ip ssh timeout *timeout*
 no ip ssh timeout

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a timeout period in seconds. The SSH server terminates the connection if protocol negotiation—including user authentication—is not complete within this timeout. The **no** version restores the default value, 600 seconds.

Options ■ *timeout*—Period in the range 10–600 seconds

Mode Global Configuration

ip ssh user-authentication-protocol

Syntax ip ssh user-authentication-protocol *protocol*
 no ip ssh user-authentication-protocol

Release Information Command introduced in JUNOS Release 10.2.0.

Description Configures the SSH user authentication protocol. E Series routers support RADIUS and TACACS+ user authentication protocols. The **no** version restores the SSH user authentication protocol to the default, RADIUS.

Options ■ *protocol*—User authentication protocol: either RADIUS or TACACS+.

Mode Global Configuration

ip static-route table-map

Syntax ip static-route table-map [vrf *vrfName*] *mapName*
 no ip static-route table-map [vrf *vrfName*] [*mapName*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Filters static routes before adding them to the routing table. The **no** version deletes the table map.

- Options** ■ *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
 ■ *mapName*—Name of the table map that you want the router to use

Mode Global Configuration

ip summary-address

Syntax `ip summary-address [rip] ipAddress ipAddressMask [metric]`
 `no ip summary-address [rip] ipAddress ipAddressMask`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Summarizes specified addresses for RIP. The **no** version removes the summarization.

- Options**
- `rip`—Specifies optional keyword for compatibility with non-E Series implementations
 - `ipAddress`—IP address identifying the route to be summarized
 - `ipAddressMask`—Network mask identifying the route to be summarized
 - `metric`—Specifies a metric for the summary address; default value is 1

Mode Address Family Configuration, Router Configuration

ip tcp ack-rst-and-syn

Syntax [no] [ip] tcp ack-rst-and-syn [vrf *vrfName*]

Description The **ip** keyword for **tcp** commands is now optional (with the exception of the **ip tcp adjust-mss** command, which is IPv4 specific). For information about this command and any other **ip tcp** command, see the **tcp** commands.

Mode Global Configuration

ip tcp adjust-mss

Syntax [ip] tcp adjust-mss *mssAdjustment*
 no [ip] tcp adjust-mss

Release Information Command introduced before JUNOS Release 7.1.0.

Description Modifies the maximum segment size (MSS) for TCP SYN packets traveling through the interface. The router compares the MSS value of incoming or outgoing packets against the MSS adjustment value. For any packet that contains an MSS value larger than the MSS adjustment value, the router replaces the MSS option with the configured adjustment value. If the packet does not contain an MSS value, the router assumes a value of 536 for the packet MSS on which to base the comparison. The **no** version removes the MSS modification.



NOTE: The purpose behind using MSS is to alleviate problems with Path MTU Discovery (PMTUD) and resulting “black hole” detection issues. See RFC 2923—TCP Problems with Path MTU Discovery (September 2000) for additional information about the black hole scenario.

- Options**
- ip—Specifies optional keyword for use with older scripts
 - *mssAdjustment*—Adjustment value for the MSS; in the range 160–10240

Mode Interface Configuration, Profile Configuration

ip ttl

Syntax `ip ttl [vrfName] ttlValue`
`no ip ttl [vrfName]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the hop count specified by the TTL field in the IP header used by IP for all operations unless overridden by another command. The **no** version restores the default value, 127.

- Options** ■ *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
 ■ *ttlValue*—Number in the range 1–255

Mode Global Configuration

ip tunnel reassembly

Syntax [no] ip tunnel reassembly

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the reassembly of fragmented IP tunnel packets that are received on the current virtual router. The **no** version restores the default disabled condition.

Mode Global Configuration

ip unnumbered

Syntax [no] ip unnumbered *interfaceType interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables IP processing on an interface without assigning an explicit IP address to the interface. The **no** version disables IP processing on the interface.

Options

- *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Interface Configuration, Profile Configuration, Subinterface Configuration

ip unreachable

Syntax [no] ip unreachable

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the generation of an ICMP unreachable message when a packet is received that cannot be delivered by the router. The **no** version disables this function.

Mode Interface Configuration, Subinterface Configuration

ip use-framed-routes ip-subscriber

Syntax [no] ip use-framed-routes ip-subscriber

Release Information Command introduced in JUNOS Release 8.1.0.

Description Configures the router to enable a static primary IP interface to use the RADIUS Framed-Route attribute [22]. The primary IP interface applies the framed routes as source IP addresses when creating and configuring dynamic subscriber interfaces. The **no** version disables the primary IP interface support of the Framed-Route RADIUS attribute.

Mode Interface Configuration

ip virtual-router

Syntax [no] ip virtual-router *vrName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a virtual router in an IP profile. Dynamic interfaces created with the profile are assigned to this VR. The **no** version removes the VR from the profile; if a VR is not specified via RADIUS, then any subsequent creation process for dynamic interfaces using the profile fails.

Options ■ *vrName*—Name of the virtual router; a string of 1–15 alphanumeric characters

Mode Profile Configuration

ip vrf

Syntax `ip vrf vrfName`
 `no ip vrf vrfName [wait-for-completion [waitSeconds]]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates a VRF or accesses VRF Configuration mode to configure a VRF. The **no** version deletes the VRF.



NOTE: After creating the VRF, you must configure a route distinguisher for it via the **rd** command; otherwise, the VRF will not operate.

- Options**
- *vrfName*—Name of the VRF; a string of 1–32 alphanumeric characters
 - *wait-for-completion*—Specifies (in the absence of *waitSeconds*) that the CLI waits for completion of the **no** version operation before it returns a prompt, regardless of how long that takes
 - *waitSeconds*—Number of seconds in the range 1–64000 that the CLI waits before it returns a prompt, regardless of whether the **no** version operation has completed

Mode Global Configuration

ip vrf forwarding

Syntax [no] ip vrf forwarding *vrfName* [fallback global]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns a VRF to an interface or subinterface. Optionally specifies secondary routing table lookup on the parent (global) virtual router forwarding table if a lookup on the initial VRF forwarding table does not yield any results. The **no** version removes the assignment or discontinues the secondary routing table lookup option.



NOTE: The **ip vrf forwarding** command changes the prompt to indicate that the CLI is now in Interface or Subinterface Configuration mode within the child VRF. This condition persists only for as long as you are configuring attributes on the given interface within the VRF. Entering a top-level command, such as **interface**, within this VRF context takes the CLI out of the VRF context back to the parent VR context.

When you issue the **ip vrf forwarding** command from within the Interface Configuration or Subinterface Configuration mode of the parent VR, the IP address and other attributes of the interface are deleted from the interface. You must then reconfigure the IP attributes in the context of the VRF after issuing the command.

-
- Options**
- *vrfName*—Name of the VRF; a string of 1–32 alphanumeric characters
 - fallback global—Specifies secondary routing table lookup on the parent (global) virtual router forwarding table, if an initial VRF forwarding table lookup does not yield results.

Mode Interface Configuration, Subinterface Configuration

ip vrrp

Syntax [no] ip vrrp *vrid*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates a VRRP instance ID. The **no** version removes a VRID. The default is disabled.

Options ■ *vrid*—VRID identifier; a number in the range 1–255

Mode Interface Configuration

ip vrrp accept-data

Syntax [no] ip vrrp *vrid* accept-data

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the backup router to process packets with an IP destination address equivalent to the virtual addresses while the backup router is in the master state. The **no** version restores the default value, disabled.



NOTE: When using this attribute and also restricting incoming packets to ICMP only, you must use policy filters to accept only ICMP packets with the virtual address as the destination address.

Options ■ *vrid*—VRID identifier; a number in the range 1–255

Mode Interface Configuration

ip vrrp advertise-interval

Syntax ip vrrp *vrid* advertise-interval *advertiseInterval* [seconds | milliseconds]
 no ip vrrp *vrid* advertise-interval

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the VRRP advertisement interval time. You must use seconds to comply with RFC 2338. Use milliseconds only if all VRRP instances peering for the given VRID are composed of E Series routers. The **no** version restores the default value, 1 second.

- Options**
- *vrid*—VRID identifier; a number in the range 1–255
 - *advertiseInterval*—Advertisement period in seconds or milliseconds; in the range 1–255 seconds or 100–255000 milliseconds
 - seconds—Specifies interval in seconds
 - milliseconds—Specifies interval in milliseconds

Mode Interface Configuration

ip vrrp authentication-key

Syntax ip vrrp *vrid* authentication-key *key*
 no ip vrrp *vrid* authentication-key

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the authentication key. This command is only valid if the **text** keyword was selected in the **ip vrrp authentication-type** command. The **no** version negates the command or restores the default.

Options ■ *vrid*—VRID identifier; a number in the range 1–255
 ■ *key*—String of 1–8 characters

Mode Interface Configuration

ip vrrp authentication-type

Syntax ip vrrp *vrid* authentication-type { none | text }
 no ip vrrp *vrid* authentication-type

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the VRRP authentication type. The **no** version restores the default value, none.

- Options**
- *vrid*—VRID identifier; a number in the range 1–255
 - none—Disables authentication
 - text—Specifies simple text password

Mode Interface Configuration

ip vrrp enable

Syntax [no] ip vrrp *vrid* [enable]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables a VRID. The **no** version disables a VRID. The default is disabled.

Options ■ *vrid*—VRID identifier; a number in the range 1–255

Mode Interface Configuration

ip vrrp icr-partition

Syntax [no] ip vrrp *vrid* icr-partition *partitionId*

Release Information Command introduced in JUNOS Release 10.3.0.

Description Creates an ICR partition that corresponds to the VRRP instance. The state of the ICR partition depends on the state of the VRRP instance. If the VRRP instance is disabled, the ICR partition is in the dormant state. If the VRRP instance is enabled, the ICR partition follows the state of the VRRP instance. The **no** version deletes the partition from the router.

- Options**
- *vrid*—VRID identifier; a number in the range 1–255
 - *partitionId*—Name that identifies the ICR partition; a string of up to 128 alphanumeric characters



NOTE: Use the ICR-Partition-Id VSA to determine the ICR partition on which subscribers are logged in. You can configure the same ICR-Partition-Id string for an active ICR partition and its corresponding backup partition. For more information on ICR-PARTITION-ID VSA, see Interaction with RADIUS for ICR.

Mode Interface Configuration, Subinterface Configuration

- Related Topics**
- Naming ICR Partitions
 - Configuring an ICR Partition

ip vrrp icr-partition group

Syntax `ip vrrp vrid icr-partition group partitionGroupingType`

Release Information Command introduced in JUNOS Release 10.3.0.

Description Configures the ICR partition to use either S-VLAN-based grouping or VLAN-based grouping for subscribers. If you specify VLAN as the grouping type or partition type, the ICR partition consists of single-tagged VLAN-based subinterfaces. By default, the ICR partition uses S-VLAN-based grouping. There is no **no** version.

- Options**
- *vrid*—VRID identifier; a number in the range 1–255
 - *partitionGroupingType*—One of the following partition types:
 - *svlan*—Configures the ICR partition to use double-tagged S-VLAN based subinterfaces.
 - *vlan*—Configures the ICR partition to use single-tagged VLAN based subinterfaces.

Mode Interface Configuration, Subinterface Configuration

- Related Topics**
- Grouping ICR Subscribers Based on S-VLAN IDs
 - Grouping ICR Subscribers Based on VLAN IDs
 - Configuring an ICR Partition

ip vrrp icr-partition svlan-list

Syntax ip vrrp *vrid* icr-partition svlan-list [*svlanIdValue*] *
 [use-default-mac] [control-interface] [advertise-mac]

no ip vrrp *vrid* icr-partition svlan-list [*svlanIdValue*] *

Release Information Command introduced in JUNOS Release 10.3.0.

Description Adds an S-VLAN to the ICR partition. You can assign only unique S-VLANs to the partition. If you attempt to assign a previously assigned S-VLAN to the ICR partition, the router displays an error message. You can assign S-VLANs only if you have selected S-VLAN based grouping by using the **ip vrrp icr-partition group** command. The **no** version deletes the S-VLAN from the ICR partition.



NOTE: You can use the listed optional parameters only when you add a S-VLAN to the ICR partition. You cannot modify an existing subinterface using these parameters. You can specify the optional parameters in any order.

- Options**
- *vrid*—VRID identifier; a number in the range 1–255
 - *svlanIdValue*—S-VLAN identifier; a number in the range 0–4095
 - **use-default-mac**—Configures the S-VLAN to use the default MAC address. By default, the router assigns the VRRP media access control (MAC) address to all subinterfaces of the ICR partition.
 - **control-interface**—Controls traffic on a subinterface that is part of a backup partition. When you use this option, the router changes the state of the corresponding subinterface to Admindown. When the subinterface is in Admindown state, the router blocks all traffic to the interface. However, the router does not block advertisements as long as VRRP is running on a separate subinterface. The router changes the state of the subinterface from Admindown to Up when the state of the partition changes from backup to master.
 - **advertise-mac**—Enables the subinterface to transmit GARP advertisements when the partition moves from backup state to master state. By default, GARP advertisements are blocked on a subinterface.

Mode Interface Configuration, Subinterface Configuration

- Related Topics**
- Grouping ICR Subscribers Based on S-VLAN IDs
 - Configuring an ICR Partition

ip vrrp icr-partition svlan-list explicit

Syntax `ip vrrp vrid icr-partition svlan-list-explicit [svlanIdValue vlanIdValue] *`
`[use-default-mac] [control-interface] [advertise-mac]`

`no ip vrrp vrid icr-partition svlan-list-explicit [svlanIdValue vlanIdValue] *`

Release Information Command introduced in JUNOS Release 10.3.0.

Description Adds an S-VLAN range and VLAN range to the ICR partition. You can assign only unique S-VLAN range and VLAN range to the partition. If you attempt to assign a previously assigned S-VLAN range and VLAN range to the ICR partition, the router displays an error message. You can assign S-VLAN range and VLAN range only if you have selected S-VLAN based grouping by using the **ip vrrp icr-partition group** command. The **no** version deletes the S-VLAN range and VLAN range from the ICR partition.



NOTE: You can use the listed optional parameters only when you add a S-VLAN, VLAN pair to the ICR partition. You cannot modify an existing subinterface using these parameters. You can specify the optional parameters in any order.

- Options**
- **vrid**—VRID identifier; a number in the range 1–255
 - **svlanIdValue**—S-VLAN identifier; a number in the range 0–4095
 - **vlanIdValue**—VLAN identifier; a number in the range 0–4095
 - **use-default-mac**—Configures the S-VLAN range and VLAN range to use the default MAC address. By default, the router assigns the VRRP media access control (MAC) address to all subinterfaces of the ICR partition.
 - **control-interface**—Controls traffic on a subinterface that is part of a backup partition. When you use this option, the router changes the state of the corresponding subinterface to Admindown. When the subinterface is in Admindown state, the router blocks all traffic to the interface. However, the router does not block advertisements as long as VRRP is running on a separate subinterface. The router changes the state of the subinterface from Admindown to Up when the state of the partition changes from backup to master.
 - **advertise-mac**—Enables the subinterface to transmit GARP advertisements when the partition moves from backup state to master state. By default, GARP advertisements are blocked on a subinterface.

Mode Interface Configuration, Subinterface Configuration

- Related Topics**
- Grouping ICR Subscribers Based on S-VLAN IDs
 - Configuring an ICR Partition

ip vrrp icr-partition svlan-range

Syntax ip vrrp *vrid* icr-partition svlan-range [*svlanIdStart svlanIdEnd*]
 [use-default-mac] [control-interface] [advertise-mac]

no ip vrrp *vrid* icr-partition svlan-range [*svlanIdStart svlanIdEnd*]

Release Information Command introduced in JUNOS Release 10.3.0.

Description Adds a range of S-VLANs to the ICR partition. You can only assign unique S-VLANs to the partition. If you attempt to assign a previously assigned S-VLAN range to the ICR partition, the router displays an error message. You can assign S-VLANs only if you have selected S-VLAN based grouping by using the **ip vrrp icr-partition group** command. The **no** version deletes the S-VLAN range from the ICR partition.



NOTE: You can use the listed optional parameters only when you add a S-VLAN or a range of S-VLANs to the ICR partition. You cannot modify an existing subinterface using these parameters. You can specify the optional parameters in any order.

- Options**
- *vrid*—VRID identifier; a number in the range 1–255
 - *svlanIdStart*—Starting S-VLAN ID of the S-VLAN subrange you are configuring; a number in the range 0–4095
 - *svlanIdEnd*—Ending S-VLAN ID of the S-VLAN subrange you are configuring; a number in the range 0–4095
 - **use-default-mac**—Configures the S-VLAN range to use the default MAC address. By default, the router assigns the VRRP MAC address to all subinterfaces of the ICR partition.
 - **control-interface**—Controls traffic on a range of subinterfaces that are part of a backup partition. When you use this option, the router changes the state of the corresponding range of subinterfaces to Admindown. When the subinterfaces are in Admindown state, the router blocks all traffic to the interfaces. However, the router does not block advertisements as long as VRRP is running on a separate subinterface. The router changes the state of the range of subinterfaces from Admindown to Up when the state of the partition changes from backup to master.
 - **advertise-mac**—Enables subinterfaces to transmit GARP advertisements when the partition moves from backup state to master state. By default, GARP advertisements are blocked on subinterfaces.

Mode Interface Configuration, Subinterface Configuration

- Related Topics**
- Grouping ICR Subscribers Based on S-VLAN IDs
 - Configuring an ICR Partition

ip vrrp icr-partition vlan-list

Syntax `ip vrrp vrid icr-partition vlan-list [vlanIdValue] *`
 `[use-default-mac] [control-interface] [advertise-mac]`
 `no ip vrrp vrid icr-partition vlan-list [vlanIdValue] *`

Release Information Command introduced in JUNOS Release 10.3.0.

Description Adds a VLAN to the ICR partition. You can assign only unique VLANs to the partition. If you attempt to assign a previously assigned VLAN to the ICR partition, the router displays an error message. You can assign VLANs only if you have selected VLAN based grouping by using the **ip vrrp icr-partition group** command. The **no** version deletes the VLAN from the ICR partition.



NOTE: You can use the listed optional parameters only when you add a VLAN to the ICR partition. You cannot modify an existing subinterface using these parameters. You can specify the optional parameters in any order.

- Options**
- *vrid*—VRID identifier; a number in the range 1–255
 - *vlanIdValue*—VLAN identifier; a number in the range 0–4095
 - **use-default-mac**—Configures the VLAN to use the default MAC address. By default, the router assigns the VRRP media access control (MAC) address to all subinterfaces of the ICR partition.
 - **control-interface**—Controls traffic on a subinterface that is part of a backup partition. When you use this option, the router changes the state of the corresponding subinterface to Admindown. When the subinterface is in Admindown state, the router blocks all traffic to the interface. However, the router does not block advertisements as long as VRRP is running on a separate subinterface. The router changes the state of the subinterface from Admindown to Up when the state of the partition changes from backup to master.
 - **advertise-mac**—Enables the subinterface to transmit GARP advertisements when the partition moves from backup state to master state. By default, GARP advertisements are blocked on subinterfaces.

Mode Interface Configuration, Subinterface Configuration

- Related Topics**
- Grouping ICR Subscribers Based on VLAN IDs
 - Configuring an ICR Partition

ip vrrp icr-partition vlan-range

Syntax ip vrrp *vrid* icr-partition vlan-range [*vlanIdStart* *vlanIdEnd*]
 [use-default-mac] [control-interface] [advertise-mac]

no ip vrrp *vrid* icr-partition vlan-range [*vlanIdStart* *vlanIdEnd*]

Release Information Command introduced in JUNOS Release 10.3.0.

Description Adds a range of VLANs to the ICR partition. You can assign only unique VLANs to the partition. If you attempt to assign a previously assigned VLAN range to the ICR partition, the router displays an error message. You can assign VLANs only if you have selected VLAN based grouping by using the **ip vrrp icr-partition group** command. The **no** version deletes the VLAN range from the ICR partition.



NOTE: You can use the listed optional parameters only when you add a VLAN or a range of VLANs to the ICR partition. You cannot modify an existing subinterface using these parameters. You can specify the optional parameters in any order.

- Options**
- *vrid*—VRID identifier; a number in the range 1–255
 - *vlanIdStart*—Starting VLAN ID of the VLAN subrange you are configuring; a number in the range 0–4095
 - *vlanIdEnd*—Ending VLAN ID of the VLAN subrange you are configuring; a number in the range 0–4095
 - **use-default-mac**—Configures the VLAN range to use the default MAC address. By default, the router assigns the VRRP MAC address to all subinterfaces of the ICR partition.
 - **control-interface**—Controls traffic on a range of subinterfaces that are part of a backup partition. When you use this option, the router changes the state of the corresponding range of subinterfaces to Admindown. When the subinterfaces are in Admindown state, the router blocks all traffic to the interfaces. However, the router does not block advertisements as long as VRRP is running on a separate subinterface. The router changes the state of the range of subinterfaces from Admindown to Up when the state of the partition changes from backup partition to master.
 - **advertise-mac**—Enables subinterfaces to transmit GARP advertisements when the partition moves from backup state to master state. By default, GARP advertisements are blocked on subinterfaces.

Mode Interface Configuration, Subinterface Configuration

Related Topics ■ Grouping ICR Subscribers Based on VLAN IDs

- Configuring an ICR Partition

ip vrrp preempt

Syntax [no] ip vrrp *vrid* preempt

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables VRRP preemption. The **no** version disables VRRP preemption. The default is enabled.

Options ■ *vrid*—VRID identifier; a number in the range 1–255

Mode Interface Configuration

ip vrrp priority

Syntax `ip vrrp vrid priority priorityValue`
 `no ip vrrp vrid priority`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the priority of VRRP routers. The **no** version restores the default value, 100.



NOTE: If you configure VRRP on a virtual router and associate the IP address with the VRRP instance ID (VRID) so that the virtual address becomes the interface address of the router, the priority of the router automatically changes to 255 making it the master router. This change of priority occurs in JUNOS Software Releases 11.0.0 and higher-numbered releases and later to enable full compliance with RFC-Virtual Router Redundancy Protocol (VRRP) (April 2004).

Also, you cannot configure the priority of the VRRP router as 255 by using the **ip vrrp priority** command, unless you configured the router to automatically learn associated addresses by using the **auto** keyword with the **ip vrrp virtual-address** command. In addition, if you change the virtual address of the VRRP router, which is operating as the IP address owner, to an IP address that is no longer the IP address owner, the priority changes automatically to the default value of 100.

Options ■ *vrid*—VRID identifier; a number in the range 1–255
 ■ *priorityValue*—Priority value of the VRRP router; a number in the range 1–255; default value is 100

Mode Interface Configuration

ip vrrp timers-learn

Syntax [no] ip vrrp *vrid* timers-learn

Release Information Command introduced in JUNOS Release 10.3.0.

Description Configures the VRRP instance to learn the VRRP advertisement interval from the master VRRP instance. This feature is useful only when you have configured different advertisement intervals for the master VRRP instance and the backup VRRP instance. This feature enables the unified ISSU operation to proceed successfully. The **no** version disables the learning timer for the VRRP instance. If you have configured different advertisement intervals for the VRRP master and VRRP backup instances, the VRRP session breaks, and both instances behave like the master instance, and the router displays an error message.

Options ■ *vrid*—VRID identifier; a number in the range 1–255

Mode Interface Configuration, Subinterface Configuration

Related Topics ■

ip vrrp track

Syntax `ip vrrp vrid track objectName [decrement priorityValue]`
 `no ip vrrp vrid track objectName`

Release Information Command introduced in JUNOS Release 7.2.0.

Description Tracks a specified object and changes the priority of that object when the state of the object changes from an up state to a down state. The priority is decremented by the specified value or by the default value (100; when no decrement value is specified). The object priority is restored when the state of the object changes from a down state to an up state. The **no** version disables any tracking for the object.

- Options**
- *vrid*—VRID identifier; a number in the range 1–255
 - *objectName*—Name of the object to track
 - *priorityValue*—Priority value of the VRRP router; a number in the range 1–255; default value is 100

Mode Interface Configuration

ip vrrp virtual-address

Syntax `ip vrrp vrid virtual-address { auto | ipAddress ipAddress [ipAddress ipAddress]* }`
 `no ip vrrp vrid virtual-address [ipAddress ipAddress]*`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Associates an IP address with a VRID. The **no** version removes a list of IP addresses associated with a VRID. The **no** version clears the auto flag, if auto addresses are being used. There is no default.

- Options**
- *vrid*—VRID identifier; a number in the range 1–255
 - *ipAddress*—IP address
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Interface Configuration

ipsec ca authenticate

Syntax ipsec ca authenticate *caName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Obtains the specified CA's public key (a self-signed certificate) during online digital certificate configuration. The CA must be previously declared by the **ipsec ca identity** command. There is no **no** version; however, to remove the CA certificate, issue the **no ipsec ca identity** command for the specified CA or boot the router using the factory defaults.

Options ■ *caName*—Name of CA

Mode Global Configuration

ipsec ca enroll

Syntax ipsec ca enroll *caName* [*password*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Generates a certificate request to the specified CA and retrieves the public key certificate for the router during online digital certificate configuration. The CA must be previously declared by the **ipsec ca identity** command. There is no **no** version.

- Options** ■ *caName*—Name of CA
- *password* —Challenge password to access the CA and enable enrollment

Mode Global Configuration

ipsec ca identity

Syntax [no] ipsec ca identity *name*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the certificate authority (CA) that the router uses for certificate requests and enters IPsec Identity Configuration mode during online digital certificate configuration. The **no** version deletes the identity information and the certificates associated with the specified CA.

Options ■ *name*—Name of CA

Mode Global Configuration

ipsec certificate-database refresh

Syntax ipsec certificate-database refresh

Release Information Command introduced before JUNOS Release 7.1.0.

Description Informs the E Series router that a public key certificate has been copied to the router. There is no **no** version.

Mode Global Configuration

ipsec certificate-request generate

Syntax ipsec certificate-request generate rsa *fileName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Generates a certificate request. There is no **no** version.

- Options**
- **rsa**—Specifies that the certificate request is issued for the RSA public key
 - ***fileName***—Name of the certificate request file generated on the E Series router; the filename must include a .crq extension

Mode Global Configuration

ipsec clear sa

Syntax ipsec clear sa { all [state *tunnelState*] | tunnel *tunnelName* } [phase { 1 | 2 }]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Refreshes ISAKMP/IKE or IPSec SAs. There is no **no** version.

- Options**
- all—Reinitializes all SAs
 - state—Reinitializes SAs on tunnels that are in a specific state
 - *tunnelState*—State of tunnel, up, down, not-present
 - tunnel—Specifies that an SA on a specific tunnel is to be reinitialized
 - *tunnelName*—Name of tunnel
 - phase—Specifies one of the following types of tunnel to be reinitialized:
 - 1—ISAKMP/IKE tunnels
 - 2—IPSec tunnels

Mode Global Configuration

ipsec crl

Syntax ipsec crl { ignored | optional | required }
no ipsec crl

Release Information Command introduced before JUNOS Release 7.1.0.

Description Controls how the router checks certificate revocation lists (CRLs) when determining whether to accept a peer's certificates. The **no** version restores the default setting.



NOTE: This command is replacing the **ike crl** command. The **ike crl** command may be removed completely in a future release.

- Options**
- ignored—Specifies that the router will not try to find or use CRLs
 - optional—Specifies that the router will try to find a CRL. If a CRL is found, the peer certificate must not appear in the CRL. If no CRL is found, the peer can still authenticate; this is the default.
 - required—Specifies that the router must find a valid CRL; the CRL must be current, and the peer certificate must not appear in the CRL

Mode Global Configuration

ipsec identity

Syntax [no] ipsec identity

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the identity that the router uses in certificate requests and during negotiations with its peers. The **no** version removes the identity configuration.

Mode Global Configuration

ipsec ike-policy-rule

Syntax ipsec ike-policy-rule *priority*
 no ipsec ike-policy-rule [*priority*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines and prioritizes an ISAKMP/IKE policy. ISAKMP/IKE policies define parameters to be used during ISAKMP/IKE negotiation. You can have up to 10 ISAKMP/IKE policies per router. The **no** version removes a policy. If you do not include a priority number with the **no** version, the software removes all ISAKMP/IKE policies.



NOTE: This command is replacing the **ipsec isakmp-policy-rule** command. The **ipsec isakmp-policy-rule** command may be removed completely in a future release.

Options ■ *priority*—Identifies and prioritizes the ISAKMP/IKE policy; in the range 1 to 10000, with 1 having the highest priority

Mode Global Configuration

ipsec isakmp-policy-rule

Syntax ipsec isakmp-policy-rule *priority*
 no ipsec isakmp-policy-rule [*priority*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines and prioritizes an ISAKMP/IKE policy. ISAKMP/IKE policies define parameters to be used during ISAKMP/IKE negotiation. You can have up to 10 ISAKMP/IKE policies per router. The **no** version removes a policy. If you do not include a priority number with the **no** version, the software removes all ISAKMP/IKE policies.



NOTE: This command has been replaced by the **ipsec ike-policy-rule** command and may be removed completely in a future release.

Options ■ *priority*—Identifies and prioritizes the ISAKMP/IKE policy; in the range 1–10000, with 1 having the highest priority

Mode Global Configuration

ipsec key generate

Syntax ipsec key generate rsa { 1024 | 2048 }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Generates RSA key pairs. Specify the length of the key in bits, either 1024 or 2048. There is no **no** version. To remove a key pair, use the **ipsec key zeroize** command.

Mode Global Configuration

ipsec key manual pre-share

Syntax [no] ipsec key manual pre-share { *ipAddress* | ip address *ipAddress* | identity *fqdn* | local-ip-address *localIpAddress* [remote-ip-address *remoteIpAddress*] }

Release Information Command introduced before JUNOS Release 7.1.0.
local-ip-address and **remote-ip-address** keywords added in JUNOS Release 7.3.0.
localIpAddress and *remoteIpAddress* variables added in JUNOS Release 7.3.0.

Description Specifies a preshared key for a remote peer, indexed by remote IP or remote identity. It can also specify a preshared key which is indexed by the local ip / remote IP pair for use in specific pairings or in group preshared keys (remote is wildcard 0.0.0.0).

Manually configured keys are used during the tunnel establishment phase when the ISAKMP/IKE policy specifies preshared key authentication.

You can identify the remote peer by either IP address or fully qualified domain name (FQDN). The **no** version deletes a preshared key.



NOTE: You must enter this command in the virtual router context where the IP address or FQDN of the peer is defined.

- Options**
- *ipAddress*—Address of the peer for which the key can be used
 - *fqdn*—Fully qualified domain name of the peer for which the key can be used; a maximum of 80 characters
 - *localIpAddress*—Address of the local peer for which the key can be used
 - *remoteIpAddress*—Address of the remote peer for which the key can be used

Mode Global Configuration

ipsec key pubkey-chain rsa

Syntax [no] ipsec key pubkey-chain rsa { address *ipAddress* | name *identityString* }

Release Information Command introduced in JUNOS Release 7.1.0.

Description Enables you to configure the public key for a remote peer with which you want to establish IKE SAs. This command accesses IPsec Peer Public Key Configuration mode, from which you can enter the peer public key data without the need for a digital certificate. Public keys are used during the tunnel establishment phase when the ISAKMP/IKE policy specifies RSA digital signature authentication. The **no** version removes the peer public key from the router.

- Options**
- *ipAddress*—IP address of the peer for which the public key can be used, in 32-bit dotted decimal format (for example, 192.168.32.2)
 - *identityString*—Identity of the remote peer for which the public key can be used, either in fully qualified domain name (FQDN) format (for example, group003.customer535.isp.net) or in FQDN format preceded by an optional *user@* specification (for example, tsmith@group003.customer535.isp.net); maximum of 80 characters

Mode Global Configuration

ipsec key zeroize

Syntax ipsec key zeroize { rsa | pre-share | all }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Deletes RSA key pairs. There is no **no** version.

- Options**
- rsa—Removes the RSA key pair from the router
 - pre-share—Removes all preshared keys from the router
 - all—Removes all keys within the VR context from the router

Mode Global Configuration

ipsec lifetime

Syntax [no] ipsec lifetime { kilobytes *kilobytes* | seconds *seconds* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the default lifetime in volume of traffic or seconds. The default lifetime applies to secure tunnels that do not have a tunnel lifetime defined. When either the volume of traffic or number of seconds limit is reached, IPSec renegotiates the SA. The **no** version restores the default values.

- Options**
- *kilobytes*—Volume of traffic in kilobytes that can pass between IPSec peers before the SA expires; in the range 102400–4294967295; default value is 4294967295 kilobytes; a setting of zero turns off the kilobyte lifetime
 - *seconds*—Number of seconds an SA lives before expiring; in the range 7200–4294967295; default value is 28800 seconds (8 hours)

Mode Global Configuration

ipsec local-endpoint

Syntax [no] ipsec local-endpoint *ipAddress* transport-virtual-router *transportVRName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a default local endpoint used for ISAKMP/IKE negotiations and all IPSec tunnels for a transport virtual router. The **no** version restores the default settings of the local endpoint.

- Options**
- *ipAddress*—IP address to use as the local endpoint
 - *transportVRName*—Name of transport virtual router in which the IP address is defined

Mode Global Configuration

ipsec option dpd

Syntax [no] ipsec option dpd

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables IPsec dead peer detection (DPD) for the current virtual router. With DPD enabled, the router detects when connectivity between the router and an IPsec peer has been terminated. The router then sets the status for the tunnel and the upper layer interfaces to down, which enables routing protocols to take alternate routes. Also, administrators can then take corrective action. The **no** version restores the default DPD setting, disabled.

Mode Global Configuration

ipsec option nat-t

Syntax [no | default] ipsec option nat-t

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables IPsec Network Address Translation Traversal (NAT-T) for the current virtual router. With NAT-T enabled, IPsec traffic flows transparently through a NAT device, thereby allowing one or more remote hosts located behind the NAT device to use secure L2TP/IPsec tunnels to access the router. The **ipsec option nat-t** command affects only IKE SAs negotiated on this virtual router after the command is issued; it has no effect on previously negotiated IKE SAs. The **no** version disables NAT-T for the current virtual router. The **default** version restores the default NAT-T setting, enabled.

Mode Global Configuration

ipsec option tx-invalid-cookie

Syntax [no] ipsec option tx-invalid-cookie

Release Information Command introduced in JUNOS Release 8.1.0.

Description Enables transmission of invalid cookie notification for the current virtual router (transport VR). With invalid cookie notification enabled, the router signals to an ISAKMP peer when it does not recognize an IKE phase 1 message received from the peer. The **no** version restores the default setting, disabled.

Mode Global Configuration

ipsec transform-set

Syntax ipsec transform-set *transformSetName* *transform0*
 [*transform1* [*transform2* [*transform3* [*transform4* [*transform5*]]]]]
 no ipsec transform-set *transformSetName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates a transform set. Transform sets used for manually configured tunnels can have only one transform. Transform sets used for signaled tunnels can have up to six transforms. Transforms are numbered in a priority sequence in the order in which you enter them. Each transform provides a different combination of data authentication and confidentiality. The **no** version deletes the transform set.

- Options** ■ *transformSetName*—Name of the transform set
- *transform0* through *transform5*—AH or ESP transform; use the online Help to view available transforms

Mode Global Configuration

ipsec transport profile

Syntax [no] ipsec transport profile { *profileName* [[virtual-router *vrName*]
ip address *ipAddress*] | [virtual-router *vrName*] ip address *ipAddress* }

no ipsec transport profile { *profileName*
| [virtual-router *vrName*] ip address *ipAddress* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates or configures a transport profile for IPSec and accesses the IPSec Transport Profile Configuration mode. The **no** version deletes the transport profile.

- Options**
- *profileName*—Name of the transport profile
 - *vrName*—Name of the VR on which you want to create the profile. If you do not specify a virtual router, the current virtual router context is used
 - *ipAddress*—Remote endpoint for the IPSec transport connection. You can enter a single IP address or the wildcard address of 0.0.0.0. If you use the wildcard address, the profile accepts any remote client connection, which is a typical scenario for secure remote access.

Mode Global Configuration

ipsec tunnel profile

Syntax ipsec tunnel profile *profileName* [virtual-router *vrName*]
 no ipsec tunnel profile *profileName*

Release Information Command introduced in JUNOS Release 7.3.0.

Description Creates or configures a tunnel profile for IPSec and accesses the IPSec Tunnel Profile Configuration mode (config-ipsec-tunnel-profile). The **no** version deletes the tunnel profile.

- Options** ■ *profileName*—Name of the tunnel profile
- *vrName*—Name of the VR on which you want to create the profile. If you do not specify a virtual router, the current virtual router context is used

Mode Global Configuration

ipv6

Syntax [no] ipv6

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables an IPv6 instance on a router that does not already have an explicit IPv6 address. Normally, performing any IPv6 configuration automatically enables IPv6 on the interface. The **no** version disables IPv6 on the router.



NOTE: Disabling IPv6 on the router disables all IPv6 unicast routing protocols.

Mode Global Configuration

ipv6 access-list

Syntax Extended IPv6 access list:

```
ipv6 access-list accessListName { permit | deny } { srcIPv6Prefix |
host srcIPHost | any } { dstIPv6Prefix | host dstIPHost | any } [ log ]

no ipv6 access-list accessListName [ { permit | deny } { srcIPv6Prefix |
host srcIPv6Host | any } { dstIPv6Prefix | host dstIPv6Host | any } [ log ] ]
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines an IPv6 access list. The extended access list enables you to specify a destination address or host, precedence, and type of service. Imposes an implicit last rule of “deny ip any any” to deny all routes that do not match previous rules in the access list. The **no** version removes the IPv6 access list, the specified entry in an access list, or the log for a specified entry.

- Options**
- *accessListName*—String of up to 32 alphanumeric characters
 - permit—Permits access if the conditions are matched
 - deny—Denies access if the conditions are matched
 - *srcIPv6Prefix*—Source IPv6 address and mask length from which the packet is being sent
 - *srcIPv6Host*—Source host IPv6 address; assumes a mask length of 128
 - any—Creates an address of :: with a mask length of 0
 - *dstIPv6Prefix*—Destination IP address and mask length
 - *dstIPv6Host*—Destination host IPv6 address to which the packet is being sent
 - log—Logs an Info event into the ipAccessList log whenever the access-list rule is matched

Mode Global Configuration

ipv6 access-route table-map

Syntax `ipv6 access-route [vrf vrfName] table-map mapName`
`no ipv6 access-route [vrf vrfName] table-map [mapName]`

Release Information Command introduced before JUNOS Release 7.1.0.
 vrf keyword and *vrfName* variable added in JUNOS Release 7.2.0.

Description Filters access routes before an access list adds them to the routing table. The **no** version deletes the table map.

- Options** ■ *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
 ■ *mapName*—Name of the table map that you want the router to use

Mode Global Configuration

ipv6 address

Syntax [no] ipv6 address *ipv6Prefix* [eui-64]
 [no] ipv6 address [*ipv6Address maskLength* [eui-64]]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns an IPv6 address (or network) to an interface and enables IPv6 processing on that interface. The **no** version deletes the association from the interface.



NOTE: The link-local address for an interface is automatically configured when IPv6 is enabled on the interface.

- Options**
- *ipv6Prefix*—Prefix that defines the IPv6 interface or network in the format *ipv6Address / length*, where
 - *ipv6Address*—Base IPv6 address of the network route that you want to filter (for example, ::ffff:a:b:c:d)
 - *length*—Length of the network prefix; number of bits masking base address to produce address to be matched
 - *ipv6Address*—Base IPv6 address of the network route that you want to filter (for example, ::ffff:a:b:c:d); the *ipv6Address* must appear in hexadecimal format using 16-bit values between colons. Refer to RFC 2373—IP Version 6 Addressing Architecture (July 1998) for details.
 - *maskLength*—Length of the IPv6 mask. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
 - eui-64—Specifies the use of the eui-64 interface identifier

Mode Interface Configuration, Profile Configuration

ipv6 address-pool local

Syntax [no] ipv6 address-pool local

Release Information Command introduced in JUNOS Release 10.1.0.

Description Enables the IPv6 local address pool functionality to allow configuration of IPv6 local address pools to assign prefixes to DHCPv6 clients. The **no** version disables the IPv6 local address functionality.



NOTE: If you attempt to configure an IPv6 local address pool without enabling the IPv6 local pool feature, an error message is displayed.

Mode Global Configuration

ipv6 block-multicast-sources

Syntax [no] ipv6 block-multicast-sources

Release Information Command introduced before JUNOS Release 7.1.0.

Description Prevents mroute creation by blocking multicast traffic that has a scope larger than link-local (for example, global). The **no** version restores the default behavior of creating mroutes upon receiving multicast packets.

Mode Global Configuration

ipv6 classifier-list

Syntax `ipv6 classifier-list classifierName [traffic-class trafficClassName]`
`[color { green | yellow | red }] [user-packet-class userPacketClassValue]`
`[source-route-class routeClassValue] [destination-route-class routeClassValue]`
`[local { true | false }]`
`[source-address ipv6Prefix | source-host ipv6Address]`
`[destination-address ipv6Prefix | destination-host ipv6Address]`
`[precedence precNum | dsfield dsFieldNum | tcfield tcFieldNum]`
`[protocol [protocolQualifier]]`

`no ipv6 classifier-list classifierName [classifierNumber]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates or modifies an IPv6 classifier control list. The **no** version removes the classifier control list.

- Options**
- *classifierName*—Name of the classifier control list entry
 - *trafficClassName*—Name of the traffic class to match
 - green—Matches packet color to green, indicating a low drop preference
 - yellow—Matches packet color to yellow, indicating a medium drop preference
 - red—Matches packet color to red, indicating a high drop preference
 - *userPacketClassValue*—User packet value to match
 - *routeClassValue*—Value of the source or destination route-class; in the range 0–255
 - local—Specifies traffic destined for this interface
 - true—Matches packets that are locally destined
 - false—Matches packets that are not locally destined
 - *ipv6Prefix*—Prefix that defines the IPv6 interface or network
 - *ipv6Address*—Base IPv6 address of the network route
 - *precNum*—Upper three bits of the traffic class byte; in the range 0–7
 - *dsFieldNum*—Upper six bits of the traffic class byte; in the range 0–63
 - *tcFieldNum*—Whole eight bits of the traffic class byte; in the range 0–255
 - *protocol*—Protocol type to match; **tcp**, **udp**, **icmpv6**, or protocol number in the range 0–255
 - *protocolQualifier*—Specifies the following protocol-specific parameters:
 For TCP and UDP:
 - source-port or destination-port—Specifies that a source or destination port is matched

- *portOperator*—One of the following classifier parameters. See Creating or Modifying Classifier Control Lists for IPv6 Policy Lists for details.
 - *lt*—Less than
 - *gt*—Greater than
 - *eq*—Equal to
 - *ne*—Not equal
 - *range*—Range of port numbers
- *portNumber*—Port number of the source or destination port

For TCP only:

- *tcpFlag*; a logic equation that specifies flag bit values; ! means logical NOT and & means logical AND; use any of the following flag names:
 - *ack*—0x10
 - *fin*—0x01
 - *psh*—0x08
 - *rst*—0x04
 - *syn*—0x02
 - *urg*—0x20

For ICMPv6:

- *icmpType*—ICMP message type
- *icmpCode*—ICMP message code
- *classifierNumber*—Index of the classifier control list entry to be deleted



NOTE: The **local-input** keyword for the **ipv6 policy** command is deprecated, and may be completely removed in a future release. The keyword should be removed from scripts.

You should recreate any local input policies using the **ipv6 classifier-list local true** command and attaching the policies using the **ipv6 policy secondary-input** command.

Mode Global Configuration

Related Topics ■ Creating or Modifying Classifier Control Lists for IPv6 Policy Lists

ipv6 description

Syntax `ipv6 description name`
`no ipv6 description`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns a text description or an alias to an IPv6 interface or subinterface. Use the **show ipv6 interface** command to display the text description. The **no** version removes the description or alias.

Options ■ *name*—Name for the IP interface; string of up to 256 characters

Mode Interface Configuration, Subinterface Configuration

ipv6 dhcpv6-local delegated-prefix

Syntax `ipv6 dhcpv6-local delegated-prefix ipv6Prefix`
 `[lifetime { days [hours [minutes [seconds]]] | infinite }]`
 `no ipv6 dhcpv6-local delegated-prefix`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the IPv6 prefix and lifetime that is to be delegated, when requested, to the DHCPv6 client on this interface by the DHCPv6 local server. This lifetime overrides the default lifetime that is set in Global Configuration mode. If no lifetime is specified, the default lifetime is used. The **no** version removes the IPv6 prefix from the interface.

- Options**
- *ipv6Prefix*—Prefix that defines the IPv6 interface
 - *days*—Number of days in the lifetime; in the range 0–32768
 - *hours*—Number of hours in the lifetime; in the range 0–24
 - *minutes*—Number of minutes in the lifetime; in the range 0–60
 - *seconds*—Number of seconds in the lifetime; in the range 0–60
 - *infinite*—Assigns a lifetime that does not expire

Mode Interface Configuration

ipv6 dhcpv6-local dns-domain-search

Syntax [no] ipv6 dhcpv6-local dns-domain-search *dnsDomainName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Adds the specified DNS domain name to the domain search list. The **no** version removes the specified domain name from the search list.

Options ■ *dnsDomainName*—Name of DNS domain name

Mode Global Configuration

ipv6 dhcpv6-local dns-server

Syntax [no] ipv6 dhcpv6-local dns-server *ipv6Address*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns the specified DNS server to all DHCPv6 clients in the current virtual router. The **no** version removes the specified DNS server.

Options ■ *ipv6Address*—IPv6 address of the DNS server

Mode Global Configuration

ipv6 dhcpv6-local prefix-lifetime

Syntax `ipv6 dhcpv6-local prefix-lifetime { days [hours [minutes [seconds]]] | infinite }`
 `no ipv6 dhcpv6-local prefix-lifetime`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the default lifetime for which a prefix delegated by this DHCPv6 local server is valid. This default is overridden by the interface-specific lifetime. The **no** version restores the default lifetime to 1 day.

- Options**
- *days*—Number of days in the lifetime; in the range 0–32768
 - *hours*—Number of hours in the lifetime; in the range 0–24
 - *minutes*—Number of minutes in the lifetime; in the range 0–60
 - *seconds*—Number of seconds in the lifetime; in the range 0–60
 - *infinite*—Assigns a lifetime that does not expire

Mode Global Configuration

ipv6 dos-protection-group

Syntax `ipv6 dos-protection-group groupName`
 `no ipv6 dos-protection-group`

Release Information Command introduced in JUNOS Release 8.1.0.

Description Attaches an IPv6 denial of service (DoS) protection group to an interface. The **no** version removes the attachment of the DoS protection group from the interface.

Options ■ *groupName*—Name of the DoS protection group; string of up to 31 alphanumeric characters

Mode Interface Configuration

ipv6 enable

Syntax [no] ipv6 enable

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables IPv6 processing on an interface that does not already have an explicit IPv6 address. The **no** version disables IPv6 processing on the interface.

Mode Interface Configuration

ipv6 hop-limit

Syntax `ipv6 hop-limit [vrf vrfName] hopLimit`
`no ipv6 hop-limit [vrf vrfName]`

Release Information Command introduced before JUNOS Release 7.1.0.
 vrf keyword and *vrfName* variable added in JUNOS Release 7.2.0.

Description Specifies the maximum number of hops that the router can use in router advertisements and all IPv6 packets. The **no** version sets the hop limit for IPv6 packets to 255 hops and router advertisements to zero [0] hops (or “ unspecified”).

- Options** ■ *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
- *hopLimit*—Maximum number of hops (from 1 to 255) that the router can use in router advertisements and in all IPv6 packets; the original default value is 64 hops

Mode Global Configuration

ipv6 http

Syntax [no] ipv6 http

Release Information Command introduced in JUNOS Release 10.1.0.

Description Creates the HTTP local server for IPv6. The **no** version deletes the HTTP local server.

Mode Global Configuration

Related Topics ■ *Configuring the HTTP Server to Support Guided Entrance in the JUNOS Broadband Access Configuration Guide*

ipv6 http port

Syntax `ipv6 http port portNumber`
`no ipv6 http port`

Release Information Command introduced in JUNOS Release 10.1.0.

Description Specifies the port on which the HTTP local server receives connection attempts for IPv6. The **no** version restores the default port number.



NOTE: Port numbers from 1 to 1024 are known as reserved ports. We recommend that you specify a port number that does not belong to this range.

Options ■ *portNumber*—Number of the port, in the range 0–65535; the default is port 80

Mode Global Configuration

Related Topics ■ *Configuring the HTTP Server to Support Guided Entrance* in the *JUNOS Broadband Access Configuration Guide*

ipv6 http redirectUrl

Syntax `ipv6 http redirectUrl url`
`no ipv6 http redirectUrl`

Release Information Command introduced in JUNOS Release 10.1.0.
Profile Configuration mode added in JUNOS Release 11.0.0.

Description Specifies the URL to which a subscriber's initial Web browser session is redirected, enabling initial provisioning and service selection for the subscriber. The **no** version removes the redirection action.

Options ■ *url*—Name of the URL; 64 characters maximum

Mode Interface Configuration, Subinterface Configuration, Profile Configuration

Related Topics ■ *Configuring the HTTP Server to Support Guided Entrance* in the *JUNOS Broadband Access Configuration Guide*

ipv6 http server

Syntax [no] ipv6 http server

Release Information Command introduced in JUNOS Release 10.1.0.

Description Enables the HTTP local server to listen for and process IPv6 exception packets. The **no** version disables the HTTP local server.

Mode Global Configuration

Related Topics ■ *Configuring the HTTP Server to Support Guided Entrance in the JUNOS Broadband Access Configuration Guide*

ipv6 initial-sequence-preference

Syntax `ipv6 initial-sequence-preference preference`
 `no ipv6 initial-sequence-preference`

Release Information Command introduced in JUNOS Release 9.3.0.

Description Configures the warm restart replay preference for an IPv6 interface after a high availability switchover. The **no** version restores the default value.

Options ■ *preference*—Preference value, 0 or 1; 1 indicates highest preference; default value is 0

Mode Subinterface Configuration

ipv6-local-interface

Syntax `ipv6-local-interface { loopback interfaceSpecifier | ipv6Prefix }`
 `no ipv6-local-interface`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Maps a domain name to a loopback interface. The **no** version deletes the mapping to the user domain name.

- Options**
- *interfaceSpecifier*—Particular loopback interface
 - *ipv6Prefix*—Prefix that defines the IPv6 interface in the format *ipv6Address / length*, where
 - *ipv6Address*—Base IPv6 address of the loopback interface (for example, `::ffff:a:b:c:d`)
 - *length*—Length of the network prefix; number of bits masking base address to produce address to be matched

Mode Domain Map Configuration

ipv6 local pool

Syntax `ipv6 local pool poolName`
`no ipv6 local pool poolName [force]`

Release Information Command introduced in JUNOS Release 10.1.0.

Description Accesses IPv6 Local Pool Configuration mode. Specifies the IPv6 local address pool from which prefixes are allocated to the requesting router in networks that use DHCPv6. The **no** version removes the IPv6 local pool.

- Options**
- *poolName*—Name of the IPv6 local address pool to be used to delegate prefixes to the requesting routers or DHCPv6 clients; string of up to 16 alphanumeric characters
 - *force*—Forcibly deletes an IPv6 local address pool from which prefixes have been allocated. When a pool from which prefixes have been assigned to DHCPv6 clients is deleted, the corresponding DHCPv6 bindings are also deleted.

Mode Global Configuration

ipv6 mld

Syntax [no] ipv6 mld

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables MLD on an interface, and sets the MLD version to MLDv2. The **no** version disables MLD on an interface.

Mode Interface Configuration, Profile Configuration

ipv6 mld access-group

Syntax `ipv6 mld access-group accessListName`
 `no ipv6 mld access-group`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Restricts hosts on this subnet to joining multicast groups on the specified IPv6 access list. The **no** version removes the association with the specified access list and allows hosts on the subnetwork to join any multicast group.

Options ■ *accessListName*—Name of the access list; a string of up to 32 characters

Mode Interface Configuration, Profile Configuration

ipv6 mld access-source-group

Syntax `ipv6 mld access-source-group accessListName`
 `no ipv6 mld access-source-group`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Restricts hosts on this subnetwork to membership in those source groups (also known as “ channels”) permitted by the specified IPv6 access list. The **no** version removes any access list restriction.

Options ■ *accessListName*—Name of the access list; a string of up to 32 characters

Mode Interface Configuration, Profile Configuration

ipv6 mld apply-oif-map

Syntax `ipv6 mld apply-oif-map mapName`
 `no ipv6 mld apply-oif-map`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Applies the specified outgoing interface (OIF) map to the current interface. The **no** version removes the outgoing interface map from the interface.

Options ■ *mapName*—Name of the OIF map

Mode Interface Configuration, Profile Configuration

ipv6 mld explicit-tracking

Syntax [no] ipv6 mld explicit-tracking [disable-if-mld-v1-detected]

Release Information Command introduced in JUNOS Release 8.2.0.

Description Enables explicit host tracking for IPv6 MLD interfaces. The **no** version disables explicit host tracking on the interface or with the **disable-if-mld-v1-detected** keyword reverts to the default explicit host tracking.

Options ■ disable-if-mld-v1-detected—Disables explicit host tracking if MLD V1 hosts detected on MLD V2 interfaces

Mode Interface Configuration, Profile Configuration

ipv6 mld group limit

Syntax `ipv6 mld group limit groupLimit`
`no ipv6 mld group limit`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Limits the number of MLD groups that an interface can accept. The **no** version restores the default situation, in which there is no limit to the number of MLD groups that the interface accepts.

Options ■ *groupLimit*—Maximum number of MLD groups that an interface can accept, in the range 0–64,000

Mode Interface Configuration, Profile Configuration

ipv6 mld immediate-leave

Syntax [no] ipv6 mld immediate-leave

Release Information Command introduced before JUNOS Release 7.1.0.

Description Removes an interface immediately when the router receives a leave group membership message from the host associated with this interface. The **no** version restores the default situation, in which the router issues query messages to multicast groups and removes an interface if the associated host does not return a group membership report within a certain length of time.



CAUTION: Issue this command only on MLDv1 interfaces to which one MLD client is connected. Do not issue this command to interfaces to which more than one MLD client is connected.

Mode Interface Configuration, Profile Configuration

ipv6 mld last-member-query-interval

Syntax `ipv6 mld last-member-query-interval tenthsOfaSecond`
`no ipv6 mld last-member-query-interval`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies in tenths of a second the maximum time the router waits for a response after sending a last member query. The router sends a last member query when it receives an MLDv1 leave message or an MLDv2 state change report. The **no** version restores the default value, 10 tenths of a second (1 second).

Options ■ *tenthsOfaSecond*—Time interval to wait after sending out of a last member query in the range 1–254 tenths of a second. Using a lower value allows members to leave groups more quickly.

Mode Interface Configuration, Profile Configuration

ipv6 mld oif-map

Syntax [no] ipv6 mld oif-map *mapName* { *interfaceType interfaceSpecifier* | self }
[*groupPrefix* [*sourcePrefix*]]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates an outgoing interface (OIF) map. The **no** version removes an outgoing interface map attribute or the entire outgoing interface map.

- Options**
- *mapName*—Name of the OIF map
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - self—Specifies that the multicast outgoing interface is the same as IGMP join interface
 - *groupPrefix*—Group prefix in the form *ipv6Address/maskLength*
 - *sourcePrefix*—Source prefix in the form *ipv6Address/maskLength*

Mode Global Configuration

ipv6 mld-proxy

Syntax [no] ipv6 mld-proxy

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables MLD proxy on an interface and specifies the version. Version 2 is enabled by default. The **no** version disables MLD proxy for an interface.

Mode Interface Configuration

ipv6 mld-proxy unsolicited-report-interval

Syntax `ipv6 mld-proxy unsolicited-report-interval tenths-of-a-second`
`no ipv6 mld-proxy unsolicited-report-interval`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies how often the upstream interface should transmit unsolicited reports. This command has no effect on interfaces other than the upstream value. The **no** version transmits unsolicited reports using the default value, 100-tenths of a second (10 seconds).



NOTE: Issue this command only on the upstream interface. Otherwise, this command will have no effect.

Options ■ *tenths-of-a-seconds*—Time interval at which the interface transmits unsolicited reports

Mode Interface Configuration

ipv6 mld-proxy version

Syntax ipv6 mld-proxy version { 1 | 2 }
 no ipv6 mld-proxy version

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the MLD proxy version for the interface. The **no** version restores the default value, MLDv2.

- Options** ■ 1—Sets MLD version 1
 ■ 2—Sets MLD version 2

Mode Interface Configuration

ipv6 mld querier-timeout

Syntax `ipv6 mld querier-timeout seconds`
`no ipv6 mld querier-timeout`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the time that the interface waits before declaring itself as the querier. The **no** version restores the default value, twice the query interval.

Options ■ *seconds*—Time interval between the last query from the previous router and the first query from this interface

Mode Interface Configuration, Profile Configuration

ipv6 mld query-interval

Syntax `ipv6 mld query-interval seconds`
 `no ipv6 mld query-interval`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets how often the router sends MLD host-query packets from this interface. The **no** version restores the default value, 125 seconds.

Options ■ *seconds*—Polling interval in the range 0–65535 seconds

Mode Interface Configuration, Profile Configuration

ipv6 mld query-max-response-time

Syntax `ipv6 mld query-max-response-time tenthsOfaSecond`
`no ipv6 mld query-max-response-time`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the period in tenths of a second during which the host is expected to respond to an MLD query. MLD version 1 includes this value in MLD query messages sent out on the interface. The **no** version restores the default value, 100 tenths of a second (10 seconds).

Options ■ *tenthsOfaSecond*—Time interval between receipt of an MLD query and the response; in the range 1–254 tenths of a second.

Mode Interface Configuration, Profile Configuration

ipv6 mld robustness

Syntax `ipv6 mld robustness numberOfMessages`
 `no ipv6 mld robustness`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the number of times that the router sends MLD group-specific queries before declaring a group to no longer have any members on an interface. The **no** version restores the default value, 2.

Options ■ *numberOfMessages*—Number of times that the router sends MLD group-specific queries in the range 1–4

Mode Interface Configuration, Profile Configuration

ipv6 mld ssm-map enable

Syntax [no] ipv6 mld ssm-map enable

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables SSM mapping on the router. SSM mapping statically assigns sources to MLDv1 groups. You must use SSM mapping for MLDv1 hosts to interoperate with PIM SSM. SSM mapping allows the router to use a statically configured list to translate <*,G> memberships to <S,G> memberships. The **no** version disables the SSM map.



NOTE: To operate correctly, the static source addresses configured with the **ipv6 mld ssm-map static** command must fall within the configured PIM SSM range.

Mode Privileged Exec, User Exec

ipv6 mld ssm-map static

Syntax [no] ipv6 mld ssm-map static *accessListName* *sourceAddress*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies an access list and source address for use in SSM mapping. SSM mapping statically assigns sources to MLDv1 groups. You must use SSM mapping for MLDv1 hosts to interoperate with PIM SSM. SSM mapping allows the router to use a statically configured list to translate <*,G> memberships to <S,G> memberships. The **no** version removes the SSM map association.



NOTE: To operate correctly, the static source addresses configured with the **ipv6 mld ssm-map static** command must fall within the configured PIM SSM range.

- Options**
- *accessListName*—Name of the access control list
 - *sourceAddress*—Address of the source

Mode Privileged Exec, User Exec

ipv6 mld static-exclude

Syntax [no] ipv6 mld static-exclude *sourceAddress groupAddress*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that an interface not handle multicast traffic for one or more (S,G) combinations. The **no** version removes the (S,G) exclusion from the interface.

- Options**
- *sourceAddress*—Address of the source
 - *groupAddress*—Address of the group

Mode Interface Configuration, Profile Configuration

ipv6 mld static-group

Syntax [no] ipv6 mld static-group *groupAddress*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns an interface to handle all multicast traffic for a group. The interface sets no timers for this group. The **no** version removes the group from the interface.

Options ■ *groupAddress*—Address of the group

Mode Interface Configuration, Profile Configuration

ipv6 mld static-include

Syntax [no] ipv6 mld static-include *sourceAddress groupAddress*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns an interface to handle multicast traffic for one or more (S,G) combinations. The **no** version removes the (S,G) association from the interface.

- Options**
- *sourceAddress*—Address of the source
 - *groupAddress*—Address of the group

Mode Interface Configuration, Profile Configuration

ipv6 mld version

Syntax `ipv6 mld version { 1 | 2 | passive }`
`no ipv6 mld version`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the MLD version for the interface. The **no** version restores the default value, MLDv1.

- Options**
- 1—Sets MLD version 1
 - 2—Sets MLD version 2
 - passive—Configures a mapped OIF as a passive interface with only multicast-data-forwarding capability

Mode Interface Configuration, Profile Configuration

ipv6 mtu

Syntax `ipv6 mtu [mtuSize]`
`no ipv6 mtu`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the maximum transmission unit size of IPv6 packets sent on an interface. The **no** version restores the default value.

Options ■ *mtuSize*—Maximum number of packet transmissions permitted on an interface; in the range 160–10240; default value is 0, which means that the router takes the value from a lower protocol layer

Mode Interface Configuration, Profile Configuration, Subinterface Configuration

ipv6 multicast admission-bandwidth-limit

Syntax [no] ipv6 multicast admission-bandwidth-limit *limitValue*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Specifies multicast admission bandwidth (in kilobits per second) for a given interface. The **no** version removes the admission bandwidth limit.

Options ■ *limitValue*—Maximum admission bandwidth (in kilobits per second) permitted on an interface; default value is 0, which disables the limit

Mode Interface Configuration, Profile Configuration

ipv6 multicast ioa-packet-replication

Syntax `ipv6 multicast ioa-packet-replication interfaceType interfaceSpecifier`
 `no ipv6 multicast ioa-packet-replication`

Release Information Command introduced in JUNOS Release 7.3.0.

Description Enables IPv6 hardware multicast packet replication on port 8 of a high-density Ethernet I/O module or IOA. The **no** version disables hardware multicast packet replication.

Options ■ *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Interface Configuration

ipv6 multicast-routing

Syntax [no] ipv6 multicast-routing

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables IPv6 multicast routing on the router. The **no** version disables IPv6 multicast routing on the router.

Mode Global Configuration

ipv6 multicast-routing bandwidth-map

Syntax `ipv6 multicast-routing bandwidth-map routeMapName`
 `no ipv6 multicast-routing bandwidth-map`

Release Information Command introduced in JUNOS Release 7.1.0.

Description Enables the QoS adjust function on the router. The **no** version disables the QoS adjust function on the router.

Options ■ *routeMapName*—Name of the route map you want to use for the bandwidth map

Mode Global Configuration

ipv6 multicast-routing disable-rpf-check

Syntax `ipv6 multicast-routing disable-rpf-check accessListName`
`no ipv6 multicast-routing disable-rpf-check`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Disables RPF checks for the (S,G) pairs in the specified access list. The **no** version restores the default situation, in which the router performs RPF checks for all (S,G) pairs.

Options ■ *accessListName*—Name of the IPv6 access list that specifies the (S,G) pairs

Mode Global Configuration

ipv6 multicast-routing permanent-mroute

Syntax `ipv6 multicast-routing permanent-mroute accessListName`
`no ipv6 multicast-routing permanent-mroute`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that newly created mroutes that match the specified access-list do not get timed out. The **no** version of this command prevents any new mroutes from becoming permanent. However, it does not remove any existing permanent mroutes. To remove existing permanent mroutes, use the **clear ipv6 mroute** command.

Options ■ *accessListName*—Name of the IPv6 access list that specifies the mroutes

Mode Global Configuration

ipv6 nd

Syntax [no] ipv6 nd

Release Information Command introduced before JUNOS Release 7.1.0.
Profile Configuration mode added in JUNOS Release 9.0.0.

Description Enables the IPv6 Neighbor Discovery process on an interface. The **no** version disables the Neighbor Discovery process.

Mode Interface Configuration, Profile Configuration

ipv6 nd active-solicitations

Syntax [no] ipv6 nd active-solicitations

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that the router can actively solicit neighbors that become stale (inactive). The **no** version disables the ability to actively solicit neighbors that become stale.

Mode Interface Configuration

ipv6 nd dad attempts

Syntax `ipv6 nd dad attempts numberOfAttempts`
`no ipv6 nd dad attempts`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the number of consecutive neighbor solicitation messages that an interface sends while the router performs duplicate address detection (DAD) on the unicast IPv6 addresses of the interface. The **no** version returns the number of neighbor solicitation messages to its default value (one message without any follow-up messages).

Options ■ *numberOfAttempts*—Number of neighbor solicitation messages that you want the router to transmit

Mode Interface Configuration

ipv6 nd managed-config-flag

Syntax [no] ipv6 nd managed-config-flag

Release Information Command introduced before JUNOS Release 7.1.0.
Profile Configuration mode added in JUNOS Release 9.0.0.

Description Sets the “managed address configuration” flag in IPv6 router advertisements. The **no** version clears the flag from IPv6 router advertisements.

Mode Interface Configuration, Profile Configuration

ipv6 nd ns-interval

Syntax `ipv6 nd ns-interval milliseconds`
`no ipv6 nd ns-interval`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the interval between IPv6 neighbor solicitation retransmissions on an interface. The **no** version returns the interval between neighbor solicitation retransmission to its default value (zero [0] milliseconds for router advertisements and 1000 milliseconds for Neighbor Discovery activity of the E Series router).

Options ■ *milliseconds*—Interval between IPv6 neighbor solicit transmissions

Mode Interface Configuration

ipv6 nd other-config-flag

Syntax [no] ipv6 nd other-config-flag

Release Information Command introduced before JUNOS Release 7.1.0.
Profile Configuration mode added in JUNOS Release 9.0.0.

Description Sets the “other stateful configuration” flag in IPv6 router advertisements. The **no** version clears the flag from IPv6 router advertisements.

Mode Interface Configuration, Profile Configuration

ipv6 nd prefix-advertisement

Syntax `ipv6 nd prefix-advertisement ipv6Prefix/ipv6PrefixLength validLifetime preferredLifetime [onlink] [autoconfig]`

`[no] ipv6 nd prefix-advertisement [ipv6Prefix/ipv6PrefixLength]`

Release Information Command introduced before JUNOS Release 7.1.0.
Profile Configuration mode added in JUNOS Release 9.0.0.

Description Specifies which IPv6 prefixes the router includes in IPv6 router advertisements. In Profile Configuration mode, you can configure a single prefix. The **no** version removes any prefixes from the IPv6 routing advertisements.

- Options**
- *ipv6Prefix*—IPv6 network number to include in router advertisements
 - *ipv6PrefixLength*—Length of the IPv6 prefix; a decimal value that indicates how many of the higher-order contiguous bits of the IPv6 address comprise the prefix (the network portion of the IPv6 address). A slash (/) must precede this value.



NOTE: When used in an IPv6 profile, the *ipv6PrefixLength* must be set to a length of 64.

- *validLifetime*—Amount of time in seconds that the router can advertise the specified IPv6 prefix as valid; in the range 0–4294967295
- *preferredLifetime*—Amount of time in seconds that the router can advertise the specified IPv6 prefix as preferred; in the range 0–4294967295
- *onlink*—Indicates that the specified prefix is assigned to the link
- *autoconfig*—Indicates that local host links can use the specified prefix for IPv6 autoconfiguration

Mode Interface Configuration, Profile Configuration

ipv6 nd proxy

Syntax [no] ipv6 nd proxy

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables IPv6 Neighbor Discovery proxy. The **no** version disables IPv6 Neighbor Discovery proxy.

Mode Global Configuration

ipv6 nd ra-interval

Syntax `ipv6 nd ra-interval seconds`
`no ipv6 nd ra-interval`

Release Information Command introduced before JUNOS Release 7.1.0.
Profile Configuration mode added in JUNOS Release 9.0.0.

Description Specifies the interval between IPv6 router advertisement retransmissions on an interface. The **no** version restores the default interval, 200 seconds.

Options ■ *seconds*—Number of seconds between IPv6 advertisement retransmissions; in the range 3–1800

Mode Interface Configuration, Profile Configuration

ipv6 nd ra-lifetime

Syntax `ipv6 nd ra-lifetime seconds`
`no ipv6 nd ra-lifetime`

Release Information Command introduced before JUNOS Release 7.1.0.
Profile Configuration mode added in JUNOS Release 9.0.0.

Description Specifies the router lifetime value in IPv6 router advertisements on an interface. The router lifetime value is the amount of time the router is considered the default router on this interface. The **no** version restores the default router lifetime value, 1800 seconds.

Options ■ *seconds*—Number of seconds this router is considered the default router on this interface; in the range 0–1800. A value of zero (0) indicates that this router is not a default router on this interface. Nonzero values indicate that the router is a default router on this interface. Nonzero values should not be less than the router advertisement interval.

Mode Interface Configuration, Profile Configuration

ipv6 nd reachable-time

Syntax `ipv6 nd reachable-time { milliseconds | hours minutes seconds }`
 `no ipv6 nd reachable-time`

Release Information Command introduced before JUNOS Release 7.1.0.
 Profile Configuration mode added in JUNOS Release 9.0.0.

Description Specifies the amount of time that the E Series router can reach a remote IPv6 node after some reachability confirmation event has occurred. The **no** version restores the default value 0 milliseconds for router advertisements and 3,600,000 milliseconds (1 hour) for Neighbor Discovery activity of the E Series router.

- Options** ■ *milliseconds*—Amount of time, in the range 0–21600000 milliseconds, that the E Series router can reach a remote node after some reachability confirmation event has occurred
- *hours minutes seconds*—Amount of time, in the range 0 hours 0 minutes 0 seconds – 6 hours 0 minutes 0 seconds, that the E Series router can reach a remote node after some reachability confirmation event has occurred; this specification is not supported in Profile Configuration mode

Mode Interface Configuration, Profile Configuration

ipv6 nd suppress-ra

Syntax [no] ipv6 nd suppress-ra

Release Information Command introduced before JUNOS Release 7.1.0.
Profile Configuration mode added in JUNOS Release 9.0.0.

Description Suppresses IPv6 router advertisement transmissions on a local area network (Ethernet) interface. The **no** version reenables the sending of IPv6 router advertisement transmissions on the LAN (Ethernet) interface.

Mode Interface Configuration, Profile Configuration

ipv6 nd suppress-ra-source-link-layer

Syntax [no] ipv6 nd suppress-ra-source-link-layer

Release Information Command introduced before JUNOS Release 7.1.0.

Description Suppresses the source link-layer option in IPv6 router advertisement transmissions. This action forces neighbors to solicit the router link layer explicitly, and may prove necessary when enabling inbound load sharing across multiple link-layer addresses. The **no** version reenables the sending of the source link-layer option in IPv6 router advertisement transmissions.

Mode Interface Configuration

ipv6 neighbor

Syntax *ipv6 neighbor [vrf vrfName] ipv6Address interfaceType interfaceSpecifier hardwareAddress*

no ipv6 neighbor [vrf vrfName] ipv6Address interfaceType interfaceSpecifier

Release Information Command introduced before JUNOS Release 7.1.0.
 vrf keyword and *vrfName* variable added in JUNOS Release 7.2.0.

Description Specifies a static entry in the IPv6 Neighbor Discovery cache. The **no** version removes the static entry from the IPv6 Neighbor Discovery cache.

- Options**
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
 - *ipv6Address*—IPv6 address that corresponds to the local data-link address
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *hardwareAddress*—Local, 48-bit data-link address

Mode Global Configuration

ipv6 ospf area

Syntax [no] ip ospf [*processId*] area { *areaId* | *areaIdInt* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates an OSPFv3 interface under the specified area ID or moves an OSPFv3 interface from its current area to a specified area. The **no** version removes the interface from the specified area.

- Options**
- *processId*—Integer in the range 1–65535
 - *areaId*—OSPF area ID in IP address format
 - *areaIdInt*—OSPF area ID as a decimal value 0–4294967295

Mode Interface Configuration, Subinterface Configuration

ipv6 ospf bfd-liveness-detection

Syntax `ipv6 ospf bfd-liveness-detection [minimum-interval minInterval |
 [minimum-receive-interval minRecInterval]
 [minimum-transmit-interval minTransInterval]] [multiplier multValue]`
 `no ipv6 ospf bfd-liveness-detection`

Release Information Command introduced in JUNOS Release 7.1.0.

Description Enables BFD (bidirectional forwarding detection) on an interface running OSPFv3 and defines BFD values to be negotiated between OSPFv3 neighbors for detection of IPv6 data path failures. The **no** version disables BFD on the OSPFv3 interface.



NOTE: BFD sessions might not be maintained when the multiplier value is 1 and configured intervals are very short. We recommend that you do not use a multiplier value of 1 with very short intervals.

- Options**
- *minInterval*—Minimum proposed transmit interval and required receive interval for BFD control packets; has the same effect as configuring the minimum receive interval and the minimum transmit interval to the same value; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *minRecInterval*—Minimum interval at which the local peer must receive BFD control packets sent by the remote peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *minTransInterval*—Minimum proposed interval between BFD control packets sent by the local peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *multValue*—Detection multiplier value that the remote peer router multiplies by the local peer's negotiated transmit interval to determine the remote peer's BFD liveness detection interval; equal to the number of BFD packets that can be missed before the BFD session is declared down; number in the range 1–255; default value is 3

Mode Interface Configuration, Subinterface Configuration

ipv6 ospf cost

Syntax `ipv6 ospf [processId] cost intfCost`
`no ipv6 ospf [processId] cost`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a cost metric for an interface. Used in the calculation of the SPF routing table. The **no** version resets the path cost to the default.

- Options** ■ *processId*—Integer in the range 1–65535
- *intfCost*—Link-state metric cost; number in the range 0–65535; default value is 10

Mode Interface Configuration, Subinterface Configuration

ipv6 ospf dead-interval

Syntax `ipv6 ospf [processId] dead-interval deadInterval`
`no ipv6 ospf [processId] dead-interval`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the time period during which the router's neighbors do not see hello packets before they declare the router to be down. The **no** version resets the dead interval to its default.

- Options** ■ *processId*—Integer in the range 1–65535
- *deadInterval*—Number in the range 0–2147483647 seconds; default value is 40 seconds

Mode Interface Configuration, Subinterface Configuration

ipv6 ospf hello-interval

Syntax `ipv6 ospf [processId] hello-interval helloInterval`
`no ipv6 ospf [processId] hello-interval`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the interval between hello packets that the router sends on the interface. The **no** version resets the hello interval to its default.

- Options** ■ *processId*—Integer in the range 1–65535
 ■ *helloInterval*—Number in the range 1–65535 seconds; default value is 10 seconds

Mode Interface Configuration, Subinterface Configuration

ipv6 ospf mtu-ignore

Syntax [no] ipv6 ospf [*processId*] mtu-ignore

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that the interface ignore the MTU size contained in the DBD packet. The interface accepts data description packets from its neighbor even if it has a different a MTU size. However, the MTU size must be less than 18000. The **no** version resets the default; that the neighbor MTU size must match the MTU size of the OSPFv3 interface from which the packet is received.

Options ■ *processId*—Integer in the range 1–65535

Mode Interface Configuration, Subinterface Configuration

ipv6 ospf network

Syntax `ipv6 ospf [processId] network { broadcast | point-to-point }`
`no ipv6 ospf [processId] network`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a network type (broadcast or point-to-point) for an interface. The **no** version resets the path cost to the default.

Options ■ *processId*—Integer in the range 1–65535

Mode Interface Configuration, Subinterface Configuration

ipv6 ospf priority

Syntax `ipv6 ospf [processId] priority intfPriority`
`no ipv6 ospf [processId] priority`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the router priority. Used in determining the designated router for the particular network. This designation applies only to multiaccess networks. Every broadcast and nonbroadcast multiaccess network has a designated router. The **no** version restores the default value.

- Options** ■ *processId*—Integer in the range 1–65535
- *intfPriority*—Priority value, an 8-bit number in the range 1–255; default value is 1

Mode Interface Configuration, Subinterface Configuration

ipv6 ospf retransmit-interval

Syntax `ipv6 ospf [processId] retransmit-interval retransInterval`
 `no ipv6 ospf [processId] retransmit-interval`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the time between LSA retransmissions for the interface when an acknowledgment for the LSA is not received. The **no** version restores the default value.

- Options** ■ *processId*—Integer in the range 1–65535
 ■ *retransInterval*—Number in the range 0–3600 seconds; default value is 5 seconds

Mode Interface Configuration, Subinterface Configuration

ipv6 ospf shutdown

Syntax [no] ipv6 [*processId*] ospf shutdown

Release Information Command introduced before JUNOS Release 7.1.0.

Description Disables OSPF on an interface. The **no** version enables OSPF on the interface.

Options ■ *processId*—Integer in the range 1–65535

Mode Interface Configuration, Subinterface Configuration

ipv6 ospf transmit-delay

Syntax `ipv6 ospf [processId] transmit-delay transmDelay`
`no ipv6 ospf [processId] transmit-delay`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the estimated time it takes to transmit a link-state update packet on the interface. The **no** version restores the default value.

- Options** ■ *processId*—Integer in the range 1–65535
- *transmDelay*—Link-state transmit delay, a number in the range 0–3600 seconds; default value is 1 second

Mode Interface Configuration, Subinterface Configuration

ipv6 pim bfd-liveness-detection

Syntax `ipv6 pim bfd-liveness-detection [minimum-interval minInterval |
[minimum-receive-interval minRecInterval]
[minimum-transmit-interval minTransInterval]] [multiplier multValue]`

`no ipv6 pim bfd-liveness-detection`

Release Information Command introduced in JUNOS Release 8.0.0.

Description Enables BFD (bidirectional forwarding detection) on an interface running PIM and defines BFD values to be negotiated between PIM neighbors for detection of IPv6 data path failures. The **no** version disables BFD on the PIM interface.



NOTE: BFD sessions might not be maintained when the multiplier value is 1 and configured intervals are very short. We recommend that you do not use a multiplier value of 1 with very short intervals.

- Options**
- *minInterval*—Minimum proposed transmit interval and required receive interval for BFD control packets; has the same effect as configuring the minimum receive interval and the minimum transmit interval to the same value; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *minRecInterval*—Minimum interval at which the local peer must receive BFD control packets sent by the remote peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *minTransInterval*—Minimum proposed interval between BFD control packets sent by the local peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *multValue*—Detection multiplier value that the remote neighbor multiplies by the local router's negotiated transmit interval to determine the remote neighbor's BFD liveness detection interval; equal to the number of BFD packets that can be missed before the BFD session is declared down; number in the range 1–255; default value is 3

Mode Interface Configuration

ipv6 pim bsr-candidate

Syntax `ipv6 pim bsr-candidate interfaceType interfaceSpecifier`
 `[hashMaskLen [priority]] [period bootstrapPeriod]`
 `no ipv6 pim bsr-candidate`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a router as a bootstrap router (BSR) candidate. The **no** version disables the router BSR candidacy.

- Options**
- *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see “Interface Types and Specifiers” on page 5. The autoRP announcement messages will contain the IP address for this interface.
 - *hashMaskLen*—Length in the range 1–128 bits of the hash mask length field sent in BSMs that the router originates; default value is 126 bits
 - *priority*—Value in the range 0–255 of the BSR-Priority field of BSMs that the router originates; default value is 0
 - *bootstrapPeriod*—Interval in the range 1–65535 seconds at which the BSR sends bootstrap messages; default value is 60 seconds

Mode Global Configuration

ipv6 pim dr-priority

Syntax `ipv6 pim dr-priority priority`
`no ipv6 pim dr-priority`

Release Information Command introduced in JUNOS Release 10.0.0.

Description Assigns a priority for the interface to be selected as the designated router. An interface with a higher priority value is preferred as a designated router over an interface with a lower priority value. In Interface Configuration mode, the **no** version restores the value that is specified in Router Configuration mode. If the designated router priority is not specified in Router Configuration mode, then the default value of one is restored.



NOTE: You cannot configure the designated router priority on PIM dense mode interfaces.

Options ■ *priority*—Value in the range 1–254; default value is 1.

Mode Interface Configuration, Router Configuration

ipv6 pim join-filter

Syntax `ipv6 pim join-filter accessListName`
 `no ipv6 pim join-filter`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies an extended access list that you want this PIM router or PIM interface to use as a join filter. If an interface-level filter exists, it takes precedence over the global-level filter. The **no** version removes the filter association.

Options ■ *accessListName*—Name of the access list that you want this interface to use as a PIM join filter; a string of up to 32 alphanumeric characters

Mode Global Configuration, Interface Configuration

ipv6 pim join-prune-interval

Syntax `ipv6 pim join-prune-interval interval`
`no ipv6 pim join-prune-interval`

Release Information Command introduced in JUNOS Release 10.0.0.

Description Specifies the time interval at which the router sends the PIM join/prune message to the upstream RPF neighbor. In Interface Configuration mode, the **no** version restores the value that is specified in Router Configuration mode. If the message interval is not specified in Router Configuration mode, then the default value of 60 seconds is restored.



NOTE: You cannot configure the designated router priority on PIM dense mode interfaces.

Options ■ *interval*—Interval in the range 10–210 seconds at which the router sends the PIM join/prune message; the default value is 60 seconds.

Mode Interface Configuration, Router Configuration

ipv6 pim query-interval

Syntax `ipv6 pim query-interval queryTime`
 `no ipv6 pim query-interval`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies how often the router sends PIM router query messages from this interface. The **no** version specifies the default time interval, 30 seconds.

Options ■ *queryTime*—Interval in the range 0–210 seconds at which the router sends PIM router query messages from this interface

Mode Interface Configuration

ipv6 pim rp-address

Syntax [no] ipv6 pim rp-address *ipv6Address* [*ipv6AccessList*] [override]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a static PIM group-to-RP mapping. The **no** version clears the mapping from this interface.

- Options**
- *ipv6Address*—IPv6 address of the router you want to designate as an RP router
 - *ipv6AccessList*—Name of the IPv6 access list that specifies which multicast groups use this RP
 - **override**—Specifies that this static RP mapping has priority over group-to-RP mappings learned by auto-RP

Mode Global Configuration

ipv6 pim rp-candidate

Syntax `ipv6 pim rp-candidate interfaceType interfaceSpecifier [group-list accessListName]`
 `[hold-time holdTime] [priority priority] [interval interval]`

`no ipv6 pim rp-candidate interfaceType interfaceSpecifier`
 `[group-list accessListName]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a router as a rendezvous point (RP) router candidate. The **no** version stops the router from being an RP candidate.

- Options**
- *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see “Interface Types and Specifiers” on page 5. The autoRP announcement messages will contain the IP address for this interface.
 - *accessListName*—Access-list containing the set of group prefixes supported by this C-RP. If no group-list is specified, the default value is the entire multicast address range.
 - *holdTime*—Amount of time in the range 1–65535 seconds that the BSR keeps an RP in its C-RP list if the BSR does not receive a C-RP advertisement message; default value is 150 seconds
 - *priority*—Priority field value in the range 0– 255 that the C-RP sends to the BSR in C-RP advertisement messages; default value is 192. In the RP election process, the RP with the lower priority value is preferred.
 - *interval*—Interval in the range 1–65535 seconds at which the C-RP sends advertisement messages to the BSR; default value is 60 seconds

Mode Global Configuration

ipv6 pim sparse-mode

Syntax [no] ipv6 pim sparse-mode

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables PIM in sparse mode on an interface. The **no** version disables PIM in sparse mode on an interface.

Mode Interface Configuration

ipv6 pim sparse-mode graceful-restart-duration

Syntax `ipv6 pim sparse-mode graceful-restart-duration seconds`
`no ipv6 pim sparse-mode graceful-restart-duration`

Release Information Command introduced in JUNOS Release 10.0.0.

Description Sets duration time for PIM sparse-mode graceful restart. The **no** version resets the duration to the default.

Options ■ *seconds*—Restart duration in seconds; default value is 30 seconds

Mode Global Configuration

ipv6 pim spt-threshold

Syntax [no] ipv6 pim spt-threshold { 0 | *nonZeroInteger* | infinity }
[group-list *ipv6AccessList*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the network configuration that PIM sparse mode uses when a source starts sending multicast messages. The **no** version restores the default value, 0.

- Options**
- 0—Configures PIM sparse mode to switch to an SPT when a source begins to send multicast messages
 - *nonZeroInteger*—Integer in the range 1–4294967294; prevents PIM sparse mode from switching from a shared tree to an SPT
 - infinity—Prevents PIM sparse mode from switching from a shared tree to an SPT
 - *ipv6AccessList*—Name of the IPv6 access list that specifies the groups to which the threshold applies

Mode Global Configuration

ipv6 pim ssm

Syntax `ipv6 pim ssm { default | range ipv6AccessList }`
`no ipv6 pim ssm`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables SSM and defines the SSM range of IPv6 multicast addresses. The **no** version disables SSM on the router.

- Options**
- `default`—Specifies that SSM use the IANA-specified range of 232/8
 - `ipv6AccessList`—Name of the IPv6 access list that specifies the range of multicast addresses you want SSM to use

Mode Global Configuration

ipv6 policy

Syntax `ipv6 policy { input | output } policyName`
`[statistics { enabled [baseline { enabled | disabled }] [preserve | merge] |`
`disabled [merge] }] merge]`

`no ipv6 policy { input | output | secondary-input } [policyName]`

For policy lists in Profile Configuration mode:

`ipv6 policy { input | output } policyName`
`[statistics { enabled | disabled }] [merge]`

`no ipv6 policy { input | output | secondary-input } [policyName]`

Release Information Command introduced before JUNOS Release 7.1.0.
merge keyword added in JUNOS Release 7.2.0.
 Profile Configuration mode added in JUNOS Release 7.2.0.

Description In Interface Configuration mode, assigns a policy list to the ingress or egress of an interface. If you enter the **ipv6 policy** command and the policy list does not exist, the router creates a policy list with no rules, the default. When a policy list does not have rules, the router inserts a default filter rule. Attaching this policy list to an interface filters all packets on that interface. You must specify the **input** or **output** keyword to assign the policy list to the ingress or egress of the interface.

In Profile Configuration mode, assigns the policy list to a profile, which then assigns the policy to an interface.

The **no** version removes the association between a policy list and an interface. In Profile Configuration mode, the **no** version removes policy reference from the profile.

- Options**
- **input**—Applies policy to data arriving at this interface before a route lookup
 - **output**—Applies policy to data leaving this interface
 - **secondary-input**—Applies policy to data that arrives at this interface after a route lookup
 - ***policyName***—Name of the policy; a maximum of 40 characters
 - **statistics**—Enables or disables collection of policy routing statistics
 - **enabled**—Enable collection of policy routing statistics
 - **baseline enabled**—Enables baselining of policy routing statistics (Interface Configuration mode only)
 - **baseline disabled**—Disables baselining of policy routing statistics (Interface Configuration mode only)

- **preserve**—Preserves existing statistics for any classifier-list that is the same for both the new and old policy attachments when you attach a new policy to an interface
- **disabled**—Disable collection of policy routing statistics
- **merge**—Enables merging of multiple policies to form a single policy



NOTE: The **local-input** keyword for the **ipv6 policy** command is deprecated, and may be completely removed in a future release. The keyword should be removed from scripts.

You should recreate any local input policies using the **ipv6 classifier-list local true** command and attaching the policies using the **ipv6 policy secondary-input** command.

Mode Interface Configuration, Profile Configuration

Related Topics ■ Setting a Statistics Baseline for Policies

ipv6 policy-list

Syntax [no] ipv6 policy-list *policyName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates or modifies an IPv6 policy list. If you execute an **ipv6 policy-list** command and type **exit**, the router creates a policy list with no rules, the default. When a policy list does not have rules, the router inserts a default filter rule. Attaching this policy list to an interface filters all packets on that interface. The **no** version removes a policy list.

Options ■ *policyName*—Name of the policy list

Mode Global Configuration

Related Topics ■ Creating Policy Lists for IPv6

ipv6 policy-parameter hierarchical

Syntax `ipv6 policy-parameter hierarchical parameterName { nodeValue | atm | atm-vc | atm-vp vpValue | ethernet | fr-vc | forwarding | ppp-interface | svlan svlanValue | vlan }`

`no ipv6 policy-parameter parameterName`

Release Information Command introduced in JUNOS Release 8.0.0.
 ppp-interface keyword added in JUNOS Release 10.3.0.

Description Specifies a parameter value for IPv6 interfaces. The **no** version removes the policy parameter and its contents.

- Options**
- *parameterName*—Name of policy parameter
 - *nodeValue*—Aggregation node number in the range 1–65535
 - *vpValue*—ATM VPI number in the range 0–255
 - *svlanValue*—S-VLAN ID number in the range 0–4095

Mode Interface Configuration, Profile Configuration

Related Topics ■ Creating a Classifier Group for a Policy List

ipv6 policy-parameter reference-rate

Syntax In Interface Configuration mode:

ipv6 policy-parameter reference-rate *parameterName* [increase] *value*

no ipv6 policy-parameter reference-rate *parameterName* [increase *value*]

In Profile Configuration mode:

ipv6 policy-parameter reference-rate *parameterName* [increase] *value*

no ipv6 policy-parameter reference-rate *parameterName*

Release Information Command introduced in JUNOS Release 8.1.0.

Description Creates an IPv6 policy parameter for a reference rate; creates a global parameter if it does not exist. The **no** version removes the policy parameter and its contents; if used with the **increase** keyword, decreases the value.

- Options**
- *parameterName*—Name of policy parameter up to 40 characters
 - increase—Increments the existing reference rate value
 - *value*—Value of the reference rate parameter, in the range 0–4292967295

Mode Interface Configuration, Profile Configuration

Related Topics

- Creating a Classifier Group for a Policy List

ipv6 prefix-list

Syntax `ipv6 prefix-list listName { description desc | { [seq sequence] { permit | deny }
ipv6Prefix [ge geNumber] [le leNumber] } }`

`no ipv6 prefix-list listName [description | [seq sequence] [{ permit | deny }
ipv6Prefix [ge geNumber] [le leNumber]]]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates an IPv6 prefix list for route filtering; specifies a list entry—a permit or deny clause for a network address. The **no** version removes the specified prefix list or the specified list entry.

- Options**
- *listName*—Name of the IPv6 prefix list; a string of up to 32 characters
 - *desc*—Description of the prefix list
 - *sequence*—Number in the range 0–65535 that indicates the position the prefix list entry has in the already existing list of entries for the prefix list; if you do not specify a *sequence*, the command uses the value of the last sequence number + 5
 - *permit*—When specified, the router redistributes any prefix that matches the filtered route based on the set actions
 - *deny*—When specified, the router drops any prefix that matches the filtered route
 - *ipv6Prefix*—Network route that you want to filter, in the format *ipv6Address / length*, where
 - *ipv6Address*—Base IPv6 address of the network route that you want to filter (for example, ::ffff:a:b:c:d)
 - *length*—Length of the network prefix; number of bits masking base address to produce address to be matched
 - *geNumber*—Route being filtered matches if its prefix is within the range specified: greater than or equal to *geNumber* and less than or equal to 32
 - *leNumber*—Route being filtered matches if its prefix is within the range specified: greater than or equal to *length* and less than or equal to *leNumber*

Mode Global Configuration

ipv6-prefix-pool-name

Syntax `ipv6-prefix-pool-name poolName`
 `no ipv6-prefix-pool-name`

Release Information Command introduced in JUNOS Release 10.1.0.

Description Specifies the IPv6 local prefix pool name to be used to delegate prefixes to the requesting router, when the RADIUS server does not return a pool name using the Framed-IPv6-Pool attribute. The **no** version removes the IPv6 local pool from the AAA domain map.

Options ■ *poolName*—Name of the IPv6 local prefix pool to associate with the domain name; string of up to 16 alphanumeric characters

Mode Domain Map Configuration

ipv6 route

Syntax `ipv6 route [vrf vrfName] prefix { nextHop | interfaceType interfaceSpecifier } [distance]`

`no ipv6 route [vrf vrfName] prefix [nextHop | interfaceType interfaceSpecifier] [distance]`

Release Information Command introduced before JUNOS Release 7.1.0.
vrf keyword and *vrfName* variable added in JUNOS Release 7.2.0.

Description Configures a static IPv6 prefix route. The **no** version removes a static IPv6 prefix route.

- Options**
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
 - *prefix*—Combination of both a prefix and prefix length (mask) value. The prefix (IP address or network) defines the IPv6 interface or network. The prefix (mask) length of the IPv6 prefix is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. An example of a prefix would be “7fff::0/16”, “7fff::0/32”, “7fff:2:3::0/24”, or “7fff::1/128”.
 - *nextHop*—IPv6 address of the next-hop to reach the destination prefix (network). The next-hop address need not be directly connected; recursion locates the physical next-hop.
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *distance*—Preference value for the IPv6 route. A default value of 1 gives static routes precedence over any other type of route (with the exception of connected routes).

Mode Global Configuration

ipv6 router isis

Syntax [no] ipv6 router isis [*tag*]

Release Information Command introduced in JUNOS Release 8.2.0.

Description Enables the IS-IS routing protocol on an interface and specifies an IS-IS process for IPv6. The **no** version disables IS-IS routing.

Options ■ *tag*—Meaningful name for a routing process; name must be unique among all IP router processes for a given router; if not specified, a null tag is assumed, and the process is referenced with a null tag

Mode Interface Configuration

ipv6 router mld

Syntax [no] ipv6 router mld

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates and enables MLD on a virtual router; accesses MLD router configuration mode. The **no** version disables MLD on a virtual router.



NOTE: This command is identical to the **router mld** command.

Mode Global Configuration

ipv6-router-name

Syntax `ipv6-router-name vrName`
 `no ipv6-router-name [vrName]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Maps a user domain name to an IPv6 virtual router. The **no** version deletes the router name parameter, and the router defaults to the default virtual router.

Options ■ *vrName*—Name of the virtual router; a string of 1–15 alphanumeric characters

Mode Domain Map Configuration

ipv6 router ospf

Syntax [no] ipv6 router ospf *processId*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures an IPv6 OSPF routing process. The **no** version disables an IPv6 OSPF routing process.

Options ■ *processId*—Number in the range 1–65535 that identifies the OSPF process

Mode Global Configuration

ipv6 router pim

Syntax [no] ipv6 router pim

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates and enables PIM for IPv6 on a virtual router; accesses PIM router configuration mode. The **no** version deletes PIM from a virtual router.

Mode Global Configuration

ipv6 route-type

Syntax For BGP

```
ipv6 route-type [ unicast | both ]
```

```
no ipv6 route-type
```

For OSPF

```
ipv6 route-type [ unicast | multicast | both ]
```

```
no ipv6 route-type
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description For BGP, specifies whether BGP IPv6 routes are available only for other unicast protocols or for both unicast protocols and multicast protocols to perform RPF checks. The **no** version restores the default value, unicast.

For OSPF, specifies whether OSPF IPv6 routes are available only for unicast forwarding, only for multicast reverse path forwarding checks, or for both. The **no** version restores the default value, both.

- Options**
- unicast—Specifies that routes for the protocol are available only for unicast forwarding
 - both—Specifies that routes for the protocol are available for both unicast forwarding and multicast route path forwarding checks
 - multicast—Specifies that routes for the protocol are available only for multicast route path forwarding checks

Mode Router Configuration

ipv6 rpf-route

Syntax `ipv6 rpf-route [vrf vrfName] ipv6Address/addressMask
 { nextHopIpv6Address | interfaceType interfaceSpecifier } [distance]`

`no ipv6 rpf-route [vrf vrfName] ipv6Address/addressMask
 [nextHopIpv6Address | interfaceType interfaceSpecifier] [distance]`

Release Information Command introduced before JUNOS Release 7.1.0.
 vrf keyword and *vrfName* variable added in JUNOS Release 7.2.0.

Description Customizes static IPv6 routes that the router can use to verify source addresses in multicast packets. The **no** version removes the static route.

- Options**
- *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
 - *ipv6Address*—IPv6 address of the destination network
 - *addressMask*—Subnet mask for the destination network
 - *nextHopIpv6Address*—IPv6 address of the next hop
 - *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *distance*—Number in the range 0–255 that indicates the preference for this route

Mode Global Configuration

ipv6 sa-validate

Syntax [no] ipv6 sa-validate

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables source address validation on an IPv6 interface. This feature verifies that a packet has been sent from a valid source address. When a packet arrives on an interface, the router performs a routing table lookup using the source address. The result from the routing table lookup is an interface to which packets destined for that address are routed. This interface must match the interface that the packet arrived on. If it does not match, the router drops the packet. The **no** version disables source address validation.

Mode Interface Configuration, Profile Configuration

ipv6 share-interface

Syntax `ipv6 share-interface interfaceType interfaceSpecifier`
 `no ipv6 share-interface`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the layer 2 interface that an IPv6 interface will share in the current virtual router. The **no** version removes the association between the layer 2 interface and the shared IPv6 interface.

- Options** ■ *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Interface Configuration

ipv6 static-route table-map

Syntax `ipv6 static-route table-map [vrf vrfName] mapName`
 `no ipv6 static-route table-map [vrf vrfName] [mapName]`

Release Information Command introduced before JUNOS Release 7.1.0.
 vrf keyword and *vrfName* variable added in JUNOS Release 7.2.0.

Description Filters static routes before adding them to the routing table. The **no** version deletes the table map.

- Options** ■ *vrfName*—Name of the VRF; string of 1–32 alphanumeric characters
 ■ *mapName*—Name of the table map that you want the router to use

Mode Global Configuration

ipv6 unnumbered

Syntax `ipv6 unnumbered interfaceType interfaceSpecifier`
 `no ipv6 unnumbered`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables or disables IPv6 processing on an interface without assigning an explicit IPv6 address to that interface. The global IPv6 address of the interface, specified by the *interfaceType interfaceSpecifier* values, becomes the source address in packets that the unnumbered interface generates. The **no** version of the command removes the IPv6 address from the interface.



NOTE: Enabling IPv6 on an interface automatically configures the link-local address on an unnumbered interface.

- Options**
- *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Interface Configuration, Profile Configuration

ipv6 virtual-router

Syntax [no] ipv6 virtual-router *vrName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a virtual router in an IPv6 profile. Dynamic interfaces created with the profile are assigned to this VR. The **no** version removes the VR from the profile; if a VR is not specified via RADIUS, then any subsequent creation process for dynamic interfaces using the profile fails.

Options ■ *vrName*—Name of the virtual router; a string of 1–15 alphanumeric characters

Mode Profile Configuration

isis authentication-key

Syntax isis authentication-key [level-1 | level-2] *authKey*
 no isis authentication-key [level-1 | level-2]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns a password for IS-IS level 1 and level 2 hellos used by neighboring routers that are using IS-IS password authentication. The **no** version deletes the password.

- Options**
- level-1—Inserts the password into level 1 hello packets
 - level-2—Inserts the password into level 2 hello packets
 - *authKey*—Password; string of up to 8 characters

Mode Interface Configuration, Subinterface Configuration

isis bfd-liveness-detection

Syntax [no] isis bfd-liveness-detection [minimum-interval *minInterval* |
[minimum-receive-interval *minRecInterval*]
[minimum-transmit-interval *minTransInterval*]] [multiplier *multValue*]

Release Information Command introduced in JUNOS Release 7.1.0.

Description Enables BFD (bidirectional forwarding detection) on an interface running IS-IS and defines BFD values to be negotiated between IS-IS neighbors for detection of IP data path failures. The **no** version disables BFD on the IS-IS interface.



NOTE: BFD sessions might not be maintained when the multiplier value is 1 and configured intervals are very short. We recommend that you do not use a multiplier value of 1 with very short intervals.

- Options**
- *minInterval*—Minimum proposed transmit interval and required receive interval for BFD control packets; has the same effect as configuring the minimum receive interval and the minimum transmit interval to the same value; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *minRecInterval*—Minimum interval at which the local peer must receive BFD control packets sent by the remote peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *minTransInterval*—Minimum proposed interval between BFD control packets sent by the local peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *multValue*—Detection multiplier value that the remote peer router multiplies by the local peer's negotiated transmit interval to determine the remote peer's BFD liveness detection interval; equal to the number of BFD packets that can be missed before the BFD session is declared down; number in the range 1–255; default value is 3

Mode Interface Configuration, Subinterface Configuration

isis circuit-type

Syntax isis circuit-type [level-1 | level-1-2 | level-2-only]
 no isis circuit-type

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the type of adjacency desired for the specified interface. The **no** version resets the circuit type to level 1 and level 2.

- Options**
- level-1—Establishes a level 1 adjacency if there is at least one area address in common between this router and its neighbors
 - level-1-2—(default) Establishes a level 1 and 2 adjacency if the neighbor is also configured as a level 1-2 router and there is at least one area in common. If there is no area in common, a level 2 adjacency is established.
 - level-2-only—Establishes a level 2 adjacency on the circuit. If the neighboring router is a level 1 only router, no adjacency will be established.

Mode Interface Configuration, Subinterface Configuration

isis csnp-interval

Syntax isis csnp-interval *seconds* [level-1 | level-2]
 no isis csnp-interval [*seconds*] [level-1 | level-2]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the IS-IS CSNP interval for the specified interface. The **no** version restores the default value.

- Options**
- *seconds*—Number in the range 0–65535; the interval of time in seconds between the transmission of CSNPs on multiaccess networks for the designated router; default value is 10 seconds, except for WAN interfaces, where the default value is 0
 - *level-1*—Sets the interval of time between transmission of CSNPs for level 1 independently
 - *level-2*—Sets the interval of time between transmission of CSNPs for level 2 independently

Mode Interface Configuration, Subinterface Configuration

isis hello-interval

Syntax isis hello-interval *seconds* [level-1 | level-2]
 no isis hello-interval [*seconds*] [level-1 | level-2]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the length of time in seconds between hello packets that the router sends on the specified interface. The **no** version restores the default value.

- Options**
- *seconds*—Time (in the range 0–65535 seconds) equal to the *hello multiplier* times the *hello interval seconds*; default value is 10 seconds.
 - level-1—Sets the hello interval for level 1 independently
 - level-2—Sets the hello interval for level 2 independently

Mode Interface Configuration, Subinterface Configuration

isis hello-multiplier

Syntax isis hello-multiplier *multiplier* [level-1 | level-2]
 no isis hello-multiplier [*multiplier* | level-1 | level-2]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the number of IS-IS hello packets a neighbor must miss before the router declares the adjacency to be down. The **no** version restores the *multiplier* default value, 3.

- Options**
- *multiplier*—Value (in the range 3–1 000) that the router uses as the hello-multiplier when calculating the advertised hold time. The default multiplier value is 3.
 - level-1—Sets the hello-multiplier independently for level 1 adjacencies
 - level-2—Sets the hello-multiplier independently for level 2 adjacencies

Mode Interface Configuration, Subinterface Configuration

isis hello padding

Syntax [no] isis hello padding

Release Information Command introduced in JUNOS Release 7.3.0.

Description Pads IS-IS hello packets to their full maximum transmission unit (MTU) size. The **no** version restores the hello padding to its default, no padding.

Mode Interface Configuration

isis lsp-interval

Syntax isis lsp-interval *milliseconds*
 no isis lsp-interval

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the time delay between successive IS-IS link-state packet transmissions. The **no** version restores the default value, 33 milliseconds.

Options ■ *milliseconds*—Number of milliseconds in the range 1–4294967295; an interval between successive link-state packets

Mode Interface Configuration, Subinterface Configuration

isis mesh-group

Syntax isis mesh-group { blocked | *number* }
 no isis mesh-group

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures an interface in the same mesh group to act as a virtual multiaccess network. The **no** version disables the feature.

- Options** ■ blocked—Blocks reserved LSPs from being flooded out on this defined configured interface
- *number*—Mesh group number in the range 1–4294967295

Mode Interface Configuration, Subinterface Configuration

isis message-digest-key

Syntax isis message-digest-key *keyId* hmac-md5 *key*
 [start-accept *startAcceptTime* [{ *startAcceptMonth* *startAcceptDay* | *startAcceptDay* *startAcceptMonth* } *startAcceptYear*]]
 [start-generate *startGenTime* [{ *startGenMonth* *startGenDay* | *startGenDay* *startGenMonth* } *startGenYear*]]
 [stop-accept { never | *stopAcceptTime* [{ *stopAcceptMonth* *stopAcceptDay* | *stopAcceptDay* *stopAcceptMonth* } *stopAcceptYear*] }]
 [stop-generate { never | *stopGenTime* [{ *stopGenMonth* *stopGenDay* | *stopGenDay* *stopGenMonth* } *stopGenYear*] }] [level-1 | level-2]
 no isis message-digest-key *keyId* [level-1 | level-2]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies an HMAC MD5 key that the router uses to create a secure, encrypted message digest of IS-IS level 1 or level 2 hello packets on the interface. Level 1 packets are the default. The digest is inserted into the packet from which it is created. Using this algorithm protects against intrusion by preventing unauthorized routers from forming adjacencies with your router.

You can specify when the router will start (default is the current time) and stop (default is never) accepting packets that include a digest made with this key. You can specify when the router will start (default is the current time plus 2 minutes) and stop (default is never) generating packets that include a digest made with this key. The **no** version deletes the key specified by the *keyId*.

- Options**
- *keyId*—Integer from 1 to 255 that is a unique identifier for the secret key, sent with the message digest in the packet.
 - *key*—String of up to 20 alphanumeric characters; secret key used by the HMAC MD5 algorithm to generate the message digest.
 - *startAcceptTime*, *startAcceptMonth*, *startAcceptDay*, *startAcceptYear*—Time, month, day, year that the router will start accepting packets created with this password. Use military time format *HH : MM[: SS]*.
 - *startGenTime*, *startGenMonth*, *startGenDay*, *startGenYear*—Time, month, day, year that the router will start inserting this password into packets. Use military time format *HH : MM[: SS]*.
 - never—Specifies that the router never stops accepting or generating packets; overrides previously specified stop times.
 - *stopAcceptTime*, *stopAcceptMonth*, *stopAcceptDay*, *stopAcceptYear*—Time, month, day, year that the router will stop accepting packets created with this password. Use military time format *HH : MM[: SS]*.
 - *stopGenTime*, *stopGenMonth*, *stopGenDay*, *stopGenYear*—Time, month, day, year that the router will stop inserting this password into packets. Use military time format *HH : MM[: SS]*.

- level-1—Inserts the password into level 1 hello packets
- level-2—Inserts the password into level 2 hello packets

Mode Interface Configuration, Subinterface Configuration

isis metric

Syntax isis metric *defaultMetric* [level-1 | level-2]
 no isis metric [*defaultMetric* | level-1 | level-2]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the metric (cost) for the interface to links at the specified level. If no level is specified, the cost is applied to both level 1 and level 2 links. The **no** version restores the default metric value.

- Options**
- *defaultMetric*—Metric used for the redistributed route; a number in the range 0–63 if the router is configured with the **metric-style narrow** command; a number in the range 0–16777215 if the router is configured with the **metric-style transition** or **metric-style wide** command; default value is 10
 - level-1—Applies metric to level 1 links
 - level-2—Applies metric to level 2 links

Mode Interface Configuration, Subinterface Configuration

isis network point-to-point

Syntax [no] isis network point-to-point

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the IS-IS circuit type as point-to-point. Issuing this command tears down existing adjacencies, originates or flushes LSPs, and establishes new adjacencies. The **no** version restores the default, treating the circuit as a broadcast circuit.

Mode Interface Configuration

isis priority

Syntax isis priority *value* [level-1 | level-2]
 no isis priority [level-1 | level-2]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the priority of this router for designated router election. The **no** version resets priority to the default value, 64.

- Options**
- *value*—Number in the range 0–127; the priority of a router; default value is 64
 - level-1—Sets the priority of a router for level 1 independently
 - level-2—Sets priority of a router for level 2 independently

Mode Interface Configuration, Subinterface Configuration

isis retransmit-interval

Syntax isis retransmit-interval *seconds*
 no isis retransmit-interval

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the number of seconds between retransmission of LSPs with the same lsp-id for point-to-point links. The **no** version restores the default value.

Options ■ *seconds*—Number of seconds in the range 1–65535; default value is 5. The number should be greater than the expected round-trip delay between any two routers on the attached network. The setting of this parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines.

Mode Interface Configuration, Subinterface Configuration

isis retransmit-throttle-interval

Syntax isis retransmit-throttle-interval *milliseconds*
 no isis retransmit-throttle-interval

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the amount of time between retransmissions of any IS-IS LSPs on a point-to-point interface. The **no** version restores the default value, 33 milliseconds.

Options ■ *milliseconds*—Number of milliseconds in the range 0–65535; the minimum delay between LSP retransmissions on the interface

Mode Interface Configuration, Subinterface Configuration

isis tag

Syntax [no] isis tag *tagValue*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a route tag value for the IP addresses on an IS-IS interface before the route is propagated to other routers in an IS-IS domain. To use the route tag, you must reference it in a route map to set values and/or redistribute routes. The **no** version removes the route tag from the interface.

Options ■ *tagValue*—Number in the range 1–4294967295 that identifies the route tag assigned to the IS-IS interface

Mode Interface Configuration, Subinterface Configuration

issuer-identifier

Syntax issuer-identifier *name*

 no issuer-identifier

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the name of the CA issuer for online digital certificate configuration. In CA authentication requests, the identifier is used together with the enrollment URL specified by the **enrollment url** command. The **no** version removes the name from the configuration.

Options ■ *name*—Name of CA issuer; in the range 1–200 characters

Mode IPSec CA Identity Configuration

issu initialize

Syntax issu initialize

Release Information Command introduced in JUNOS Release 9.0.0.

Description Starts the initialization phase of unified ISSU. There is no **no** version.

Mode Privileged Exec

issu start

Syntax issu start

Release Information Command introduced in JUNOS Release 9.0.0.

Description Starts the upgrade phase of unified ISSU. There is no **no** version.

Mode Privileged Exec

issu stop

Syntax issu stop

Release Information Command introduced in JUNOS Release 9.0.0.

Description Stops the unified ISSU operation and restores the router to the state existing before you issued the **issu initialize** command. There is no **no** version.

Mode Privileged Exec

is-type

Syntax is-type { level-1 | level-1-2 | level-2-only }
no is-type

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the IS-IS level at which the router is to operate. The **no** version restores the default value, level-1-2.

- Options**
- level-1—Causes the router to act as a station router
 - level-1-2—Causes the router to act as both a station router and an area router; the default setting
 - level-2-only—Causes the router to act as an area router

Mode Router Configuration

Chapter 11

K Commands

key

Syntax To assign a RADIUS key:

key secret

no key

To assign a RADIUS relay key:

key ipAddress ipMask relaySecret

no key ipAddress ipMask

To assign an ISAKMP/IKE key:

key keyString

no key

Release Information Command introduced before JUNOS Release 7.1.0.

Description From RADIUS Configuration mode, specifies the secret for the RADIUS authentication, accounting, dynamic-request server, or preauthentication server that is used to calculate the RADIUS authenticator field during exchanges with the RADIUS server. The **no** version removes the secret and causes the router to drop all requests for the RADIUS client.

From RADIUS Relay Configuration mode, specifies the IP address and mask of the network that will use the relay authentication or accounting server, and the secret used during exchanges between the RADIUS relay server and client. The **no** version removes the secret.

From IPsec Manual Key Configuration mode, configures a manual ISAKMP/IKE preshared key. There is no **no** version. To delete a key, use the **no** version of the **ipsec key manual** command.

- Options**
- *secret*—Authentication, accounting, dynamic-request, or preauthentication server secret text string used by RADIUS to encrypt the client and server authenticator field during exchanges between the router and a RADIUS server. The router encrypts PPP PAP passwords using this text string.
 - *ipAddress*—IP address for client network
 - *ipMask*—IP mask for the client network
 - *relaySecret*—Text string; up to 32 characters
 - *keyString*—Key value in ASCII format; up to 200 characters

Mode IPsec Manual Key Configuration, RADIUS Configuration, RADIUS Relay Configuration

Related Topics ■ Configuring RADIUS-Based Mirroring

key-string

Syntax `key-string keyStringData`

Release Information Command introduced in JUNOS Release 7.1.0.

Description Manually configures a 1024-bit or 2048-bit ISAKMP/IKE public key that a remote peer uses for RSA authentication without the need for a digital certificate. The key string represents the public key hexadecimal data that includes the ASN.1 object identifier and sequence tags for RSA encryption. There is no **no** version. To remove a peer public key from the router, use the **no** version of the **ipsec key pubkey-chain rsa** command.

Options ■ *keyStringData*—Alphanumeric string with a maximum length of 1999 characters; delimited by the first character of the string, which must be repeated at the end of the string and must not occur anywhere else in the string

Mode IPSec Peer Public Key Configuration

Chapter 12

L Commands

l2c

Syntax [no] l2c

Release Information Command introduced before JUNOS Release 7.1.0.

Description Accesses the L2C Configuration (config-l2c) mode for ANCP. The **no** version exits the L2C Configuration mode and removes all ANCP configuration.

Mode Global Configuration

l2c end-user-id

Syntax `l2c end-user-id idString neighbor neighborName`
 `no l2c end-user-id idString`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates the GSMP output label associated with the interface. In addition to the label, this command also specifies the access node using the **neighbor** keyword. The **no** version removes the output label association.

- Options** ■ *idString*—String to identify the GSMP label
 ■ *neighborName*—Name of the neighboring access node

Mode Interface Configuration, Subinterface Configuration

l2c ip listen

Syntax [no] l2c ip listen

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates a listening TCP socket at the virtual router within the ANCP context. ANCP needs TCP sockets so that neighbors can open GSMP sessions. The **no** version removes the listening TCP socket and stops any new sessions from being established. The **no** version does not terminate any existing GSMP sessions.

Mode Global Configuration

l2c ip oif

Syntax [no] l2c ip oif

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates an IGMP session at the virtual router within the context. ANCP needs IGMP sessions so it can convey OIF mapping events to the appropriate ANCP neighbor. The **no** version removes the IGMP session.

Mode Global Configuration

I2c line-configuration

Syntax I2c line-configuration interface *interfaceType interfaceSpecifier profileName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Generates a GSMP port management message to the access node for the purpose of configuring a DSL profile string on the specified neighbor interface. There is no **no** version.

- Options**
- *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *profileName*—Name of profile to be used in the line configuration (port management) message

Mode Global Configuration

I2c max-branches

Syntax [no] I2c max-branches *maxBranches*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the maximum number of branches the ANCP end user can have. The **no** version returns the maximum number of branches to its default value (unlimited branches).

Options ■ *maxBranches*—Maximum number of branches allowed for the ANCP end user in the range 1–64000

Mode Interface Configuration, Subinterface Configuration

I2c oam

Syntax `I2c oam { neighbor neighborName end-user-id endUserId | interface interfaceType interfaceSpecifier } [count countValue] [timeout timeoutValue]`

Release Information Command introduced in JUNOS Release 7.2.0.

Description Triggers the access node to run a local loopback test on the specified interface. There is no **no** version.

- Options**
- *neighborName*—Name of the neighbor
 - *endUserId*—Output ANCP label
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *countValue*—Number of local loopback messages
 - *timeoutValue*—Time (in seconds) for the access node to wait for a loopback response from the neighbor

Mode Privileged Exec, User Exec

l2c peer-attachment-id

Syntax l2c peer-attachment-id *idString*
 no l2c peer-attachment-id

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates the GSMP input label associated with the interface. The **no** version removes the input label association.

Options ■ *idString*—String to identify the GSMP label

Mode Interface Configuration, Subinterface Configuration

l2tp checksum

Syntax [no] l2tp checksum

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the generation of a UDP data integrity checksum in data packets sent to an L2TP peer. The default setting is disabled. The **no** version disables the generation of the checksums.

Mode Global Configuration

I2tp classifier-list

Syntax `i2tp classifier-list classifierName [traffic-class trafficClassName]`
 `[color { green | yellow | red }] [user-packet-class userPacketClassValue]`
 `no i2tp classifier-list classifierName [classifierNumber]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates or modifies a classifier control list. The **no** version removes the classifier control list.

- Options**
- *classifierName*—Name of the classifier control list entry
 - *classifierNumber*—Index of the classifier list entry; use the **show classifier-list** command to see a list of entries with index numbers
 - *trafficClassName*—Name of the traffic class to match
 - green—Matches packet color to green, indicating a low drop preference
 - yellow—Matches packet color to yellow, indicating a medium drop preference
 - red—Matches packet color to red, indicating a high drop preference
 - *userPacketClassValue*—User packet class value

Mode Global Configuration

Related Topics ■ Creating or Modifying Classifier Control Lists for L2TP Policy Lists

l2tp destination lockdown-test

Syntax [no] l2tp destination lockdown-test

Release Information Command introduced in JUNOS Release 7.2.0.

Description Configures L2TP to test locked-out destinations to verify whether a destination is available before it is returned to service. The **no** version restores the default behavior, in which locked-out destinations are not tested.

Mode Global Configuration

l2tp destination lockout-timeout

Syntax l2tp destination lockout-timeout *timeOutValue*
 no l2tp destination lockout-timeout

Release Information Command introduced in JUNOS Release 7.2.0.

Description Specifies the amount of time an L2TP destination remains in the lockout state after the destination becomes unavailable. When the timeout period expires, the router either begins the lockout test procedure (if configured to do so) or immediately returns the destination to service. The **no** version restores the default lockout timeout value.

Options ■ *timeOutValue*—Number of seconds in the range 60–3600; default is 300 seconds (5 minutes)

Mode Global Configuration

l2tp destination profile

Syntax l2tp destination profile { *profileName* [[virtual-router *vrName*]
ip address *ipAddress*] | [virtual-router *vrName*] ip address *ipAddress* }

no l2tp destination profile { *profileName* |
[virtual-router *vrName*] ip address *ipAddress* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates or accesses a destination profile that defines the location of a LAC. The **no** version removes the L2TP destination profile.

- Options**
- *profileName*—Name of the L2TP destination profile
 - *vrName*—Name of the virtual router to be used to reach the destination (that is, the LAC). If you do not specify a virtual router, the current virtual router context is used.
 - *ipAddress*—IP address to be used to reach the destination

Mode Global Configuration

l2tp destruct-timeout

Syntax l2tp destruct-timeout *seconds*
 no l2tp destruct-timeout

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the maximum time for which the router maintains dynamic destinations, tunnels, and sessions that have terminated. If resources are low, the router will replace the terminated objects with new requests. The **no** version restores the default value, 600 seconds.

Options ■ *seconds*—Time in the range 10–3600 seconds (1 hour)

Mode Global Configuration

l2tp dial-out connecting-timer-value

Syntax [no] l2tp dial-out connecting-timer-value *connectingTime*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the maximum amount of time allowed for successful establishment of an L2TP dial-out session. The **no** version restores the default value, 30 seconds.

Options ■ *connectingTime*—Range 30–3600 seconds

Mode Global Configuration

l2tp dial-out dormant-timer-value

Syntax [no] l2tp dial-out dormant-timer-value *dormantTime*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines how long the dial-out session stays in the dormant state waiting for a new trigger after the associated L2TP outgoing call is ended. The **no** version set the dormant timer to the default value, 300 seconds (5 minutes).

Options ■ *dormantTime*—Range 0–3600 seconds

Mode Global Configuration

l2tp dial-out max-buffered-triggers

Syntax [no] l2tp dial-out max-buffered-triggers *maxBuffers*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the maximum number of buffered trigger packets held for any dial-out session pending the successful establishment of the L2TP session. The **no** version set the number of trigger buffers to the default value, 0.

Options ■ *maxBuffers*—Range 0–50 buffered packets

Mode Global Configuration

I2tp dial-out session delete

Syntax I2tp dial-out session delete *triggerIpAddress*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Deletes a dial-out session. There is no **no** version.

Options ■ *triggerIpAddress*—Target IP address of the session

Mode Privileged Exec

l2tp dial-out session reset

Syntax l2tp dial-out session reset *triggerIpAddress*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Resets the state of a dial-out session by forcing it to the dormant state. There is no **no** version.

Options ■ *triggerIpAddress*—Trigger IP address of the session

Mode Privileged Exec

l2tp dial-out target

Syntax l2tp dial-out target *ipAddress ipAddressMask domainName* profile *profileName*
 no l2tp dial-out target *ipAddress ipAddressMask*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines an L2TP dial-out target that enables the creation of a dial-out session. The **no** version removes the L2TP dial-out route or target.

- Options**
- *ipAddress*—IP address of the target
 - *ipAddressMask*—IP address mask of the target
 - *domainName*—Domain name to be used in the outgoing call Access-Request message
 - *profileName*—Name of profile to be used in the creation of the interface stack

Mode Global Configuration

l2tp disable calling-number-avp

Syntax [no] l2tp disable calling-number-avp

Release Information Command introduced before JUNOS Release 7.1.0.

Description Prevents the E Series LAC from sending the Calling Number attribute value pair (AVP) in incoming-call-request (ICRQ) packets. The **no** version enables sending of the Calling Number AVP, the default setting.

Mode Global Configuration

l2tp disable challenge

Syntax [no] l2tp disable challenge

Release Information Command introduced before JUNOS Release 7.1.0.

Description Disables the generation of local tunnel authentication challenges. The **no** version enables local challenge generation, which is the default setting.

Mode Global Configuration

l2tp disconnect-cause

Syntax [no] l2tp disconnect-cause

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables an E Series LNS to generate, for all L2TP sessions, a PPP Disconnect Cause Code attribute value pair (AVP) and include it in all L2TP Call-Disconnect-Notify (CDN) messages that it sends to an LAC. This action provides a mechanism for the LAC to obtain information about the cause of a session disconnection. The **no** version disables generation of the PPP Disconnect Cause Code AVP, which is the default setting.

Mode Global Configuration

l2tp drain

Syntax [no] l2tp drain

Release Information Command introduced before JUNOS Release 7.1.0.

Description Prevents the creation of new destinations, tunnels, and sessions for the router. This command works in conjunction with the **l2tp shutdown** command. Both commands affect the status of the administrative state of L2TP on the router; the **l2tp drain** command sets the administrative state to drain. The **no** version allows the creation of new destinations, tunnels, and sessions for the router.

Mode Global Configuration

l2tp drain destination

Syntax [no] l2tp drain destination { *destinationName*
| [virtual-router *vrName*] ip *ipAddress* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Prevents the creation of new tunnels and sessions at a destination. This command works in conjunction with the **l2tp shutdown destination** command. Both commands affect the status of the administrative state of L2TP for the destination; the **l2tp drain destination** command sets the administrative state to drain. The **no** version allows the creation of new tunnels and sessions at a destination.

- Options**
- *destinationName*—Name the router assigns to the LNS
 - *vrName*—Name of the virtual router on which the destination exists
 - *ipAddress*—IP address of the LNS

Mode Global Configuration

l2tp drain tunnel

Syntax [no] l2tp drain tunnel { *destinationName* |
[virtual-router *vrName*] ip *ipAddress* *tunnelName* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Prevents the assignment of new sessions to a tunnel. This command works in conjunction with the **l2tp shutdown tunnel** command. Both commands affect the status of the administrative state of L2TP for the tunnel; the **l2tp drain tunnel** command sets the administrative state to drain. The **no** version allows the assignment of new sessions to a tunnel.

- Options**
- *destinationName*—Name the router assigns to the LNS
 - *vrName*—Name of the virtual router on which the tunnel exists
 - *ipAddress*—IP address of the LNS
 - *tunnelName*—Name of the tunnel

Mode Global Configuration

l2tp failover-resync

Syntax l2tp failover-resync { failover-protocol | failover-protocol-fallback-to-silent-failover | silent-failover | disable }

no l2tp failover-resync

Release Information Command introduced in JUNOS Release 7.3.0.

Description Configures the global L2TP peer resynchronization method that an L2TP failed endpoint uses to resynchronize with its peer non-failed endpoint. This setting can be overridden by a peer resynchronization method that is configured by either an L2TP host profile or an AAA domain map tunnel configuration. The **no** version disables peer resynchronization. The **default** version restores the default peer resynchronization method, failover-protocol-fallback-to-silent-failover.

- Options**
- failover-protocol—Specifies the L2TP failover protocol method
 - failover-protocol-fallback-to-silent-failover—Specifies the L2TP failover protocol method; however, if the peer does not support this method, the silent failover method is used; this is the default setting
 - silent-failover—Specifies the silent failover method
 - disable—Disables peer resynchronization

Mode Global Configuration

l2tp fail-over-within-preference

Syntax [no] l2tp fail-over-within-preference

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables tunnel selection within a preference level. The **no** version restores the default behavior, which is to drop down a preference level when a connection attempt has failed.

Mode Global Configuration

l2tp ignore-receive-data-sequencing

Syntax [no] l2tp ignore-receive-data-sequencing

Release Information Command introduced before JUNOS Release 7.1.0.

Description Suppresses sequence number checking for data packets received on all L2TP tunnels in the router. This setting affects only packets received on a tunnel, not packets sent on a tunnel. The L2TP LAC still inserts sequence numbers into data packets if the LAC receives packets from the LNS that contain sequence numbers. The **no** version restores the default, which causes the router to check the sequence numbers in data packets that it receives on L2TP tunnels.



NOTE: If you are using IP reassembly, we recommend that you set up the router to ignore sequence numbers in received data packets. Because IP reassembly may reorder L2TP packets, out-of-order packets may be dropped if sequence numbers are being used on L2TP data packets.

Mode Global Configuration

l2tp ignore-transmit-address-change

Syntax [no] l2tp ignore-transmit-address-change [ip-address | udp-port]

Release Information Command introduced before JUNOS Release 7.1.0.
ip-address and **udp-port** keywords added in JUNOS Release 7.1.0.

Description Specifies that E Series routers ignore address changes in Start-Control-Connection-Reply (SCCRP) control packets received from the remote endpoint. If you do not include a keyword, the router ignores the entire address change. The **no** version restores the default, which causes the router to accept address changes in response to SCCRP packets.

- Options**
- ip-address—Ignores only IP address changes
 - udp-port—Ignores only UDP port number changes

Mode Global Configuration

l2tp policy

Syntax `l2tp policy { input | output } policyName [statistics
 { enabled | disabled } [merge]`

`no l2tp policy { input | output }`

Release Information Command introduced before JUNOS Release 7.1.0.
merge keyword added in JUNOS Release 7.2.0.

Description Assigns an L2TP policy list to a profile, which then assigns the policy to an interface. If you enter the **l2tp policy** command and the policy list does not exist, the router creates a policy list with no rules, the default. Attaching this policy list to an interface filters all packets on that interface. You must specify the **input** or **output** keyword to assign the policy list to the ingress or egress of the interface. The **no** version removes the association between a policy list and a profile.

- Options**
- **input**—Applies policy to data arriving at the interface
 - **output**—Applies policy to data leaving the interface
 - ***policyName***—Name of the policy; maximum of 40 characters
 - **statistics**—Enables or disables collection of policy routing statistics
 - **enabled**—Enables collection of policy routing statistics
 - **disabled**—Disables collection of policy routing statistics
 - **merge**—Enables merging of multiple policies to form a single policy

Mode Profile Configuration

Related Topics ■ Setting a Statistics Baseline for Policies

l2tp policy-list

Syntax [no] l2tp policy-list [*policyName*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates or modifies an L2TP policy list. If you enter an **l2tp policy-list** command and type **exit**, the router creates a policy list with no rules. When a policy list does not have rules, the router inserts a default filter rule. Attaching this policy list to an interface filters all packets on that interface. The **no** version removes a policy list.

Options ■ *policyName*—Name of the policy list

Mode Global Configuration

Related Topics ■ Creating Policy Lists for L2TP

l2tp policy-parameter hierarchical

Syntax l2tp policy-parameter hierarchical *parameterName* { *nodeValue* | atm | atm-vc | atm-vp *vpValue* | ethernet | fr-vc | forwarding | svlan *svlanValue* | vlan }

no policy-parameter *parameterName*

Release Information Command introduced in JUNOS Release 8.0.0.

Description Specifies a parameter value for L2TP interfaces. The **no** version removes the policy parameter and its contents.

- Options**
- *parameterName*—Name of policy parameter
 - *nodeValue*—Aggregation node number in the range 1–65535
 - *vpValue*—ATM VPI number in the range 0–255
 - *svlanValue*—SVLAN ID number in the range 0–4095

Mode Interface Configuration

Related Topics

- Creating a Classifier Group for a Policy List

l2tp policy-parameter reference-rate

Syntax l2tp policy-parameter reference-rate *parameterName* [increase] *value*
 no l2tp policy-parameter reference-rate *parameterName*

Release Information Command introduced in JUNOS Release 8.1.0.

Description Creates an L2TP policy parameter for a reference rate; creates a global parameter if it does not exist. The **no** version removes the policy parameter and its contents; if used with the **increase** keyword, decreases the value.

- Options**
- *parameterName*—Name of policy parameter up to 40 characters
 - increase—Increments the existing reference rate value
 - *value*—Value of the reference rate parameter, in the range 0–4292967295

Mode Profile Configuration

- Related Topics**
- Creating a Classifier Group for a Policy List

l2tp reject-transmit-address-change

Syntax [no] l2tp reject-transmit-address-change [ip-address | udp-port]

Release Information Command introduced in JUNOS Release 7.1.0.

Description Specifies that E Series routers reject address changes in Start-Control-Connection-Reply (SCCRP) control packets received from the remote endpoint. If you do not include a keyword, the router rejects the entire address change. The **no** version restores the default, which causes the router to accept address changes in response to SCCRP packets.

- Options**
- ip-address—Rejects only IP address changes
 - udp-port—Rejects only UDP port number changes

Mode Global Configuration

l2tp retransmission

Syntax l2tp retransmission *retries* [established | not-established]
 no l2tp retransmission [*retries*] [established | not-established]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the number of retransmission retries, and allows you to apply the retry count to established and/or unestablished tunnels. If you do not include a keyword, the router applies the retry count to all tunnels. The **no** version resets the number of retransmissions to the default value, 5.

- Options**
- *retries*—Number in the range 2–30
 - *established*—Applies the retry count only to established tunnels
 - *not-established*—Applies the retry count only to tunnels that are not established

Mode Global Configuration

l2tp rx-connect-speed-when-equal

Syntax [no] l2tp rx-connect-speed-when-equal

Release Information Command introduced before JUNOS Release 7.1.0.

Description Generates the L2TP receive (RX) speed AVP when the RX and TX speeds are equal. The **no** version disables generation of the RX speed AVP when the RX and TX speeds are equal.

Mode Global Configuration

l2tp shutdown

Syntax [no] l2tp shutdown

Release Information Command introduced before JUNOS Release 7.1.0.

Description Closes all destinations, tunnels, and sessions and prevents the creation of new destinations, tunnels, and sessions for the router. This command works in conjunction with the **l2tp drain** command. Both commands affect the status of the administrative state of L2TP on the router; the **l2tp shutdown** command sets the administrative state to disabled. The **no** version enables the creation of new destinations, tunnels, and sessions for the router.

Mode Global Configuration

l2tp shutdown destination

Syntax [no] l2tp shutdown destination { *destinationName* |
[virtual-router *vrName*] ip *ipAddress* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Closes all tunnels and sessions at a destination, and prevents the creation of new tunnels and sessions at that destination. This command works in conjunction with the **l2tp drain destination** command. Both commands affect the status of the administrative state of L2TP on the destination; the **l2tp shutdown destination** command sets the administrative state to disabled. The **no** version enables the creation of new tunnels and sessions at that destination.

- Options**
- *destinationName*—Name the router assigns to the LNS
 - *vrName*—Name of the virtual router on which the destination exists
 - *ipAddress*—IP address of the LNS

Mode Global Configuration

l2tp shutdown session

Syntax [no] l2tp shutdown session { *destinationName* |
[virtual-router *vrName*] ip *ipAddress* *sessionName* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Closes a specific session. The **no** version has no effect because all L2TP sessions are dynamic and cannot be restarted after they have been shut down.

- Options**
- *destinationName*—Name that the router assigns to the LNS
 - *vrName*—Name of the virtual router on which the destination exists
 - *ipAddress*—IP address of the LNS
 - *sessionName*—Name of the session

Mode Global Configuration

l2tp shutdown tunnel

Syntax [no] l2tp shutdown tunnel { *destinationName* |
[virtual-router *vrName*] ip *ipAddress* *tunnelName* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Closes all sessions in a tunnel, and prevents the creation of new sessions in that tunnel. This command works in conjunction with the **l2tp drain tunnel** command. Both commands affect the status of the administrative state of L2TP on the tunnel; the **l2tp shutdown tunnel** command sets the administrative state to disabled. The **no** version enables the creation of new sessions in that tunnel.

- Options**
- *destinationName*—Name the router assigns to the LNS
 - *vrName*—Name of the virtual router on which the tunnel exists
 - *ipAddress*—IP address of the LNS
 - *tunnelName*—Name of the tunnel

Mode Global Configuration

l2tp switch-profile

Syntax [no] l2tp switch-profile *profileName*

Release Information Command introduced in JUNOS Release 7.2.0.

Description Creates and names an L2TP tunnel switch profile. This command accesses L2TP Tunnel Switch Profile Configuration mode, from which you can define the L2TP tunnel switching behavior for the interfaces to which this profile is assigned. The **no** version removes the named tunnel switch profile from the router.

Options ■ *profileName*—Name of the tunnel switch profile; a string of up to 64 alphanumeric characters

Mode Global Configuration

l2tp tunnel default-receive-window

Syntax l2tp tunnel default-receive-window *receiveWindowSize*
 no l2tp tunnel default-receive-window

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the default L2TP receive window size (RWS) for a tunnel on both the LAC and the LNS. The RWS is the number of packets that the peer can transmit without receiving an acknowledgment from the router. This command affects only those tunnels configured on the router after the command is issued; it has no effect on previously configured tunnels. The **no** version restores the default behavior, in which the router chooses the default RWS.

Options ■ *receiveWindowSize*—Default receive window size, in packets; currently, the only supported value is 4

Mode Global Configuration

l2tp tunnel idle-timeout

Syntax l2tp tunnel idle-timeout [*timeOutValue*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the tunnel idle-timeout value. Creates persistent tunnels by setting the value to 0. There is no **no** version.

Options ■ *timeOutValue*—Number in the range 0–86400 seconds

Mode Global Configuration

l2tp tunnel short-drain-timeout

Syntax l2tp tunnel short-drain-timeout [*timeOutValue*]
 no l2tp tunnel short-drain-timeout

Release Information Command introduced in JUNOS Release 7.1.0.

Description Configures the amount of time a disconnected LAC L2TP tunnel waits (the drain timeout) before restarting after a restart request is received. The **no** version restores the default setting.

Options ■ *timeOutValue*—Short drain timeout in seconds, in the range 0–31; default value is 2 seconds

Mode Global Configuration

l2tp tunnel-switching

Syntax [no] l2tp tunnel-switching

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables tunnel switching chassis-wide. The **no** version restores the default, disabling tunnel switching.

Mode Global Configuration

l2tp tunnel test

Syntax l2tp tunnel test *authenticateName* [*tunnelName*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Allows you to force the establishment of a tunnel in order to verify the tunnel configuration and to verify connectivity. There is no **no** version.

- Options**
- *authenticateName*—Authenticate name used to look up tunnel test parameters
 - *tunnelName*—Name of the tunnel to be tested

Mode Privileged Exec

l2tp unlock destination

Syntax l2tp unlock destination { *destinationName* | [virtual-router *vrName*] ip *ipAddress* }

Release Information Command introduced in JUNOS Release 7.2.0.

Description Forces L2TP to immediately unlock the specified L2TP destination and return the destination to the available state. Any remaining lockout time and the lockout test setting (if configured) are not taken into account. There is **no** version.

- Options**
- *destinationName*—Name of the L2TP destination
 - *vrName*—Name of the virtual router on which the destination exists
 - *ipAddress*—IP address of the destination

Mode Privileged Exec (at privilege level 10 or higher)

l2tp unlock-test destination

Syntax l2tp unlock-test destination { *destinationName* |
[virtual-router *vrName*] ip *ipAddress* }

Release Information Command introduced in JUNOS Release 7.2.0.

Description Forces L2TP to disregard any remaining lockout time and immediately begin the lockout test procedure for the specified destination. If lockout testing is not enabled, this command immediately unlocks the destination. There is **no** no version.

- Options**
- *destinationName*—Name of the L2TP destination
 - *vrName*—Name of the virtual router on which the destination exists
 - *ipAddress*—IP address of the destination

Mode Privileged Exec (at privilege level 10 or higher)

l2tp weighted-load-balancing

Syntax [no] l2tp weighted-load-balancing

Release Information Command introduced before JUNOS Release 7.1.0.

Description Allows you to use a weighted load balancing scheme for session distribution. The **no** version restores the default behavior, wherein the session load of a chassis is distributed evenly across all tunnels defined to be at the same preference level.

Mode Global Configuration

l2vpn control-word

Syntax [no | default] l2vpn *l2vpnName* control-word

Release Information Command introduced in JUNOS Release 8.1.0.

Description Indicates that the local preference is to use the control word for the layer 2 packets encapsulated in the MPLS packets that are sent to the remote PE router. The **no** version indicates that the local preference is to not use the control word for the layer 2 packets encapsulated in the MPLS packets that are sent to the remote PE router. The **default** version accepts the preference determined by the interface stack on which the MPLS interface is stacked.

Options ■ *l2vpnName*—Name of the VPWS instance

Mode Global Configuration

Related Topics ■ *Configuring an L2VPN Instance in the JUNOS BGP and MPLS Configuration Guide*

l2vpn encapsulation-type

Syntax `l2vpn l2VpnName encapsulation-type { atm-aal5-vcc | atm-vcc-cell | cisco-hdlc | ethernet | frame-relay | ppp | vlan }`
`no l2vpn l2VpnName`

Release Information Command introduced in JUNOS Release 8.1.0.

Description Creates a VPWS L2VPN instance and configures the encapsulation type for interfaces in that VPWS instance. The **no** version removes the VPWS instance.

- Options**
- *l2VpnName*—Name of the VPWS instance
 - atm-aal5-vcc—Specifies ATM AAL5 VCC encapsulation
 - atm-vcc-cell—Specifies ATM VCC Cell encapsulation
 - cisco-hdlc—Specifies Cisco HDLC encapsulation
 - ethernet—Specifies Ethernet encapsulation
 - frame-relay—Specifies Frame-Relay encapsulation
 - ppp—Specifies PPP encapsulation
 - vlan—Specifies VLAN encapsulation

Mode Global Configuration

Related Topics ■ *Configuring an L2VPN Instance in the JUNOS BGP and MPLS Configuration Guide*

l2vpn local-site-id remote-site-id

Syntax `l2vpn l2VpnName local-site-id localSiteId remote-site-id remoteSiteId`
`no l2vpn l2VpnName`

Release Information Command introduced in JUNOS Release 8.1.0.

Description Configures a layer 2 interface as a member of a VPWS L2VPN by specifying local and remote customer site IDs. The **no** version removes the interface as a member of the VPWS L2VPN.

- Options**
- *l2VpnName*—Name of the VPWS instance
 - *localSiteId*—Numerical identifier for the local site in the VPWS L2VPN, in the range 1–65535
 - *remoteSiteId*—Numerical identifier for the remote site in the VPWS L2VPN, in the range 1–65535

Mode Interface Configuration, Subinterface Configuration

- Related Topics**
- *Configuring Customer-Facing Interfaces in the L2VPN Instance* in the *JUNOS BGP and MPLS Configuration Guide*

l2vpn rd

Syntax `l2vpn l2VpnName rd distinguisher`

Release Information Command introduced in JUNOS Release 8.1.0.

Description Specifies the unique two-part route distinguisher for the VPWS L2VPN instance. Once configured, you cannot change or remove the route distinguisher. There is no **no** version.

- Options**
- *l2VpnName*—Name of the VPWS instance
 - *distinguisher*—Unique two-part identifier of the format *number1:number2* where:
 - *number1*—AS number or an IP address
 - *number2*—Unique integer; 32 bits if *number1* is an AS number; 16 bits if *number1* is an IP address

Mode Global Configuration

Related Topics ■ *Configuring an L2VPN Instance in the JUNOS BGP and MPLS Configuration Guide*

l2vpn route-target

Syntax [no] l2vpn *l2VpnName* route-target { import | export | both } *extendedCommunity*

Release Information Command introduced in JUNOS Release 8.1.0.

Description Creates or adds to a list of VPWS L2VPN extended communities that the router uses to determine which routes are imported by the specified VPWS L2VPN instance. The **no** version removes a route target from the specified list.

- Options**
- *l2VpnName*—Name of the VPWS instance
 - import—Adds the route target to the import list for the specified VPWS instance; the VPWS accepts only routes that have at least one route target that matches a route target in the import list
 - export—Adds the route target to the export list for the specified VPWS instance; all routes advertised from this VPWS are associated with the route targets in the export list; at least one route target in the export list must match a route target in the import list of a VPWS L2VPN receiving the route for the route to be accepted by the VPWS L2VPN.
 - both—Adds the route target to both the import list and export list for the specified VPWS instance; recommended setting for a VPWS instance
 - *extendedCommunity*—Two-part number of the format *number1:number2* that identifies an extended community of VPWS L2VPNs where:
 - *number1*—AS number or an IP address
 - *number2*—Unique integer; 32 bits if *number1* is an AS number; 16 bits if *number1* is an IP address

Mode Global Configuration

Related Topics ■ *Configuring an L2VPN Instance in the JUNOS BGP and MPLS Configuration Guide*

l2vpn sequencing

Syntax [no | default] l2vpn *l2VpnName* sequencing

Release Information Command introduced in JUNOS Release 8.1.0.

Description Specifies that the local preference is to include nonzero sequence numbers with the control word, enabling the remote PE to detect out-of-order packets. This command has no effect if no control word is sent in the packets. The router always accepts zero sequence numbers and checks the order of nonzero sequence numbers of MPLS packets received from the remote PE. Any out of order packets are dropped, regardless of whether sequencing is configured. The **no** version specifies that the sequencing number in the control word is set to zero, instructing the remote PE router to not attempt to detect out-of-order packets; has no effect if no control word is sent in the packets. The **default** version accepts the preference determined by the interface stack on which the MPLS shim interface is stacked.

Options ■ *l2VpnName*—Name of the VPWS instance

Mode Global Configuration

Related Topics ■ *Configuring an L2VPN Instance in the JUNOS BGP and MPLS Configuration Guide*

l2vpn site-name site-id

Syntax [no] l2vpn *l2VpnName* site-name *siteName* site-id *siteId*
 [multi-homed priority *priority*]

Release Information Command introduced in JUNOS Release 8.1.0.
multi-homed priority keywords and *priority* variable added in JUNOS Release 9.3.0.

Description Configures a name and a unique site identifier for a customer site that belongs to the specified VPWS instance. Optionally configures the site to be multihomed. In a VPWS configuration, each customer site is represented by one or more customer edge (CE) devices located at the edge of the customer's network. The **no** version removes the site name and site identifier from the VPWS instance, or removes the multihomed configuration for the customer site and returns it to a single-homed state.

- Options**
- *l2VpnName*—Name of the VPWS instance
 - *siteName*—Name of the site; string of up to 128 alphanumeric characters
 - *siteId*—Numerical identifier for the site, in the range 1–65535; must be unique across the VPWS domain
 - *priority*—Number that sets the priority of this VPWS instance for a multi-homed site, in the range 1–65535; priority is sent in BGP advertisements as the Local-Preference attribute and determines whether the router hosting the VPWS instance becomes the designated VE router for this multihomed site

Mode Global Configuration

Related Topics ■ *Configuring an L2VPN Instance in the JUNOS BGP and MPLS Configuration Guide*

l2vpn site-range

Syntax `l2vpn l2VpnName site-range siteRange`
`no l2vpn l2VpnName site-range`

Release Information Command introduced in JUNOS Release 8.1.0.

Description Configures the maximum number of customer sites that can participate in the specified VPWS L2VPN. In a VPWS L2VPN configuration, each customer site is represented by a customer edge (CE) device located at the edge of the customer's network. The **no** version restores the default site range, 1.

- Options**
- *l2VpnName*—Name of the VPWS instance
 - *siteRange*—Maximum number of sites that can participate in the VPWS domain, in the range 1–65535; default value is 1

Mode Global Configuration

Related Topics

- *Configuring an L2VPN Instance* in the *JUNOS BGP and MPLS Configuration Guide*

lacp

Syntax lacp { active | passive }
no lacp

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures whether an Ethernet link in an IEEE 802.3ad link aggregation group (LAG) bundle participates actively or passively in the Link Aggregation Control Protocol (LACP). LACP controls the transmission of protocol data units (PDUs) to exchange information between partner links in a LAG bundle. By default, Ethernet links do not send LACP PDUs. The **no** version restores the default behavior.

- Options**
- active—Causes the Ethernet link to always transmit LACP PDUs, regardless of whether its partner link is set to active or passive LACP participation
 - passive—Causes the Ethernet link to transmit LACP PDUs only when it receives LACP PDUs from its partner link

Mode Interface Configuration

lacp port-priority

Syntax lacp port-priority *portPriority*
no lacp port-priority

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the priority for an Ethernet member link, also known as an Ethernet port, in an IEEE 802.3ad link aggregation group (LAG) bundle. The member link with the lowest numerical priority value has the highest priority. The Ethernet member link with the highest priority is selected first to join the LAG bundle. The **no** version restores the default priority value, 32768.

Options ■ *portPriority*—Priority value; integer in the range 0–65535; default value is 32768

Mode Interface Configuration

lag dos-protection-group

Syntax lag dos-protection-group *groupName*
 no lag dos-protection-group

Release Information Command introduced in JUNOS Release 8.1.0.

Description Attaches a lag denial of service (DoS) protection group to an interface. The **no** version removes the attachment of the DoS protection group from the interface.

Options ■ *groupName*—Name of the DoS protection group; string of up to 31 alphanumeric characters

Mode Interface Configuration

lease

Syntax `lease { days [hours [minutes [seconds]]] | infinite }`
 `no lease`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the time period for which the supplied IP address is valid. The **no** version restores the default lease time, 30 minutes.



NOTE: Ensure that DHCP clients have a minimum lease of 120 minutes before you begin a unified in-service software upgrade to prevent unwanted lease expirations due to the length of the unified ISSU process.

- Options**
- *days*—Number of days for which the IP address is valid; in the range 0–32768
 - *hours*—Number of hours for which the IP address is valid in the range 0–24
 - *minutes*—Number of minutes for which the IP address is valid; in the range 0–60
 - *seconds*—Number of seconds for which the IP address is valid; in the range 0–60
 - *infinite*—Assigns a lease that does not expire

Mode DHCP Local Pool Configuration

license bfd

Syntax license bfd *licenseKey*
 no license bfd

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the Bidirectional Forwarding Detection (BFD) license provided by your sales representative or Juniper Networks Customer Service. The **no** version disables the license.

Options ■ *licenseKey*—Unique string of up to 15 alphanumeric characters that we provide to you

Mode Global Configuration

license b-ras

Syntax license b-ras *licenseKey*
 no license b-ras

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the B-RAS license provided by your sales representative or Juniper Networks Customer Service. Depending on the license purchased, the router supports up to 2,000, 4,000, 8,000, 16,000, or 20,000 authenticated PPP or SRC sessions. The **no** version disables the license.

Options ■ *licenseKey*—Unique string of up to 15 alphanumeric characters that we provide to you

Mode Global Configuration

license ipsec-tunnels

Syntax license ipsec-tunnels *licenseKey*
 no license ipsec-tunnels

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the IPSec license key provided by your sales representative or Juniper Networks Customer Service. Depending on the license purchased, the router supports up to 5,000, 7,500, or 10,000 tunnels per chassis. The **no** version disables the license.

Options ■ *licenseKey*—Unique string of alphanumeric characters that we provide to you

Mode Global Configuration

license ipv6

Syntax `license ipv6 licenseKey`
`no license ipv6`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the IPv6 license key provided by your sales representative or Juniper Networks Customer Service. The **no** version disables the license.

Options ■ *licenseKey*—Unique string of alphanumeric characters that we provide to you

Mode Global Configuration

license issu

Syntax license issu *licenseKey*
 no license issu

Release Information Command introduced in JUNOS Release 9.2.0.

Description Specifies the unified ISSU license key for the ERX1440 router provided by your sales representative or Juniper Networks Customer Service. No license key is required or available for the E120 and E320 routers. The **no** version disables the license.

Options ■ *licenseKey*—Unique string of alphanumeric characters that we provide to you

Mode Global Configuration

license l2tp-session

Syntax `license l2tp-session licenseKey`
 `no license l2tp-session`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the L2TP license key provided by your sales representative or Juniper Networks Customer Service. You can use the license on ERX1440 routers, E120 routers, and E320 routers to increase the number of supported L2TP sessions from 16,000 to 32,000. The **no** version removes the license.



NOTE: This command is deprecated and might be removed completely in a future release.

JUNOS software no longer requires you to configure a license to enable support for 32,000 L2TP sessions. The ERX1440 routers, E120 routers, and E320 routers support 32,000 L2TP sessions by default; all other models support a maximum of 16,000 L2TP sessions.

Although the **license l2tp-session** command remains in the CLI, the command has no effect on the actual enforced limit.

Options ■ *licenseKey*—Unique string of alphanumeric characters that we provide to you

Mode Global Configuration

license mobile-ip home-agent

Syntax license mobile-ip home-agent *licenseKey*
 no license mobile-ip home-agent

Release Information Command introduced in JUNOS Release 9.0.0.

Description Configures the license key to enable a home agent. The **no** version does not change any existing Mobile IP configurations such as deleting the existing bindings or preventing any new registrations, but disables the license key. You cannot modify, but only delete, the Mobile IP configurations after enabling the **no** version. For example, if you disable the home agent and delete all existing bindings, you cannot re-enable it until a valid license is provided.

Options ■ *licenseKey*—Unique alphanumeric license key, up to a maximum of 16 alphanumeric characters, to enable a Mobile IP home agent configuration

Mode Global Configuration

license nat

Syntax license nat *licenseKey*
 no license nat

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the NAT license key provided by your sales representative or Juniper Networks Customer Service. The **no** version disables the license.

Options ■ *licenseKey*—Unique string of alphanumeric characters that we provide to you

Mode Global Configuration

license service-management

Syntax license service-management *licenseKey*
 no license service-management

Release Information Command introduced in JUNOS Release 7.2.0.

Description Specifies the Service Manager license key provided by your sales representative or Juniper Networks Customer Service. The **no** version removes the license.

Options ■ *licenseKey*—Unique string of alphanumeric characters that Juniper Networks provides to you

Mode Global Configuration

lifetime

Syntax To set an IKE lifetime:

lifetime *seconds*

no lifetime

To set an IPSec transport profile lifetime:

lifetime { kilobytes *lowKilobytes highKilobytes* | seconds *txLowSeconds txHighSeconds*
| seconds *txLowSeconds txHighSeconds* kilobytes *lowKilobytes highKilobytes* }

no lifetime

To set an IPSec tunnel profile lifetime:

lifetime { seconds *tunLowSeconds tunHighSeconds* | kilobytes *lowKilobytes*
highKilobytes | seconds *tunLowSeconds tunHighSeconds* kilobytes *lowKilobytes*
highKilobytes }

no lifetime

Release Information Command introduced before JUNOS Release 7.1.0.
IPSec Tunnel Profile Configuration mode added in JUNOS Release 7.3.0.

Description From IKE Policy Configuration mode, associates a lifetime with IKE SAs established with this IKE policy. The **no** version restores the lifetime to its default, 28800 seconds (8 hours).

From IPSec Transport Profile Configuration mode, sets a lifetime range for the IPSec connection in volume of traffic and/or in seconds. If the client PC offers a lifetime within this range, the router accepts the offer. The **no** version returns the lifetime to the default, 100000–4294967295 KB and 900–86400 seconds (1–24 hours).

From IPSec Tunnel Profile Configuration mode, specifies the IPSec lifetime range used on IPSec security association negotiations. The **no** version returns the lifetime to its default, 28800 seconds (8 hours) and no traffic volume limit.

- Options**
- *seconds*—Number of seconds an SA lives before expiring; in the range 900–86400 seconds
 - *lowKilobytes*—Lower range of the lifetime in kilobytes; in the range 100000–4294967295 KB; default value is 100000
 - *highKilobytes*—Higher range of the lifetime in kilobytes; in the range 100000–4294967295 KB; default value is 4294967295
 - *txLowSeconds*—Lower range of the lifetime in seconds; in the range 300–86400 seconds; default value is 3600

- *txHighSeconds*—Higher range of the lifetime in seconds; in the range 300–86400 seconds; default value is 86400
- *tunLowSeconds*—Lower range of the lifetime in seconds; in the range 900–86400 seconds; default value is 3600
- *tunHighSeconds*—Higher range of the lifetime in seconds; in the range 900–86400 seconds; default value is 86400
- *lowKilobytes*—Lower range of the lifetime in kilobytes; in the range 100000–4294967295 KB; default value is 100000
- *highKilobytes*—Higher range of the lifetime in kilobytes; in the range 100000–4294967295 KB; default value is 4294967295

Mode IKE Policy Configuration, IPSec Transport Profile Configuration, IPSec Tunnel Profile Configuration

line

Syntax `line { console lineNumber | vty lineRangeStart [lineRangeEnd] }`
 `no line vty lineNumber`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Opens virtual terminal lines or the console line and allows you to configure the lines. By default five vty lines (0–4) are open. The **no** version removes a vty line or a range of lines from your configuration; users will not be able to run Telnet, SSH, or FTP to lines that you remove. When you remove a vty line, the router removes all lines above that line. For example, **no line vty 6** causes the router to remove lines 6 through 29. You cannot remove lines 0 through 4.



NOTE: Once lines are open, login is enabled by default. Before users can access the lines, you must configure a password, disable login using the **no login** command, or configure AAA authentication on the line.

- Options**
- `console`—Specifies the console line
 - `vtty`—Specifies vty lines
 - `lineNumber`—Number of a single line; 0 for the console line
 - `lineRangeStart`—Start of the vty line range; a number from 0–29
 - `lineRangeEnd`—End of the vty line range; a number from 0–29

Mode Global Configuration

link

Syntax link *poolName*
 no link

Release Information Command introduced before JUNOS Release 7.1.0.

Description Links the pool currently being configured to another DHCP local address pool. The linked pool acts as a backup pool. The **no** version removes the link.

Options ■ *poolName*—Name of pool to which you want to link the pool currently being configured

Mode DHCP Local Pool Configuration

link failover arp-flush

Syntax [no] link failover arp-flush

Release Information Command introduced in JUNOS Release 10.3.0.

Description Clears the ARP cache on an interface with redundant ports when the primary link fails. The **no** version maintains the ARP entries on the interface.

Mode Interface Configuration

link failover force

Syntax link failover force

Release Information Command introduced before JUNOS Release 7.1.0.

Description Forces a GE I/O module to switch from one port to another. There is no **no** version.

Mode Interface Configuration

link failover timeout

Syntax link failover timeout *failTime*
no link failover timeout

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the time that the router waits for a port on a GE I/O module to become active before the router switches to the redundant port. The **no** version restores the default setting, in which the router sets this time automatically.

Options ■ *failTime*—Time that the router waits; in the range 100–10000 ms

Mode Interface Configuration

link selection

Syntax link selection { primary | secondary }
no link selection

Release Information Command introduced before JUNOS Release 7.1.0.

Description Disables redundancy on a GE I/O module by allowing operation on the specified port only. The **no** version restores the default situation, in which port redundancy is enabled.

- Options**
- primary—Allows operation on only the primary port
 - secondary—Allows operation on only the redundant port

Mode Interface Configuration

list

Syntax list [*index*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Lists the currently configured MPLS explicit path (optionally starting at a particular index). There is no **no** version.

Options ■ *index*—Number of a node in an ordered set of abstract nodes set with the **index** command; in the range 1–255

Mode Explicit Path Configuration

load-interval

Syntax load-interval *timeInterval*

no load-interval

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the time interval at which the router calculates bit rates and packet rates for an interface. The **no** version restores the default value, 300 seconds. This command is not available for the Ethernet interface on the SRP module.

Options ■ *timeInterval*—Multiple of 30 seconds; in the range 30–300

Mode Interface Configuration

load-rebalance

Syntax [no] load-rebalance [period *rebalancePeriod* start-threshold *rebalanceStartThreshold* [percent | subscribers] stop-threshold *rebalanceStopThreshold* [percent | subscribers] maximum-improvement *rebalanceMaximumImprovement* [percent | subscribers]]

Release Information Command introduced in JUNOS Release 8.1.0.

Description Configures the QoS algorithm for rebalancing the links in an 802.3ad link aggregation group (LAG). To configure the algorithm to dynamically rebalance the LAG using existing parameters, issue the **load-rebalance** command without any keywords. The **no** version restores the default parameters.

- Options**
- *rebalancePeriod*—Time period for rebalancing in seconds; in the range 0–86400; the default is 60 seconds
 - *rebalanceStartThreshold*—Amount of imbalance in the LAG that triggers the algorithm to start rebalancing; the default is 0 percent
 - percent—Specifies that the threshold is measured as a percentage of the average load per link; in the range 0–100
 - subscribers—Specifies that the threshold is measured by the number of subscribers away from the average subscriber count per link in the LAG; in the range 0–100000
 - *rebalanceStopThreshold*—Amount of imbalance in the LAG that triggers the algorithm to stop rebalancing; the default is 0 percent
 - percent—Specifies that the amount of imbalance is measured as a percentage of the average load per link; in the range 0–100
 - subscribers—Specifies that the threshold is measured by the number of subscribers away from the average subscriber count link in the LAG; in the range 0–100000
 - *rebalanceMaximumImprovement*—Maximum number of links in the LAG to rebalance; the default is 100 percent
 - percent—Specifies that the maximum number of links is measured as a percentage of the total links; in the range 0–100
 - subscribers—Specifies that the maximum number of links is measured by the number of subscribers; in the range 0–100000

Mode Interface Configuration

Related Topics ■ Configuring Load Rebalancing for 802.3ad Link Aggregation Groups

local host

Syntax local host *hostname*

no local host

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures an L2TP local hostname to be used with a remote host. The **no** version removes the local hostname from use with a remote host.

Options ■ *hostname*—L2TP local hostname; string of up to 64 characters (no spaces)

Mode L2TP Destination Profile Host Configuration

local-interface

Syntax `local-interface { interfaceType interfaceSpecifier | ipAddress ipAddressMask }`
 `no local-interface`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Maps a domain name to a loopback interface. The **no** version deletes the mapping to the user domain name.



NOTE: In Domain Map Configuration mode, this command is replacing the deprecated **loopback** command for mapping a domain name to a loopback interface. The **loopback** command may be removed completely from the Domain Map Configuration mode in a future release.

- Options**
- *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *ipAddress*—IP address of the loopback interface
 - *ipAddressMask*—IP address mask of the loopback interface

Mode Domain Map Configuration

local ip address

Syntax From L2TP Destination Profile Host Configuration mode:

local ip address *ipAddress*

no local ip address

From IPsec Transport Profile Configuration mode:

[no] local ip address *transportIpAddress*

From IPsec Tunnel Profile Configuration mode:

local ip address *transportIpAddress* { pre-share *keyString*
| pre-share-masked *maskedKeyString* }

no local ip address

Release Information Command introduced before JUNOS Release 7.1.0.
IPsec Tunnel Profile Configuration mode added in JUNOS Release 7.3.0.

Description From L2TP Destination Profile Host Configuration mode, configures a local IP address for use with a remote host. The **no** version removes the local IP address from use with a remote host.

From IPsec Transport Profile Configuration mode, specifies the local endpoint of the IPsec transport connection. It also enters Local IPsec Transport Profile Configuration mode. The **no** version deletes the local IP address.

From IPsec Tunnel Profile Configuration mode, specifies the given local IP address as a server address. The router continues to monitor UDP port 500 for incoming user login requests (that is, IKE source address negotiations). When using global preshared keys, consider the following points:

- Global preshared keys enable a group of users to share a single authentication key. Using a shared key for a group of users simplifies the administrative job of setting up keys. However, changing or removing a preshared key for one user (for security reasons) affects other users with the same key.
- Specific keys for individual users take precedence over global keys assigned to the same user. In other words, if a user has both an assigned specific key and a global key that user must use the specific key or authentication fails.
- Avoid specifying the same local endpoint and virtual router in the same profile. Local endpoint and virtual router values override each other. The last value set in the profile is the value used.

The **no** version causes the router to stop monitoring UDP port 500 for user requests and removes any preshared key associations with the local IP address.

- Options**
- *ipAddress*—IP address used in packets sent to the LAC
 - *transportIpAddress*—Local endpoint for the IPSec transport connection
 - *keyString*—Key value in ASCII format
 - *maskedKeyString*—Key value in ascii format
- Mode** IPSec Transport Profile Configuration, IPSec Tunnel Profile Configuration, L2TP Destination Profile Host Configuration

local ip identity

Syntax local ip identity
 { address *ipAddress* | range *ipRangeLow* *ipRangeHigh* | subnet *netAddress* *netMask* }
 no local ip identity

Release Information Command introduced in JUNOS Release 7.3.0.

Description Overrides the local identity (phase 2 identity) used for IPSec security association negotiations. For IPSec negotiations to succeed, the local and peer identities at one end of the tunnel must match the peer and local identities at the other end (respectively). The **no** version restores the default value, wildcard network value 0.0.0.0/0.

- Options**
- *ipAddress*—IP address used as the local identity for IPSec security association negotiations
 - *ipRangeLow*—Low end of a range used as the local identity for IPSec security association negotiations
 - *ipRangeHigh*—High end of a range used as the local identity for IPSec security association negotiations
 - *netAddress*—IP network address used as the local identity for IPSec security association negotiations
 - *netMask*—IP network mask used as the local identity for IPSec security association negotiations

Mode IPSec Tunnel Profile Configuration

local ip network

Syntax local ip network *ipNetwork ipMask*
no local ip network

Release Information Command introduced in JUNOS Release 7.3.0.

Description Specifies networks that are reachable through the IPSec tunnel. You can configure up to 16 networks for this method of “split-tunneling.” The **no** version removes the specified network from the reachable list.

- Options**
- *ipNetwork*—IP network reachable through the secure connection
 - *ipMask*—IPv4 subnetwork mask for the IP network

Mode IPSec Tunnel Profile Configuration

log

Syntax [no] [suspend] log

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a IP policy rule that configures logging settings for packets that match the current classifier control list. The **no** version removes a log rule from a policy list; the **suspend** keyword temporarily suspends the rule; the **no suspend** version resumes application of a suspended rule.



NOTE: This command replaces the Policy List Configuration version of the **log** command, which may be removed completely in a future release.

Mode Classifier Group Configuration

Related Topics ■ Policy Rule Precedence

log-adjacency-changes

Syntax For IS-IS adjacencies:

```
log-adjacency-changes [ severity { severityValue | severityNumber } ]
[ verbosity verbosityLevel ]
```

```
no log-adjacency-changes
```

For OSPFv3 adjacencies:

```
[ no ] log-adjacency-changes [ severity { severityValue | severityNumber } ]
[ verbosity verbosityLevel ]
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description Generates a log message when the state of an IS-IS adjacency or an OSPFv3 neighbor changes. For OSPFv2 neighbors, use the `ospf log-adjacency-changes` command. Manipulates the same log as the Global Configuration **log** commands. The **no** version disables this function.

- Options**
- **severity**—Sets minimum severity of the log messages for this category; described either by a descriptive term—*severityValue*—or by a corresponding number—*severityNumber*—in the range 0–7. The lower the number, the higher the priority:
 - *emergency or 0*—System unusable
 - *alert or 1*—Immediate action needed
 - *critical or 2*—Critical condition exists
 - *error or 3*—Error condition
 - *warning or 4*—Warning condition
 - *notice or 5*—Normal but significant condition
 - *info or 6*—Informational message
 - *debug or 7*—Debug message
 - **verbosity**—Specifies the verbosity of this log category's messages
 - **verbosityLevel**—Specifies the verbosity of the log category's messages; can be any of the following:
 - *high*—Verbose
 - *low*—Terse
 - *medium*—Moderate detail

Mode Router Configuration

log destination

Syntax To specify the destination and severity of messages logged:

```
log destination { console | nv-file | syslog ipAddress [ facility facilityId ] }
{ severity { severityValue | severityNumber } | off }
```

```
no log destination [ console | nv-file | syslog [ ipAddress ] ]
```

To specify which event categories are logged to syslog:

```
log destination syslog ipAddress { include | exclude } category [ category ]*
```

```
no log destination syslog ipAddress { include | exclude } [ category ]*
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the logging of system messages. You can direct messages to a destination, limit the messages logged based on severity level, or limit the event categories for which messages are logged. The **no** versions restore default settings or reverse the effect of previous commands that limited event categories.



NOTE: You can display traffic logs—such as ipTraffic, icmpTraffic, tcpTraffic, and udpTraffic—only via the show log data command or from the *SRP module* console. You cannot redirect traffic logs elsewhere, such as to a system log or nonvolatile storage file, or to a Telnet session.

- Options**
- console—Configures or modifies logging to the local console
 - nv-file—Configures or modifies logging to the nonvolatile log file; the nv-file can accept only events at a severity level of critical or higher in importance
 - syslog—Configures or modifies logging to a system log server
 - *ipAddress*—IP address of the system log application on a remote host
 - facility—Specifies the system log facility on the host
 - *facilityId*—Number in the range 0–7 that identifies the corresponding logging facility, local0–local7
 - severity—Sets minimum severity of the log messages displayed; described either by a descriptive term—*severityValue*—or by a corresponding number—*severityNumber*—in the range 0–7. The lower the number, the higher the priority:
 - emergency or 0—System unusable
 - alert or 1—Immediate action needed
 - critical or 2—Critical condition exists

- *error or 3*—Error condition
- *warning or 4*—Warning condition
- *notice or 5*—Normal but significant condition
- *info or 6*—Informational message
- *debug or 7*—Debug message
- *off*—Disables logging to this destination
- *include*—Sends only the specified event categories to the system log server
- *exclude*—Sends all event categories except those specified to the system log server

Issuing an **include** command after an **exclude** command (or vice versa) overrides the earlier command.

You can issue successive **include** commands or successive **exclude** commands. Successive commands expand the list of included or excluded categories.

- *category*—Log category; refer to the CLI online Help for available options
- ***—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

log destination syslog source

Syntax log destination syslog *ipAddress* source *interfaceType* *interfaceSpecifier*
 no log destination syslog *ipAddress* source [*interfaceType* *interfaceSpecifier*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a source interface type and location for events logged to a system log server. Overrides the type and location of the actual source to enable server access behind firewalls. The **no** version restores the default state, which is to use the actual interface type and location of the source.

- Options**
- *ipAddress*—IP address of the system log application
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Global Configuration

log engineering

Syntax [no] log engineering

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables engineering logs. The **no** version disables engineering logs.

Mode Global Configuration

log fields

Syntax log fields { timestamp | no-timestamp } { instance | no-instance }
 { calling-task | no-calling-task }

 no log fields

Release Information Command introduced before JUNOS Release 7.1.0.

Description Selects optional fields to be added to all logs. The **no** version disables the optional log fields.

- Options**
- timestamp—Includes the timestamp in log messages
 - no-timestamp—Does not include the timestamp in log messages
 - instance—Includes the event ID in log messages
 - no-instance—Does not include the event ID in log messages
 - calling-task—Includes the logging task name in log messages
 - no-calling-task—Does not include the logging task name in log messages

Mode Global Configuration

log filters

Syntax no log filters

Description This command has only a **no** version. See the no log filters command for a complete description.

Mode Global Configuration

log here

Syntax [no] log here

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the current terminal as a log console. The **no** version disables logs destined for a console from being displayed on the current terminal.

Mode Global Configuration, Privileged Exec, User Exec

log severity

Syntax log severity { *severityValue* | off | *severityNumber* }
 [*eventCategory* [*instanceTree*] | *eventCategory* *instanceTree* | *eventCategory*]

no log severity [*severityValue* | off | *severityNumber*] [*eventCategory*
 [*filters* | *instanceTree*] | *eventCategory* { *filters* | *instanceTree* } | *eventCategory* | *]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the severity level for systemwide logs (that is, when no individual event category is specified) or for a specific event category. The **no** version returns severity changes to their default settings or the systemwide setting.



NOTE: After you change the log severity level for an individual log event category, you cannot use systemwide commands to subsequently change the severity level for that category. To change individually altered log event categories using systemwide commands, you must first change the log event back to its default setting.

- Options**
- *severityValue* and *severityNumber*—Minimum severity of the log messages displayed for the selected category; described either by a descriptive term—*severityValue*—or by a corresponding number—*severityNumber*—in the range 0–7. The lower the number, the higher the priority:
 - emergency or 0—System unusable
 - alert or 1—Immediate action needed
 - critical or 2—Critical condition exists
 - error or 3—Error condition
 - warning or 4—Warning condition
 - notice or 5—Normal but significant condition
 - info or 6—Informational message
 - debug or 7—Debug message
 - off—Disables systemwide log severity for all default level event categories when no event category is specified or disables log severity for a specified event category
 - *eventCategory*—Log category; refer to the CLI online Help for available options
 - *filters*—Removes all log filters for the event category
 - *instanceTree*—Log-specific filter parameters; refer to the CLI online Help for available options
 - *—Resets all log severities, systemwide and individual, to default settings

Mode Global Configuration

log unlimited

Syntax [no] log unlimited [*eventCategory*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Removes the limit on the number of outstanding buffers for an event category. The **no** version returns the number of buffers to the default value.

Options ■ *eventCategory*—Log category; refer to the CLI online Help for available options

Mode Global Configuration, Privileged Exec, User Exec

log verbosity

Syntax log verbosity *verbosityLevel* [*eventCategory*]

no log verbosity [*verbosityLevel*] [*eventCategory*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the verbosity level for a selected category. The **no** version returns the log verbosity to the default value, low.

- Options**
- *verbosityLevel*—Verbosity for the log category:
 - low—Terse (default)
 - medium—Moderate detail
 - high—Verbose
 - *eventCategory*—Log category; refer to the CLI online Help for available options

Mode Global Configuration

login

Syntax [no] login

Release Information Command introduced before JUNOS Release 7.1.0.

Description Requires you to log in with a password. The **no** version removes the password requirement and allows connections without a password.



NOTE: If you issue this command when no password has been configured, access to Telnet is refused.

Mode Line Configuration

login authentication

Syntax login authentication *authListName*
 no login authentication

Release Information Command introduced before JUNOS Release 7.1.0.

Description Applies an AAA authentication list to the vty sessions that you specified for AAA authentication. The **no** version removes all authentication methods, which means the router accepts Telnet sessions without challenge.

Options ■ *authListName*—Authentication list name of up to 32 characters

Mode Line Configuration

logout subscribers

Syntax logout subscribers { all | domain *domainName* | icr-partition *icrPartitionId* | port *interfaceSpecifier* | username *userName* | virtual-router *vrName* }

Release Information Command introduced before JUNOS Release 7.1.0.
icr-partition keyword and *icrPartitionLocationId* variable added in JUNOS Release 10.3.0

Description Logs out the authenticated PPP or DHCP local server users. Also, logs out subscribers based on the ICR partition ID. There is no **no** version.

- Options**
- all—Logs out all PPP or DHCP local server sessions.
 - *domainName*—Active PPP or DHCP local server session whose usernames have that domain name.
 - icr-partition—Logs out subscribers based on the location ID of the partition in the ICR cluster.
 - *icrPartitionLocationID*—A unique identifier for each ICR partition on a chassis; a maximum of 128 characters. Note that this ID different from the partition ID, which is configured using the **ip vrrp vrid icr-partition partitionId** command. The partition location ID that you specify here is a combination of the interface within the chassis on which the ICR partition is configured and the VRRP ID, which is system-defined and nonconfigurable.
 - *interfaceSpecifier*—Location of the port with active PPP subscribers; format varies according to interface type; see “Interface Types and Specifiers” on page 5.
 - *userName*—Active PPP or DHCP local server session whose names match the username.
 - *vrName*—Active PPP or DHCP local server session whose interfaces are bound to a specific virtual router.

Mode Privileged Exec

loopback

Syntax For module controllers, the options available vary depending on the module being configured.

CT3 module:

loopback { local | network | payload }

no loopback

[no] loopback remote

cOCx/STMx SONET controller (SONET/SDH section layer), OCx/STMx line modules:

loopback { local | network }

no loopback

COCX-F3 module:

loopback { local | network | payload }

no loopback

For interfaces; the options available vary depending on the interface being configured.

ATM interface (cannot be used on a subinterface):

loopback { diagnostic | line }

no loopback

POS interface:

[no] loopback { internal | line }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the loopback mode for a module controller or interface. The **no** version clears all loopback on the module or interface (the default), or deletes the mapping to the user domain name.



NOTE: In Domain Map Configuration mode, this command has been replaced by the **local-interface** command and may be removed completely from Domain Map Configuration mode in a future release.

- Options**
- **local**—Loops the data back toward the router; on supported line modules also sends an alarm indication signal (AIS) out toward the network.
 - **network payload**—Loops the data toward the network after the framer has processed the data.
 - **network line**—Loops the data toward the network before the data reaches the framer.
 - **remote**—Sends a signal notifying the device at the remote end to activate or deactivate the line loopback.
 - **network**—Loops the data toward the network before the data reaches the framer.
 - **payload**—Loops the data toward the network after the framer has processed the data.
 - **diagnostic**—Places the interface into internal loopback
 - **line**—ATM interface: places the interface into external loopback; POS interface: connects the received network signal directly to the transmit network signal. When configured in line loopback mode, the router never receives data from the network.
 - **internal**—Connects the local transmitted signal to the local received signal

Mode Controller Configuration, Interface Configuration

lsp-gen-interval

Syntax `lsp-gen-interval [level-1 | level-2] seconds`
 `no lsp-gen-interval [level-1 | level-2]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the minimum interval at which originated IS-IS link-state packets are generated on a per LSP basis. The **no** version restores the default value, 5 seconds.

- Options**
- `level-1`—Sets interval for level 1 only
 - `level-2`—Sets interval for level 2 only
 - `seconds`—Number in the range 0–120; the minimum interval in seconds; default value is 5 seconds

Mode Router Configuration

lsp-mtu

Syntax `lsp-mtu bytes`
`no lsp-mtu`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the maximum size of an IS-IS link-state packet generated by the software. The **no** version restores the default value, 1497 bytes.

Options ■ *bytes*—Number in the range 128–9180; the MTU size in bytes; default value is 1497

Mode Router Configuration

lsp-refresh-interval

Syntax `lsp-refresh-interval seconds`
`no lsp-refresh-interval`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the link-state packet rate at which locally generated IS-IS link-state packets are periodically transmitted. The **no** version restores the default value, 900.

Options ■ *seconds*—Number in the range 1–65535; the refresh interval in seconds; default value is 900

Mode Router Configuration

Chapter 13

M Commands

macro

Syntax macro [test | verbose] { *fileName*.mac [*macroName* [*arg*]*] |
name *macroName* [*arg*]* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Executes a macro file, which can consist of one or more macros. If you do not use the *macroName* option to specify a macro, the command searches in the specified macro file for a macro named “ start,” and returns an error if the “ start” macro is not found. If you do not specify *fileName*.mac, you must specify **name** *macroName*; the command then searches only in local memory for a file called *macroName*.mac that contains the *macroName* macro. There is no **no** version.

- Options**
- test—Displays the output of the macro without issuing the commands to the router, and displays comments
 - verbose—Echoes each command as the macro executes and displays comments
 - *fileName*—Name of the file containing the macro; requires the .mac extension
 - *macroName*—Name of a macro within the macro file
 - *arg*—Zero or more arguments passed to the macro; if the argument contains a space or other special character, the argument must be enclosed within double quotation marks
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode All modes

map-class frame-relay

Syntax [no] map-class frame-relay *mapName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates a map class. Command is used when configuring Frame Relay end-to-end fragmentation and reassembly. The **no** version removes the map-class.

Options ■ *mapName*—Name of the map class; use up to 64 characters

Mode Global Configuration

map-group

Syntax [no] map-group *name*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Associates a map list to an NBMA interface when configuring static mapping. The **no** version removes the association. Use in conjunction with the **map-list** command.

Options ■ *name*—Name of the map group

Mode Interface Configuration

map-list

Syntax [no] map-list *name*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates a map list for an NBMA interface when configuring static mapping. The **no** version removes the map list. Use in conjunction with the **map-group** command.

Options ■ *name*—Name of the map list; a string of up to 31 characters

Mode Map List Configuration

mark

Syntax For IPv4:

```
[ no ] [ suspend ] mark { tosByteValue mask maskValue |
  tos-precedence tosPrecNum | tos tosNum | dsfield dsFieldNum }
  profile colorMarkProfileName }
```

For IPv6:

```
[ no ] [ suspend ] mark { tcByteValue mask tcMaskValue | tc-precedence
  tcPrecNum | tcfield tcFieldNum | dsfield dsFieldNum } profile
  colorMarkProfileName }
```

Release Information Command introduced before JUNOS Release 7.1.0.
colorMarkProfileName variable added in JUNOS Release 7.2.0.

Description Sets the precedence field of the ToS byte (for IPv4) or traffic class byte (for IPv6) in the IP header to a specified value for packets that match the current classifier control list. This command is not tied to a rate limit profile, but marks packets based on a classifier control list. The **no** version removes the mark rule from the policy list; the **suspend** version temporarily suspends the mark rule; the **no suspend** version resumes application of a suspended rule.



NOTE: This command replaces the Policy List Configuration mode version of the **mark** command, which may be removed completely in a future release.

- Options**
- *tosByteValue*—ToS byte value to be assigned to packets; in the range 0–255
 - *maskValue*—Mask to be used when applying ToS byte values to packets; in the range 1–255
 - *tosPrecNum*—ToS precedence value to be assigned to packets; in the range 0–7
 - *tosNum*—ToS value to be assigned to packets; in the range 0–255
 - *dsFieldNum*—DS field value to be assigned to packets; in the range 0–63
 - *colorMarkProfileName*—Name of the color-mark profile (up to 40 alphanumeric characters)
 - *tcByteValue*—Traffic class field value to be assigned to packets; in the range 0–255
 - *tcMaskValue*—Mask to be used when applying traffic class field values to packets; in the range 1–255
 - *tcPrecNum*—Traffic class field precedence value to be assigned to packets; in the range 0–7
 - *tcFieldNum*—Traffic class field value to be assigned to packets; in the range 0–255

Mode Classifier Group Configuration

Related Topics ■ Policy Rule Precedence

mark-clp

Syntax [no] [suspend] mark-clp *clpValue*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Marks the CLP bit in the ATM header of packets matching the current classifier control list. The **no** version removes the mark rule from a policy list; the **suspend** version temporarily suspends a mark rule; the **no suspend** version resumes application of a suspended rule.

Options ■ *clpValue*—Value of the CLP bit, 0 or 1

Mode Classifier Group Configuration

Related Topics ■ Assigning Values to the ATM CLP Bit
■ Policy Rule Precedence

mark-de

Syntax [no] [suspend] mark-de *deValue*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Marks the DE bit in the Frame Relay header of packets matching the current classifier control list. The **no** version removes the mark rule from a policy list; the **suspend** version temporarily suspends a mark rule; the **no suspend** version resumes application of a suspended rule.



NOTE: This command replaces the Policy List Configuration version of the **mark-de** command, which may be removed completely in a future release.

Options ■ *deValue*—Value of the DE bit; 0 or 1

Mode Classifier Group Configuration

Related Topics ■ Assigning Values to the ATM CLP Bit
 ■ Policy Rule Precedence

mark-exp

Syntax [no] [suspend] mark-exp *expValue* [mask *expMask*] [profile *ProfileName*]

Release Information Command introduced before JUNOS Release 7.1.0.
profileName variable added in JUNOS Release 7.2.0.

Description Defines an MPLS policy rule that specifies the value of the EXP bits. The **no** version removes the rule from the policy list; the **suspend** version temporarily suspends the policy rule; the **no suspend** version resumes application of a suspended rule.



NOTE: This command replaces the Policy List Configuration version of the **mark-exp** command, which may be removed completely in a future release.

- Options**
- *expValue*—EXP bit value assigned to packets; number in the range 0–7
 - *expMask*—Mask applied to modify some of the EXP bits in IP packet; integer in the range 1–7
 - *profileName*—Name of the rate-limit profile to be used in a policy (up to 40 alphanumeric characters)

Mode Classifier Group Configuration

- Related Topics**
- Assigning Values to the ATM CLP Bit
 - Policy Rule Precedence

mark-user-priority

Syntax [no] [suspend] mark-user-priority *userPriorityValue*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines a policy rule that specifies the value of the 802.1p VLAN user priority bits. The **no** version removes the rule from the policy list; the **suspend** version temporarily suspends the policy rule; the **no suspend** version resumes application of a suspended rule.



NOTE: This command replaces the Policy List Configuration version of the **mark-user-priority** command, which may be removed completely in a future release.

Options ■ *userPriorityValue*—EXP bit value assigned to packets; number in the range 0–7

Mode Classifier List Configuration

Related Topics ■ Policy Rule Precedence

mask destination

Syntax mask destination *destinationMinimumSize*
 no mask destination

Release Information Command introduced in JUNOS Release 8.1.0.

Description Sets the minimum mask size for the destination address for the prefix and destination prefix aggregation caches. The **no** version restores the default mask size.

Options ■ *destinationMinimumSize*—Mask number in the range 1—32; default is 0

Mode Flow Cache Configuration

masked-key

Syntax masked-key *encryptedKey*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the encrypted form of the preshared key that the router uses in IKE negotiations. Once you enter a preshared key, the router encrypts the key and displays it in masked form to increase the security of the key. If you need to reenter the key, you can enter it in its masked form using this command. There is no **no** version. To delete a key, use the **no** version of the **ipsec key manual** command.

Options ■ *encryptedKey*—Encrypted key value; to obtain this value, enter the unencrypted key using the **key** command in IPsec Manual Key Configuration mode, and then display the masked version of the key with the **show configuration** command

Mode IPsec Manual Key Configuration

mask source

Syntax mask source *sourceMinimumSize*
 no mask source

Release Information Command introduced in JUNOS Release 8.1.0.

Description Sets the minimum mask size for the source address for the prefix and source prefix aggregation caches. The **no** version restores the default mask size.

Options ■ *sourceMinimumSize*—Mask number in the range 1—32; default is 0

Mode Flow Cache Configuration

mask-val

Syntax [no] mask-val *value*

Release Information Command introduced before JUNOS Release 7.1.0.
Color Mark Profile Configuration mode added in JUNOS Release 7.2.0.

Description Sets the mask value. For rate limits, use this command with the **committed-action**, **conformed-action**, and **exceeded-action** commands. For color-mark profiles, use the **mask-val** command in Color Mark Profile Configuration mode. The **no** version restores the default value, 255.

- Options**
- *value*—Mask value in the range 0–255. Use the following mask values to set the appropriate bits in the ToS field of the IP packet header:
 - IP Precedence—0xE0 (three most significant bits)
 - DS Field—0xFC (six significant bits)
 - TOS (IP) or Traffic Class field (IPv6)—0xFF (default)

Mode Color Mark Profile Configuration, Rate Limit Profile Configuration

- Related Topics**
- Creating a Two-Rate Rate-Limit Profile
 - Setting the Mask Value for MPLS Rate-Limit Profiles
 - Setting the Mask Value for IP and IPv6 Rate-Limit Profiles

match as-path

Syntax match as-path *listName* [*listName*]*
 no match as-path [*listName*]*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Matches a BGP AS path access list. The **no** version removes the match clause from a route map unless you specify a value, in which case only that value is removed from the match clause.

- Options** ■ *listName*—Name of an AS path access list; string of up to 32 characters
- *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Policy List Configuration, Route Map Configuration

match community

Syntax match community *listName* [*listName*]* [exact-match]
 no match community [*listName*]* [exact-match]

Release Information Command introduced before JUNOS Release 7.1.0. match distance

Description Matches a BGP community list. The **no** version removes the match clause from a route map unless you specify a value, in which case only that value is removed from the match clause.

- Options**
- *listName*—String of up to 32 characters that designates a community list; you can optionally use a regular expression to specify the listName
 - exact-match—Limits the match to a route that contains only the communities contained in the specified list; cannot be used with a community list specified by a regular expression
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Policy List Configuration, Route Map Configuration

match distance

Syntax match distance *distance* [*distance*]*
 no match distance [*distance*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Matches any routes that have the specified administrative distance. The **no** version removes the match clause from a route map unless you specify a value, in which case only that value is removed from the match clause.



NOTE: Matching a distance is useful only when applied to a route being redistributed out of a routing table. Distance is used to determine the relative preference between routes to the same prefix in order to pick the best route to that prefix in the routing table. Distance has no meaning in any other circumstance and any attempt to match distance will fail.

- Options**
- *distance*—Administrative distance in the range 0–255
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Policy List Configuration, Route Map Configuration

match extcommunity

Syntax match extcommunity *listName* [*listName*]* [exact-match]
 no match extcommunity [*listName*]*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Matches a BGP extcommunity list. The **no** version removes the match clause from a route map unless you specify a value, in which case only that value is removed from the match clause.

- Options**
- *listName*—Name of the extended-community list
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line
 - exact-match—Limits the match to a route that contains only the extended communities contained in the specified list; cannot be used with an extended community list specified by a regular expression

Mode Policy List Configuration, Route Map Configuration

match ip address

Syntax match ip address { *accessListName* [*accessListName*]* |
 prefix-list *prefixListName* [*prefixListName*]* | prefix-tree *treeName* [*treeName*]* }
 no match ip address [*accessListName*]* | prefix-list [*prefixListName*]* |
 prefix-tree [*treeName*]*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Matches any routes that have a destination network number address that is permitted by a standard or extended access list, a prefix list, or a prefix tree, or performs policy routing on packets. You cannot mix references in the same match command; you can only specify either access list(s), prefix list(s), or prefix tree(s). The **no** version removes the match clause from a route map unless you specify a value, in which case only that value is removed from the match clause.

- Options**
- *accessListName*—String of up to 32 alphanumeric characters
 - *prefixListName*—Name of a single prefix list; string of up to 32 characters
 - *treeName*—Name of a single prefix tree; string of up to 32 characters
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Policy List Configuration, Route Map Configuration

match ip next-hop

Syntax match ip next-hop { *accessListName* [*accessListName*]* |
 prefix-list *prefixListName* [*prefixListName*]* | prefix-tree *treeName* [*treeName*]* }
 no match ip next-hop [*accessListNumber*]* | prefix-list [*listName*]* |
 prefix-tree [*treeName*]*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Matches any routes that have a next-hop router address passed by the specified access list, prefix list, or prefix tree. You cannot mix references in the same match command; you can only specify either access list(s), prefix list(s), or prefix tree(s). The **no** version removes the match clause from a route map unless you specify a value, in which case only that value is removed from the match clause.

- Options**
- *accessListName*—Name of a single standard access list; string of up to 32 characters
 - *prefixListName*—Name of a single prefix list; string of up to 32 characters
 - *treeName*—Name of a single prefix tree; string of up to 32 characters
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Policy List Configuration, Route Map Configuration

match ipv6 address

Syntax match ipv6 address
 { *accessListName* [*accessListName*]* | prefix-list *prefixListName*
 [*prefixListName*]* }
 no match ipv6 address [[*accessListName*]* | prefix-list [*prefixListName*]*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Matches any routes that have a destination network number address that is permitted by an access list or prefix list. The **no** version removes all address match clauses from a route map unless you specify either an access list or a prefix list, in which case only the list match is removed from the route map.

- Options**
- *accessListName*—String of up to 32 alphanumeric characters
 - *prefixListName*—Name of a single prefix list; string of up to 32 characters
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Policy List Configuration, Route Map Configuration

match ipv6 next-hop

Syntax match ipv6 next-hop
 { *accessListName* [*accessListName*]* | prefix-list *prefixListName*
 [*prefixListName*]* }
 no match ipv6 next-hop [[*accessListName*]* | prefix-list [*prefixListName*]*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Matches any routes that have a next-hop router address passed by the specified access list or prefix list. The **no** version removes all next-hop match clauses from a route map unless you specify either an access list or prefix list, in which case only the list match is removed from the route map.

- Options**
- *accessListName*—String of up to 32 alphanumeric characters
 - *prefixListName*—Name of a single prefix list; string of up to 32 characters
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Policy List Configuration, Route Map Configuration

match ipv6 route-source

Syntax match ipv6 route-source *prefixListName* [*prefixListName*]*
 no match ipv6 route-source [*prefixListName*]*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Matches any routes that are advertised from addresses contained in the specified prefix list. The **no** version removes all route-source match clauses from a route map unless you specify a prefix list, in which case only that prefix list match is removed from the route map.

- Options** ■ *prefixListName*—Name of a single prefix list; string of up to 32 characters
- *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Policy List Configuration, Route Map Configuration

match level

Syntax match level { backbone | level-1 | level-1-2 | level-2 | stub-area } *
 no match level [backbone | level-1 | level-1-2 | level-2 | stub-area]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Matches import routes for the specified type. The **no** version removes the match clause from a route map unless you specify a value, in which case only that value is removed from the match clause.

- Options**
- backbone—Specifies OSPF backbone area
 - level-1—Specifies Level 1 area
 - level-1-2—Specifies Level 1 and a level 2 area
 - level-2—Specifies Level 2 subdomain
 - stub-area—Specifies OSPF NSSA area
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Policy List Configuration, Route Map Configuration

match metric

Syntax match metric *metricValue* [*metricValue*]*
 no match metric [*metricValue*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Matches a route for the specified metric value. The **no** version removes the match clause from a route map unless you specify a value, in which case only that value is removed from the match clause.

- Options**
- *metricValue*—Number in the range 0–4294967295, which indicates the preference value for a specific route in a route map
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Policy List Configuration, Route Map Configuration

match metric-type

Syntax match metric-type { external | internal }
 no match metric-type [external | internal]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Matches routes having the specified metric type. The **no** version removes the match clause from a route map.

- Options** ■ external—Specifies IS-IS external metric type
 ■ internal—Specifies IS-IS internal metric type

Mode Policy List Configuration, Route Map Configuration

match mpls-label

Syntax [no] match mpls-label

Release Information Command introduced in JUNOS Release 7.1.0.

Description Matches on MPLS-labeled routes. By including this command in the appropriate route map (export, global export, global import route map), you can restrict importing or exporting to only labeled or only unlabeled routes. The **no** version removes the configuration.

Mode Route Map Configuration

match policy-list

Syntax match policy-list *listname* [*listName*]*
 no match policy-list [*listName*]*

Release Information Command introduced before JUNOS Release 7.1.0.

Description References a policy list having the specified name. The **no** version removes the match clause from a route map.

- Options**
- *listName*—Name of a policy list; string of up to 32 characters
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Route Map Configuration

match route-type

Syntax

```
match route-type internal [ intra | inter ] [ level-1 | level-2 ]
[ external [ type-1 | type-2 ] ] [ level-1 | level-2 ]*
```

```
match route-type external [ type-1 | type-2 ] [ level-1 | level-2 ]
[ internal [ intra | inter ] ] [ level-1 | level-2 ]*
```

```
match route-type { level-1 | level-2 } [ internal [ intra | inter ] ]
[level-1 | level-2 ] [ external [ type-1 | type-2 ] ] [ level-1 | level-2 ]*
```

```
match route-type { level-1 | level-2 } [ external [ type-1 | type-2 ] ]
[ level-1 | level-2 ] [ internal [ intra | inter ] ] [ level-1 | level-2 ]*
```

```
no match route-type [ internal [ intra | inter ] | external [ type-1 | type-2 ] |
level-1 | level-2 ]
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description Matches routes of the specified type. The **no** version removes the match clause from a route map unless you specify a value, in which case only that value is removed from the match clause.

- Options**
- **internal**—Specifies internal routes
 - **intra**—OSPF intra-area routes
 - **inter**—OSPF interarea routes
 - **external**—Specifies external routes
 - **type-1**—OSPF type 1 external routes
 - **type-2**—OSPF type 2 external routes
 - **level-1**—Specifies IS-IS level 1 routes
 - **level-2**—Specifies IS-IS level 2 routes
 - *****—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Policy List Configuration, Route Map Configuration

match-set summary prefix-tree

Syntax match-set summary prefix-tree *treeName*
no match-set summary prefix-tree

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets condition for a route map that matches routes based on the network base address set in the specified prefix tree and summarizes them by preserving only the bits set in the prefix tree. The **no** version disables the use of the prefix tree by the route map.

Options ■ *treeName*—Name of the prefix tree

Mode Route Map Configuration

match tag

Syntax match tag *tagValue* [*tagValue*]*
 no match tag [*tagValue*]*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Matches the tag value of the destination routing protocol. The **no** version removes the match clause from a route map unless you specify a value, in which case only that value is removed from the match clause.

- Options**
- *tagValue*—Number in the range 0–4294967295
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Policy List Configuration, Route Map Configuration

max-branches

Syntax [no] max-branches *maxBranches*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the maximum number of branches the ANCP neighbor can have. The **no** version returns the maximum number of branches to its default value (unlimited branches).

Options ■ *maxBranches*—Maximum number of branches allowed for the ANCP neighbor in the range 1–64000

Mode L2C Neighbor Configuration

max-discovery-table-entries

Syntax max-discovery-table-entries *maxEntries*
 no max-discovery-table-entries

Release Information Command introduced in JUNOS Release 7.2.0.

Description Specifies the maximum number of discovery table entries the ANCP neighbor can have. The **no** version returns the maximum number of table entries to its default value, 10,000 entries.

Options ■ *maxEntries*—Maximum number of discovery table entries allowed for the ANCP neighbor in the range 1–64000

Mode L2C Neighbor Configuration

maximum-paths

Syntax For BGP:

maximum-paths [ibgp | eibgp] *maxPaths*

no maximum-paths [ibgp | eibgp] [*maxPaths*]

For IS-IS and RIP:

maximum-paths *maxPaths*

no maximum-paths

For OSPF:

maximum-paths *maxPaths*

no maximum-paths *maxPaths*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Controls the maximum number of equal-cost paths to the same destination that BGP, IS-IS, OSPF, or RIP can install in the routing table to support ECMP.

For BGP and RIP, issue the command from Router Configuration mode to apply the value to routes in the global RIB. In Address Family Configuration mode, issue the command only in the context of IPv4 unicast and IPv6 unicast address families to apply the value only to routes in the global RIB or the specific VRF for the IPv4 unicast or IPv6 unicast address family; This command is not supported for VPNv4 or VPNv6 address families.

For IS-IS or OSPF, issue the command from Router Configuration mode.

The **no** version restores the default value, 1 path for BGP or 4 paths for IS-IS, OSPF, and RIP.

- Options**
- **ibgp**—Specifies that the *maxPaths* value applies only to routes received from internal (IBGP) peers; if no keyword is specified, the *maxPaths* value applies only to routes received from external (EBGP) peers
 - **eibgp**—Specifies that the *maxPaths* value applies to routes received from IBGP and EBGP peers; can be used only for VRF IPv4 unicast and IPv6 unicast address families
 - ***maxPaths***—Maximum number of parallel paths (routes) in the range 1–16

Mode Address Family Configuration, Router Configuration

maximum routes

Syntax maximum routes *limit* { *warningThreshold* | warning-only }
 no maximum routes

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets a warning threshold and maximum limit for routes imported by a PE router into a VRF from associated CE routers. The **no** version removes the limit and warning threshold.

- Options**
- *limit*—Number in the range 1–4294967295 that when exceeded prevents routes from being imported into the routing table; when first exceeded generates a limit-exceeded log entry; if the route count fluctuates below and up to this value, an interval of five minutes must pass before another limit-exceeded log entry can be generated
 - *warningThreshold*—Percentage in the range 1–100 that when first exceeded generates a warning-threshold-exceeded log entry; if the route count fluctuates around this value, an interval of five minutes must pass before another warning-threshold-exceeded log entry can be generated
 - warning-only—Causes the *limit* to function as a *warningThreshold*; specifies that exceeding the *limit* generates a warning-threshold-exceeded log entry instead of a limit-exceeded log entry and permits routes exceeding the *limit* to be added to the routing table; if the route count fluctuates around the *limit*, an interval of five minutes must pass before another warning-threshold-exceeded log entry can be generated

Mode VRF Configuration

maximum-voql

Syntax maximum-voql *maximumVoqlValue*
 no maximum-voql

Release Information Command introduced in JUNOS Release 8.0.0.

Description Specifies a maximum value for the virtual output queue length (VOQL) for all simple shared shapers on the router. The VOQL tracks the amount of data over queued between simple shared-shaper rate periods. The **no** version removes the specified maximum VOQL value from all simple shared shapers on the router.

Options ■ *maximumVoqlValue*—Maximum value for the VOQL in the range 0–10000; default value is 4000

Mode QoS Shared Shaper Control Configuration

Related Topics ■ Configuring Simple Shared Shaper Algorithm Variables

max-interfaces

Syntax For Tunnel Server Configuration mode:

max-interfaces { *maxInterfacesValue* | all-available }

no max-interfaces

For IPsec Tunnel Profile Configuration mode:

max-interfaces *maxInterfacesValue*

no max-interfaces

Release Information Command introduced before JUNOS Release 7.1.0.
IPsec Tunnel Profile Configuration mode added in JUNOS Release 7.3.0.

Description For Tunnel Server Configuration mode, provisions the maximum number of tunnel-service interfaces to be used on a tunnel-server port. The **default** version restores the default configuration. On dedicated tunnel-server ports, the default configuration is **all-available** (the maximum number of tunnel-service interfaces that the tunnel-service module supports). On shared tunnel-server ports, the default configuration is zero tunnel-service interfaces provisioned. The **no** version unprovisions the tunnel-server port by reducing the number of provisioned tunnel-service interfaces to zero.

For IPsec Tunnel Profile Configuration mode, defines the maximum number of interfaces that the IPsec tunnel profile can instantiate. The **no** version returns the maximum value to zero (0) to indicate no limit to the number of interfaces that can be instantiated on this profile.

- Options**
- *maxInterfacesValue*—For Tunnel Server configuration, the maximum number of tunnel-service interfaces that can be provisioned on a tunnel-server port in the range 0–16000; For IPsec Tunnel Profile configuration, the maximum number of interfaces that the IPsec tunnel profile can instantiate in the range 0–32767
 - all-available—Specifies that the maximum number of tunnel-service interfaces that can be provisioned on a tunnel-server port matches the maximum number supported by the tunnel-server module

Mode IPsec Tunnel Profile Configuration, Tunnel Server Configuration

max-lsp-lifetime

Syntax max-lsp-lifetime *seconds*
 no max-lsp-lifetime

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the maximum time that IS-IS link-state packets persist without being refreshed. The **no** version restores the default time.

Options ■ *seconds*—Number in the range 1–65535; the lifetime of LSP in seconds; default value is 1200 seconds

Mode Router Configuration

max-response-failure

Syntax max-response-failure *maxFailureValue*

no max-response-failure

Release Information Command introduced before JUNOS Release 7.1.0.

Description Terminates a test when the *maxFailureValue* is reached. That is, when there is no response to a designated number of operation requests, the test is terminated. This feature applies only to pathEcho entries. The **no** version restores the default value, five consecutive failures.

Options ■ *maxFailureValue*—Number of operation requests not responded to; 0 turns this feature off; default value is 5

Mode RTR Configuration

max-sessions

Syntax For RADIUS:

max-sessions *sessionLimit*

no max-sessions

For AAA domain map and tunnel group tunnels:

max-sessions *maxSessionsPerTunnel*

{ no | default } max-sessions

For L2TP:

max-sessions *maxSessionsPerProfile*

{ no | default } max-sessions

Release Information Command introduced before JUNOS Release 7.1.0.

Description For RADIUS, specifies the number of outstanding requests to a server. The **no** version reverts to the default value.

For AAA domain map, and tunnel group tunnels, sets the maximum sessions per tunnel. The **no** version disables the feature. The **default** version sets the value to zero.

For L2TP, sets the maximum sessions allowed for destination and host profiles by the LNS. The **no** and **default** versions disable the feature.

- Options**
- *sessionLimit*—Maximum number of outstanding requests to a specific server in the range from 10 through to the maximum value; default value is 255
For information about the number of concurrent RADIUS requests that the router supports for authentication and accounting servers, see *JUNOS Release Notes, Appendix A, System Maximums*.
 - *maxSessionsPerTunnel*—Maximum number of sessions that can be configured on a tunnel in the range 0–4294967295; default value is zero
 - *maxSessionsPerProfile*—Maximum number of sessions that can be established at the LNS for a destination or host profile; in the range from 1 through to a maximum of the chassis-wide limit; default value is the chassis-wide limit
For information about the maximum number of L2TP sessions supported per chassis, see *JUNOS Release Notes, Appendix A, System Maximums*.

Mode Domain Map Tunnel Configuration, L2TP Destination Profile Configuration, L2TP Destination Profile Host Configuration, RADIUS Configuration, Tunnel Group Tunnel Configuration

mdl carrier

Syntax [no] mdl carrier

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies that a T3 interface is used in the carrier environment. The **no** version restores the default situation, in which an interface does not operate in the carrier environment.

Mode Controller Configuration

mdl string

Syntax `mdl string { eic eicValue | fic ficValue | lic licValue | unit unitValue | pfi pfiCode |
port portValue | generator genValue }`

`no mdl string { eic | fic | lic | unit | pfi | port | generator }`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Allows you to specify an MDL message on a T3 interface as defined in the ANSI T1.107a-1990 specification. The **no** version restores the default value to the specified MDL message or to all MDL messages.

- Options**
- *eicValue*—Equipment identification code; 1–10 characters; default value is the null value.
 - *ficValue*—Frame identification code; 1–10 characters; default value is the null value.
 - *licValue*—Line identification code; 1–11 characters; default value is the null value.
 - *unitValue*—Unit identification code; 1–6 characters; default value is the null value.
 - *pfiCode*—Facility identification code to send in the MDL path message; 1–38 characters; default value is the null value.
 - *portValue*—Equipment port number to send in the MDL idle signal message; 1–38 characters; default value is the null value.
 - *genValue*—Generator number to send in the MDL test signal message; 1–38 characters; default value is the null value.

Mode Controller Configuration

mdl transmit

Syntax [no] mdl transmit { path-id | idle-signal | test signal }
no mdl transmit

Release Information Command introduced before JUNOS Release 7.1.0.

Description Transmits an MDL message from a T3 interface. The **no** version disables transmission of the specified MDL message or all MDL messages.

- Options**
- path-id—Transmits a path identification message every second; default value is disabled
 - idle-signal—Transmits an idle signal message every second; default value is disabled
 - test-signal—Transmits a test signal message every second; default value is disabled

Mode Controller Configuration

mdt-data-delay

Syntax mdt-data-delay *timeout*
 no mdt-data-delay

Release Information Command introduced in JUNOS Release 8.2.0.

Description Configures a timeout before switching to data MDT. The **no** version returns to the default.

Options ■ *timeout*—Timeout value measured in 0.1 seconds in the range 1-255 seconds; the default is 30

Mode IP PIM Data MDT Configuration

mdt-data-holddown

Syntax mdt-data-holddown *timeout*
 no mdt-data-holddown

Release Information Command introduced in JUNOS Release 8.2.0.

Description Configures the time in seconds before switching back to the default MDT group from the data MDT group. The **no** version returns to the default.

Options ■ *timeout*—Time before switching back to the default MDT group, in the range 1–300 seconds; the default is 60

Mode IP PIM Data MDT Configuration

mdt-data-timeout

Syntax mdt-data-timeout *timeout*
 no mdt-data-timeout

Release Information Command introduced in JUNOS Release 8.2.0.

Description Configures the time in seconds before leaving the data MDT group. The **no** version returns to the default.

Options ■ *timeout*—Time before leaving the data MDT group, in the range 1–1200 seconds; the default is 180

Mode IP PIM Data MDT Configuration

mdt-interval

Syntax mdt-interval *time*
 no mdt-interval

Release Information Command introduced in JUNOS Release 8.2.0.

Description Configures the time in seconds between successive MLD join TLVs. The **no** version returns to the default.

Options ■ *time*—Time between successive MLD join TLV in the range 1–300 seconds; the default is 60

Mode IP PIM Data MDT Configuration

medium ipv4

Syntax medium ipv4
 no medium

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the medium type of a tunnel to IPv4 (the only medium type currently supported). The **no** version restores the default value, ipv4.

Mode Domain Map Tunnel Configuration, Tunnel Group Tunnel Configuration

member interface

Syntax [no] member interface *interfaceType* *interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Adds a member VLAN or S-VLAN subinterface to a Martini layer 2 circuit associated with a load-balancing group. This command creates an MPLS shim interface and associates it with the group. The **no** version removes the member subinterface from the circuit. Repeat as needed to remove all member subinterfaces used by a load-balanced circuit, thereby deleting the circuit from the group.

- Options**
- *interfaceType*—One of the following interface types listed in Interface Types and Specifiers on page 5
 - serial
 - pos
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode L2 Transport Load-Balancing-Circuit Configuration

Related Topics

- *Configuring CE-Side Load Balancing for Martini Layer 2 Transport* in the *JUNOS BGP and MPLS Configuration Guide*

member-interface

Syntax [no] member-interface *interfaceType interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Adds a member interface, also known as a bundle member, to an MLPPP bundle, an MLFR bundle, or an IEEE 802.3ad link aggregation group (LAG) bundle. The **no** version removes the specified member interface from the bundle.

- Options**
- *interfaceType*—One of the following interface types listed in Interface Types and Specifiers on page 5
 - serial (MLFR bundle or MLPPP bundle)
 - pos (MLFR bundle only)
 - fastEthernet (IEEE 802.3ad LAG bundle only)
 - gigabitEthernet (IEEE 802.3ad LAG bundle only)
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Interface Configuration, Subinterface Configuration

member-interface-type

Syntax member-interface-type {vlan | atm-vc | ip}
 no member-interface-type

Release Information Command introduced in JUNOS Release 9.2.0.

Description Configures the member-interface type for a QoS interface set. The **no** version removes the member-interface type from the parameter definition.

- Options** ■ vlan—Specifies the member-interface-type as VLAN
 ■ atm-vc—Specifies the member-interface-type as VLAN
 ■ ip—Specifies the member-interface-type as VLAN

Mode QoS Interface Set Configuration

Related Topics ■ Configuring Interface Sets for QoS

memory

Syntax [no] memory warning *highUtilization abatedUtilization*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures memory warning parameters. When the router reaches the high memory utilization value, it sends warning messages. When memory usage falls to the abated memory utilization value, the router stops sending warning messages. The **no** version returns the memory warning parameters to the default values.

- Options**
- *highUtilization*—High memory utilization value; in the range 1–99; default value is 85
 - *abatedUtilization*—Abated memory utilization value; in the range 1–99; default value is 75

Mode Global Configuration

message-digest-key md5

Syntax message-digest-key *keyID* md5 [0 | 8] *msgDigestKey*
 no message-digest-key *keyID*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables OSPF MD5 authentication for the remote-neighbor interface and configures the MD5 key. The **no** version deletes an MD5 key.



NOTE: If all the MD5 keys have been deleted, the authentication type is still MD5, but you need to configure MD5 keys.

To disable MD5 authentication for the remote-neighbor interface, use the **authentication-none** command.

- Options**
- *keyID*—Key identifier in the range 1–255
 - md5—Specifies use of the MD5 algorithm
 - 0—Indicates the *msgDigestKey* is entered in unencrypted form (plaintext); this is the default option
 - 8—Indicates the *msgDigestKey* is entered in encrypted form (ciphertext)
 - *msgDigestKey*—OSPF password; string of up to 16 alphanumeric characters

Mode Remote Neighbor Configuration

metric

Syntax `metric globalDefault [level-1 | level-2]`
`no metric [level-1 | level-2]`

Release Information Command introduced in JUNOS Release 9.0.0.

Description Sets the metric to the same value for all active IS-IS IPv4 and IPv6 interfaces at the specified level. If you do not specify level 1 routers or level 2 routers, then the metric is applied to both level 1 and level 2 routers. The **no** version restores the individual default value, 10.

- Options**
- *globalDefault*—Metric used for all IS-IS interfaces; a number in the range 1–16777215; overridden by the **isis metric** command
 - *level-1*—Configuration applies only to level 1 routing
 - *level-2*—Configuration applies only to level 2 routing

Mode Router Configuration

metric-style narrow

Syntax [no] metric-style narrow [transition] [level-1 | level-2 | level-1-2]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the router to generate and accept only old-style IS-IS TLVs with narrow (six-bit) metric fields. If you issue this command, the value configured with the **isis metric** command can range only from 0–63. The **no** version restores the default value, which is to generate and accept only old-style TLVs with narrow (six-bit) metric fields.

- Options**
- transition—Configures the router to additionally accept new-style TLVs with wider metric fields
 - level-1—Configuration applies only to level 1 routing
 - level-2—Configuration applies only to level 2 routing
 - level-1-2—Configuration applies to both level 1 and level 2 routing

Mode Router Configuration

metric-style transition

Syntax [no] metric-style transition [level-1 | level-2 | level-1-2]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the router to generate and accept both old-style IS-IS TLVs with narrow (six-bit) metric fields and new-style IS-IS TLVs with wider metric fields. If you issue this command, the value configured with the **isis metric** command can range from 0–16777215. The **no** version restores the default value, which is to generate and accept only old-style TLVs with narrow (six-bit) metric fields.

- Options**
- level-1—Configuration applies only to level 1 routing
 - level-2—Configuration applies only to level 2 routing
 - level-1-2—Configuration applies to both level 1 and level 2 routing

Mode Router Configuration

metric-style wide

Syntax [no] metric-style wide [transition] [level-1 | level-2 | level-1-2]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the router to generate and accept only new-style IS-IS TLVs with wider metric fields. If you issue this command, the value configured with the **isis metric** command can range from 0–16777215. The **no** version restores the default value, which is to generate and accept only old-style TLVs with narrow (six-bit) metric fields.

- Options**
- transition—Configures the router to additionally accept old-style TLVs with narrow (six-bit) metric fields
 - level-1—Configuration applies only to level 1 routing
 - level-2—Configuration applies only to level 2 routing
 - level-1-2—Configuration applies to both level 1 and level 2 routing

Mode Router Configuration

minimum-dynamic-rate-percent

Syntax minimum-dynamic-rate-percent *minimumDynamicRatePercent*
 no minimum-dynamic-rate-percent

Release Information Command introduced in JUNOS Release 8.0.0.

Description Specifies the minimum value of the dynamic shaping rate as a percentage of the shared shaping rate for all simple shared shapers on the router. The **no** version removes the specified minimum dynamic rate from all simple shared shapers on the router.

Options ■ *minimumDynamicRatePercent*—Minimum percentage value of the dynamic shared shaper in the range 0–100; default value is 0

Mode QoS Shared Shaper Control Configuration

Related Topics ■ Configuring Simple Shared Shaper Algorithm Variables

minimum-links

Syntax minimum-links *minimumLinkValue*
 no minimum-links

Release Information Command introduced in JUNOS Release 10.0.0.

Description Configures the minimum number of member links in the link aggregation group (LAG) bundle that must be in the Collecting/Distributing state for the LAG interface to be considered up. The **no** version resets the minimum number of member links to the default value.

Options ■ *minimumLinkValue*—Minimum number of links in the LAG bundle in the range 1-8 (8 is the maximum number of member links per LAG bundle); default value is 1.

Mode Interface Configuration

Related Topics ■ *Configuring 802.3ad Link Aggregation and Link Redundancy* in the *JUNOS Link Layer Configuration Guide*

mirror

Syntax To mirror a specified trigger type:

```
mirror triggerType [hex] triggerValue { ip | ipv6 | l2tp } secure-policy-list policyName
```

```
no mirror triggerType [hex] triggerValue { ip | ipv6 | l2tp }
```

To mirror the agent-circuit-id or agent-remote-id trigger types, when the hex variant is used:

```
mirror triggerType hex triggerValue { ip | ipv6 | l2tp } secure-policy-list policyName
```

```
no mirror triggerType hex triggerValue { ip | ipv6 | l2tp }
```

To mirror the dhcp-option-82 trigger type:

```
mirror dhcp-option-82 agent-circuit-id triggerValue1 agent-remote-id triggerValue2  
ip secure-policy-list policyName
```

```
no mirror dhcp-option-82 agent-circuit-id triggerValue1 agent-remote-id triggerValue2  
ip
```

To mirror the dhcp-option-82 trigger type, when the hex variant is used:

```
mirror dhcp-option-82 hex triggerValue ip secure-policy-list policyName
```

```
no mirror dhcp-option-82 hex triggerValue ip
```

Release Information Command introduced before JUNOS Release 7.1.0.
nas-port-id keyword added in JUNOS Release 7.1.0.
 IPv6 support added in JUNOS Release 10.1.0.
hex keyword added in JUNOS Release 11.1.0.

Description Enables packet mirroring based on the specified trigger and specifies the secure policy to attach to the subscriber's interface. The **no** version disables packet mirroring for the subscriber and removes the trigger configuration.



NOTE: The hex variant is applicable only for agent-circuit-id, agent-remote-id, and dhcp-option-82 trigger types. If the hex variant is used then the *triggerValue* must be a hexadecimal number.

- Options**
- *triggerType*—One of the following RADIUS attributes
 - acct-session-id—Acct-Session-Id, RADIUS attribute [44]
 - agent-circuit-id—Agent Circuit ID, RADIUS attribute [26–1], Vendor ID 3561

- `agent-remote-id`—Agent Remote ID, RADIUS attribute [26–2], Vendor ID 3561
- `calling-station-id`—Calling-Station-Id, RADIUS attribute [31]
- `dhcp-option-82`—DHCP Option 82, RADIUS attribute [26–159], Vendor ID 4874
- `ip-address`—Framed-IP-Address, RADIUS attribute [8]; associated with the virtual router where the command is issued, RADIUS VSA [26-1]
- `nas-port-id`—NAS-Port-Id, RADIUS attribute [87]
- `username`—User-Name, RADIUS attribute [1]; associated with the virtual router where the command is issued, RADIUS VSA [26-1]
- *triggerValue*—Value of the *triggerType* (the specified RADIUS attribute) that identifies the subscriber
- `ip`—Configures mirroring for an IP subscriber
- `ipv6`—Configures mirroring for an IPv6 subscriber
- `l2tp`—Configures mirroring for an L2TP subscriber
- *policyName*—Secure policy to attach to the subscriber's interface

Mode Global Configuration

Related Topics ■ Configuring CLI-Based Mirroring

mirror analyzer-ip-address

Syntax mirror analyzer-ip-address *analyzerIpAddress* analyzer-virtual-router *vrName*
 [analyzer-udp-port *udpPort* [mirror-identifier *mirrorId*
 [session-identifier *sessionId*]]]
 no mirror

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the mirror action for a classifier group in a secure IP or L2TP policy list. The **no** version deletes the mirror rule.

- Options**
- *analyzerIpAddress*—IP address of the analyzer
 - *vrName*—Name of the virtual router where the analyzer interface is configured
 - *udpPort*—UDP port of the analyzer; required for L2TP packet mirror rules
 - *mirrorId*—Mirror identifier
 - *sessionId*—Session identifier

Mode Classifier-Group Configuration

- Related Topics**
- Configuring CLI-Based Mirroring

mirror disable

Syntax To disable mirroring for a specified trigger type:

```
mirror disable triggerType [hex] triggerValue
```

To disable mirroring for the agent-circuit-id or agent-remote-id trigger types, when the hex variant is used:

```
mirror disable triggerType hex triggerValue
```

To disable mirroring for the dhcp-option-82 trigger type:

```
mirror disable dhcp-option-82 agent-circuit-id triggerValue1 agent-remote-id  
triggerValue2
```

To disable mirroring for the dhcp-option-82 trigger type, when the hex variant is used:

```
mirror disable dhcp-option-82 hex triggerValue
```

Release Information Command introduced before JUNOS Release 7.1.0.
nas-port-id added in JUNOS Release 7.1.0.
hex keyword added in JUNOS Release 11.1.0.

Description Disables a packet mirroring session that was dynamically configured for a subscriber; uses the trigger information to identify the subscriber's session. There is no **no** version.



NOTE: The hex variant is applicable only for agent-circuit-id, agent-remote-id, and dhcp-option-82 trigger types. If the hex variant is used then the *triggerValue* must be a hexadecimal number.

- Options**
- *triggerType*—One of the following RADIUS attributes that was used as the trigger to start the packet mirroring session
 - acct-session-id—Acct-Session-Id, RADIUS attribute [44]
 - agent-circuit-id—Agent Circuit ID, RADIUS attribute [26–1], Vendor ID 3561
 - agent-remote-id—Agent Remote ID, RADIUS attribute [26–2], Vendor ID 3561
 - calling-station-id—Calling-Station-Id, RADIUS attribute [31]
 - dhcp-option-82—DHCP Option 82, RADIUS attribute [26–159], Vendor ID 4874
 - ip-address—Framed-IP-Address, RADIUS attribute [8]; associated with the virtual router where the command is issued, RADIUS VSA [26-1]

- nas-port-id—NAS-Port-Id, RADIUS attribute [87]
- username—User-Name, RADIUS attribute [1]; associated with the virtual router where the command is issued, RADIUS VSA [26-1]
- triggerValue—Value of the *triggerType* (the specified RADIUS attribute) that identifies the subscriber

Mode Privileged Exec

- Related Topics**
- Configuring CLI-Based Mirroring
 - Configuring RADIUS-Based Mirroring

mirror-enable

Syntax [no] mirror-enable

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the use of the secure packet mirroring commands. The secure commands are then visible and can be used during the current CLI session. The **no** version disables the use of packet mirroring commands; the commands no longer appear in the CLI.

Mode Privileged Exec

Related Topics ■ [Configuring CLI-Based Mirroring](#)

mirror trap-enable

Syntax [no] mirror trap-enable

Release Information Command introduced in JUNOS Release 7.2.0.

Description Configures the packet mirroring application to generate secure packet mirroring traps. The **no** version disables the trap generation.

Mode Global Configuration

Related Topics ■ [Monitoring SNMP Secure Packet Mirroring Traps](#)

mld disable

Syntax [no] mld disable

Release Information Command introduced before JUNOS Release 7.1.0.

Description Disables MLD on a virtual router. The **no** version reenables MLD on a virtual router.

Mode Router Configuration

mode

Syntax mode { file-system-synchronization | high-availability }
no mode

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables high availability mode (hitless SRP switchover) operation. The **no** version returns high availability mode operation to its default (file-system-synchronization).

- Options**
- file-system-synchronization—Uses file synchronization to keep the configuration of the standby SRP coordinated with the configuration of the active SRP
 - high-availability—Uses mirroring to keep the configuration and state of the standby SRP coordinated with the configuration and state of the active SRP

Mode Redundancy Configuration

monitor atm vc

Syntax `monitor atm vc atm interfaceSpecifier vcd [atm interfaceSpecifier vcd]*`
 [*load-interval seconds*] [*display-time-of-day*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Displays bit rate and packet rate statistics over a specified time interval for one or more ATM virtual circuits (VCs). There is no **no** version.

- Options**
- *interfaceSpecifier*—ATM interface specifier; see Interface Types and Specifiers on page 5
 - *vcd*—Virtual circuit descriptor that is an identifier for the VC in other commands; number in the range 1–2147483647
 - *seconds*—Number of seconds in the range 5–30 that specifies the time interval at which the router calculates bit rates and packet rates for the specified VC; default value is 5 seconds
 - *display-time-of-day*—Sets time at which the router calculates the bit rate and packet rate statistics for the current interval
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Privileged Exec, User Exec

monitor atm vp

Syntax monitor atm vp atm *interfaceSpecifier* *vpi* [atm *interfaceSpecifier* *vpi*]*
[load-interval *seconds*] [display-time-of-day]

Release Information Command introduced in JUNOS Release 7.1.0.

Description Displays bit rate and packet rate statistics over a specified time interval for one or more ATM virtual paths (VPs). There is no **no** version.

- Options**
- *interfaceSpecifier*—ATM interface specifier; see Interface Types and Specifiers on page 5
 - *vpi*—Virtual path identifier of the PVC. The numeric range of the VPI depends on the line module capabilities and current configuration.
 - *seconds*—Number of seconds in the range 5–300 that specifies the time interval at which the router calculates bit rates and packet rates for the specified VP; default value is 5 seconds
 - display-time-of-day—Sets time at which the router calculates the bit rate and packet rate statistics for the current interval
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Privileged Exec, User Exec

monitor vlan interface

Syntax monitor vlan interface *interfaceType interfaceSpecifier*
 [*interfaceType interfaceSpecifier*]* [load-interval *seconds*] [display-time-of-day]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Displays bit rate and packet rate statistics over a specified time interval for one or more VLAN subinterfaces. There is no **no** version.

- Options**
- *interfaceType*—One of the following interface types listed in Interface Types and Specifiers on page 5
 - atm
 - fastEthernet
 - gigabitEthernet
 - lag
 - tenGigabitEthernet
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *seconds*—Number of seconds in the range 5–30 that specifies the time interval at which the router calculates bit rates and packet rates for the specified VLAN; default value is 5 seconds
 - display-time-of-day—Sets time at which the router calculates the bit rate and packet rate statistics for the current interval
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Privileged Exec, User Exec

more

Syntax To display a file that resides in NVS on the primary SRP module:

`more fileName`

To display a file that resides in NVS on the redundant (standby) SRP module:

`more standby:fileName`

To display a file that resides on a remote server:

`more serverName:filePathName`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Displays the contents of a macro, script, or text file. The file can reside in NVS on the primary SRP module, in NVS on the redundant (standby) SRP module, or on a remote server that you access using FTP. There is no **no** version.

- Options**
- *fileName*—Name of the file you want to display
 - *serverName*—Name of the remote server on which the file resides
 - *filePathName*—Complete path of the file on the remote server

Mode Privileged Exec

motd-banner

Syntax [no | default] motd-banner

Release Information Command introduced before JUNOS Release 7.1.0.

Description Controls display of a message-of-the-day banner (configured with the **banner** command) on a particular line when a connection is initiated. The **no** version disables the motd banner on the line; the motd banner is also disabled by the **no exec-banner** command. The **default** version restores the default setting, in which the banner is enabled on all lines.

Mode Line Configuration

mount

Syntax mount { disk0 | disk1 }
 no mount { disk0 | disk1 } [force]

Release Information Command introduced in JUNOS Release 8.0.0.

Description Mounts the specified flash card. If the card was not safely unmounted previously, the command also performs disk and file system integrity checks before mounting the card and permitting user access. The **no** version prepares the card for safe unmounting by rejecting requests to open files and waiting for currently open files to close; only then is the user notified that the unmounted card can be safely ejected.

- Options**
- disk0—Specifies flash card in slot 0 of the SRP module; although this option is displayed by the CLI, it is rejected when specified because disk0 is required for router operation
 - disk1—Specifies flash card in slot 1 of the SRP module; supported only on the E120 router and the E320 router
 - force—Forces the dismount even when files on the disk are open for modification

Mode Privileged Exec

mpls

Syntax To enable MPLS on a virtual router in Global Configuration mode, or to create an MPLS major interface in Interface Configuration mode:

```
[ no ] mpls
```

To modify the subscriber policy for MPLS packets in Subscriber Policy Configuration mode:

```
mpls { permit | deny }
```

```
no mpls
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description In Global Configuration mode, creates MPLS in the current virtual router. By default, MPLS does not exist in a VR. The **no mpls** version removes MPLS from the VR, and additionally removes all MPLS major interfaces, MPLS shim interfaces, MPLS load-balancing groups, MPLS minor interfaces, and MPLS forwarding tables from the VR.

In Interface Configuration mode, creates an MPLS major interface stacked on the current layer 2 interface, and automatically enables MPLS in the current VR if it has not already been enabled. If the MPLS major interface already exists, no action is taken and no message is generated. An error message is generated if you issue the command for a layer 2 interface that does not support MPLS major interfaces. You cannot enable MPLS on a loopback interface. The **no mpls** version removes the MPLS major interface.

In Subscriber Policy Configuration mode, modifies the subscriber policy for MPLS to define whether the subscriber (client) interfaces that belong to a bridge group or to a VPLS instance forward (permit) or filter (deny) MPLS packets. The **no** version restores the default value, permit MPLS packets.

In Subscriber Policy Configuration mode, you cannot change the default subscriber policy values for trunk (server) interfaces that belong to a bridge group or to a VPLS instance. You also cannot change the default subscriber policy values for a VPLS virtual core interface, which acts as a trunk interface. The VPLS virtual core interface represents all of the MPLS tunnels from the router to the remote VPLS edge (VE) devices.



NOTE: MPLS does not exist by default and must be created, either explicitly with this command, or implicitly with another **mpls** configuration command. If you create MPLS implicitly, for example by issuing the command **mpls lsp retries 10**, MPLS remains disabled until you enable it, by issuing the **mpls** command.

- Options**
- permit—Specifies that the subscriber interface associated with the bridge group or VPLS instance forwards MPLS packets
 - deny—Specifies that the subscriber interface associated with the bridge group or VPLS instance filters MPLS packets

Mode Global Configuration, Interface Configuration, Subscriber Policy Configuration

- Related Topics**
- *Configuring MPLS LSPs for L2VPNs and Configuring MPLS LSPs for VPLS in the JUNOS BGP and MPLS Configuration Guide*

mpls atm vci range

Syntax mpls atm vci range *minVCI maxVCI*
 no mpls atm vci range

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the range for virtual circuit identifiers that can be used in MPLS labels for an MPLS major interface on an ATM AAL5 interface using the interface label space. Creates the MPLS major interface if it does not yet exist. An error message is generated if you issue the command for any other layer 2 interface, as they do not support the interface label space. The **no** version deletes the range.

- Options** ■ *minVCI*—Lowest virtual circuit identifier acceptable for a label, a value from 33–65535
- *maxVCI*—Highest virtual circuit identifier acceptable for a label, a value from 33–65535

Mode Interface Configuration

mpls atm vpi range

Syntax mpls atm vpi range *minVPI maxVPI*
 no mpls atm vpi range

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the range for virtual path identifiers that can be used in MPLS labels for an MPLS major interface on an ATM AAL5 interface using the interface label space. Creates the MPLS major interface if it does not yet exist. An error message is generated if you issue the command for any other layer 2 interface, as they do not support the interface label space. The **no** version deletes the range.

- Options** ■ *minVPI*—Lowest virtual path identifier acceptable for a label, a value in the range 0–255
- *maxVPI*—Highest virtual path identifier acceptable for a label, a value in the range 0–255

Mode Interface Configuration

mpls backup-path

Syntax [no] mpls [traffic-eng] backup-path *bypassTunnelName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns the specified bypass tunnel to the interface that you want to protect. The **no** version removes the assignment.

- Options**
- traffic-eng—Specifies optional keyword for compatibility with non-E Series implementations
 - *bypassTunnelName*—Name of the bypass tunnel

Mode Interface Configuration

mpls bandwidth

Syntax { ip rsvp | mpls } bandwidth *bandwidth*
no { ip rsvp | mpls } bandwidth

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the total bandwidth reservable for MPLS on the interface. The **no** version restores the default value, 0.

- Options**
- ip rsvp—Specifies keyword for compatibility with non-E Series implementations of MPLS
 - mpls—Specifies JUNOS MPLS implementation
 - *bandwidth*—Reservable bandwidth in kilobits per second, a value in the range 1–10000000

Mode Interface Configuration

mpls classifier-list

Syntax mpls classifier-list *classifierName*
 [traffic-class *className*] [color { green | yellow | red }]
 [user-packet-class *userPacketClassValue*] [exp-bits *expValue*
 [exp-mask *maskValue*]

 no mpls classifier-list *classifierName* [*classifierNumber*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates or modifies an MPLS classifier control list. The **no** version deletes the MPLS classifier control list.

- Options**
- *classifierName*—Name of a classifier list entry
 - *className*—Name of a traffic class; the router supports up to eight traffic classes
 - green—Matches packet color to green, indicating a low drop preference
 - yellow—Matches packet color to yellow, indicating a medium drop preference
 - red—Matches packet color to red, indicating a high drop preference
 - *userPacketClassValue*—Value of the user packet class in the range 0–15
 - *expValue*—Value of the EXP bits in the range 0–7
 - *maskValue*—Mask applied to the EXP bits in the range 1–7
 - *classifierNumber*—Index of the classifier control list entry to be deleted; an integer in the range 1–10000

Mode Global Configuration

Related Topics ■ Creating or Modifying Classifier Control Lists for MPLS Policy Lists

mpls copy-upc-to-exp

Syntax [no] mpls copy-upc-to-exp

Release Information Command introduced in JUNOS Release 7.1.0.

Description Sets the initial value of the EXP bits in pushed or swapped labels to the user packet class value associated with the packets. This command does not modify EXP bits in labels already in the received MPLS packet. The **no** version restores the default condition, where the EXP bits are set to 000 (for non-MPLS/IP traffic) or to the IP precedence value from the TOS field of the IP packet header (for IP traffic).

Mode Global Configuration

mpls create-dynamic-interfaces

Syntax mpls create-dynamic-interfaces
 { ip | ipv6 } on-major-interfaces [for-vpn-traffic] [profile *profileName*]

no mpls create-dynamic-interfaces
 { ip | ipv6 } on-major-interfaces [for-vpn-traffic]

Release Information Command introduced in JUNOS Release 7.1.0.

Description Specifies whether dynamic IP interfaces are automatically created on top of all MPLS major interfaces, and if so, which profile is used to create them. By default, one IPv4 dynamic interface without a profile is created and used for both VPN and non-VPN traffic. If IPv6 is enabled on the virtual router, then by default, one IPv6 dynamic interface without a profile is created and used for both VPN and non-VPN traffic. The **no** version restores the default behavior.

- Options**
- ip—Specifies that the created dynamic interfaces are IPv4
 - ipv6—Specifies that the created dynamic interfaces are IPv6
 - for-vpn-traffic—Specifies that the created dynamic interface is used for BGP/MPLS VPN traffic; VPN traffic uses the same IP interface as non-VPN traffic if separate IP interfaces are not created for the VPN traffic
 - *profileName*—Name of a profile that sets the values that configure the IP interface; if you do not specify a profile, the interface attributes are set to their default values

Mode Global Configuration

mpls diff-serv phb-id traffic-class

Syntax mpls diff-serv phb-id { private *privateId* | standard *standardId* }
 traffic-class *className* [color { green | yellow | red }]

no mpls diff-serv phb-id { private *privateId* | standard *standardId* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Maps the specified PHB ID to the internal traffic class and color combination. If color is specified, the PHB ID can be used only for E-LSPs. If color is *not* specified, the PHB ID can be used only for L-LSPs. The **no** version removes the mapping.

- Options**
- *privateId*—Number in the range 0–4032 designating the private PHB identifier
 - *standardId*—Number in the range 0–63 designating the standard PHB identifier using the DSCP bits
 - *className*—Name of a traffic class; the router supports up to eight traffic classes
 - green—Sets packet color to green, indicating a low drop preference
 - yellow—Sets packet color to yellow, indicating a medium drop preference
 - red—Sets packet color to red, indicating a high drop preference

Mode Global Configuration

mpls disable

Syntax [no] mpls disable

Release Information Command introduced before JUNOS Release 7.1.0.

Description Administratively disables the MPLS major interface. MPLS major interfaces are administratively enabled by default. The **no** version restores the default condition, and creates an MPLS major interface if it does not already exist.

Mode Interface Configuration

mpls explicit-path

Syntax { ip | mpls } explicit-path { name *name* | identifier *number* } [enable | disable]
 no { ip | mpls } explicit-path { name *name* | identifier *number* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Defines an explicit path by name or ID number and also enables or disables the explicit path. The **no** version deletes the explicit path.

- Options**
- ip—Specifies alternative keyword for compatibility with non-E Series implementations
 - mpls—Specifies JUNOS MPLS implementation
 - *name*—Name for the explicit path; string of up to 20 characters
 - *number*—Number identifying the explicit path in the range 1–65535
 - enable—Reenables the explicit path that was previously disabled on the virtual router; to prevent a partially configured explicit path from being used, do not enable it until you have finished configuring or modifying the path
 - disable—Disables the explicit path that was previously enabled on the virtual router

Mode Global Configuration

mpls ip propagate-ttl

Syntax [no | default] mpls ip propagate-ttl [forwarded | local]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Controls the value for the TTL field in the MPLS header at the tunnel ingress when a label is assigned to an IP packet. Enabled by default, this command sets the TTL to the TTL value from the IP packet header.

The **no** version sets the value to 255 to hide the network structure from all traffic, preventing the **traceroute** command from discovering and displaying LSP hops. The **no** version changes the TTL processing model from the default uniform model to the pipe model.

The **default** version reverts to the global default, causing the TTL field to be copied from the IP packet header and enabling the **traceroute** command to show all the hops in the network.

- Options**
- **forwarded**—Reveals the network structure to traceroute for forwarded packets; when used with the **no** version, hides the network structure from traceroute only for local packets, enabling you to hide the structure of the MPLS network from your customers, and sets the tunnel model to pipe for forwarded packets
 - **local**—Reveals the network structure to traceroute for local packets; when used with the **no** version, hides the network structure from traceroute only for local packets, sets the tunnel model to pipe for locally originated packets, and sets the tunnel model to pipe for locally originated packets

Mode Global Configuration

mpls l2transport load-balancing-group

Syntax mpls l2transport load-balancing-group *groupNumber*
 [mpls-relay *remoteIpAddress* | route interface tunnel *lspName*]
 [vc-id] *vcIdValue* [group-id *groupIdValue*]
 [control-word | no-control-word] [sequencing | no-sequencing]
 [relay-format { ethernet | ppp | vlan }]

no mpls l2transport load-balancing-group *groupNumber*
 { mpls-relay *remoteIpAddress* | route interface tunnel *lspName* } [vc-id] *vcId*

Release Information Command introduced before JUNOS Release 7.1.0.
control-word, **no-control-word**, **sequencing**, and **no-sequencing** keywords added in JUNOS Release 7.1.0.

Description Specifies a Martini layer 2 transport circuit, associates it with a load-balancing group, and accesses L2 Transport Load-Balancing-Circuit Configuration mode. The **no** version removes a circuit from the load-balancing group and all subinterfaces that the circuit was configured on.



NOTE: Using the **mpls-relay** keywords has the same effect as using the **mpls-relay** command. Using the **route interface** keywords has the same effect as using the **route interface** commands. The **relay-format frame-relay** option is not supported for the **mpls l2transport load-balancing-group** command.

- *groupNumber*—Integer in the range 1–127
- *remoteIpAddress*—IP address of the router on the remote end of the layer 2 circuit
- *lspName*—Name of the route interface tunnel
- *vcIdValue*—Integer in the range 1–4294967295 that identifies the virtual connection; the two ends across the MPLS core must match inside each VC type
- *groupIdValue*—Integer in the range 0–4294967295 that identifies a group of virtual connections; not currently used
- **control-word**—Indicates that the local preference is to use the control word for the layer 2 packets encapsulated in MPLS packets sent to the remote PE router. The default preference is determined by the interface stack on which the MPLS interface is stacked.
- **no-control-word**—Indicates that the local preference is to not use the control word for the layer 2 packets encapsulated in MPLS packets sent to the remote PE router. The default preference is determined by the interface stack on which the MPLS interface is stacked.
- **sequencing**—Specifies that the local preference is to include nonzero sequence numbers with the control word; enabling the remote PE to detect out-of-order packets; has no effect if no control word is sent in the packets. The router always accepts zero sequence numbers and checks the order of nonzero sequence

numbers of MPLS packets received from the remote PE; any out of order packets are dropped, regardless of whether sequencing is configured.

- **no-sequencing**—Specifies that the sequencing number in the control word is set to zero, instructing the remote PE router to not attempt to detect out-of-order packets; has no effect if no control word is sent in the packets.
- **relay-format ethernet**—Specifies that the router uses Ethernet signaling and encapsulation, which causes the VLAN interface to appear as an Ethernet interface to the other side of the connection; enables a VLAN interface on one side of an MPLS tunnel to communicate with an Ethernet or a bridged Ethernet interface on the other side of an MPLS tunnel. The VLAN tag is not included in the MPLS encapsulation. This option is not available on serial or POS interfaces for HDLC layer 2 circuits. It is available only on VLAN interfaces
- **relay-format frame-relay**—Specifies that the router uses legacy (pre-RFC 4619) Frame Relay pseudowire type value for signaling and encapsulation. Enables a router running JUNOS software that supports the pseudowire type value defined in RFC 4619, Encapsulation methods for transport of Frame Relay over MPLS Networks, to interoperate with a router that uses the legacy (pre-RFC 4619) pseudowire type value. This option is available on serial or POS interfaces for Frame Relay layer 2 circuits. It is not supported on E120 and E320 routers.
- **relay-format ppp**—Specifies that the router uses VC-type PPP signaling and PPP encapsulation instead of VC-type HDLC signaling and HDLC encapsulation. The router uses VC-type HDLC signaling and HDLC encapsulation by default. This option is available only on serial and POS interfaces for HDLC layer 2 circuits.
- **relay-format vlan**—Specifies that the router uses VLAN signaling and encapsulation. This option is not available on serial or POS interfaces for HDLC layer 2 circuits. It is available for VLAN interfaces.

Mode Global Configuration

Related Topics ■ *Configuring CE-Side Load Balancing for Martini Layer 2 Transport in the JUNOS BGP and MPLS Configuration Guide*

mpls ldp

Syntax [no] mpls ldp

Release Information Command introduced in JUNOS Release 7.1.0.

Description Enables LDP and topology-driven LSP, as does any LDP-related command, using an implicit default profile. You cannot enable LDP and topology-driven LSPs on a loopback interface. The **no** version disables LDP globally or on the interface.

Mode Global Configuration, Interface Configuration, Subinterface Configuration

Related Topics ■ *Configuring MPLS LSPs for L2VPNs and Configuring MPLS LSPs for VPLS in the JUNOS BGP and MPLS Configuration Guide*

mpls ldp advertise-labels

Syntax mpls ldp advertise-labels { host-only | for *routeAccessList* [to *neighborAccessList*] | interface *interfaceType* *interfaceSpecifier* }

no mpls ldp advertise-labels { policy-list | host-only | for *routeAccessList* [to *neighborAccessList*] | interface *interfaceType* *interfaceSpecifier* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Controls the distribution of incoming labels advertised by LDP. The **no** version halts advertisement of all incoming labels or the specified labels.

- Options**
- *host-only*—Advertises only labels for host routes (routes with a 32-bit mask)
 - *routeAccessList*—Name of access list identifying routes for which label advertisement is permitted or denied
 - *neighborAccessList*—Name of access list identifying neighbors to which the LSR advertises labels
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
 - *policy-list*—Deletes all lists configured with the **for** *routeAccessList* option

Mode Global Configuration

mpls ldp autoconfig

Syntax From Interface Configuration mode and Subinterface Configuration mode:

```
[ no ] mpls ldp { isis | ospf } autoconfig
```

From Router Configuration mode for IS-IS:

```
mpls ldp autoconfig [ level-1 | level-2 | level-1-2 ]
```

```
no mpls ldp autoconfig
```

From Router Configuration mode for OSPF:

```
mpls ldp autoconfig [ areald | arealdInt ]
```

```
no mpls ldp autoconfig
```

Release Information Command introduced in JUNOS Release 8.1.0.

Description In Interface Configuration mode, creates LDP on the current interface. The **no** version removes LDP from the interface.

In Router Configuration mode, creates LDP on all interfaces in the IS-IS or OSPF router, on interfaces in the specified level (IS-IS), or on interfaces in the specified area (OSPF). The **no** version removes the LDP configuration for all qualifying interfaces.

- Options**
- **level-1**—Enables LDP on all IS-IS level 1 interfaces
 - **level-1-2**—Enables LDP on all IS-IS level 1-2 interfaces
 - **level-2**—Enables LDP on all IS-IS level-2-only interfaces
 - ***areald***—OSPF area ID in IP address format
 - ***arealdInt***—OSPF area ID as a decimal value in the range 0–4294967295

Mode Interface Configuration, Router Configuration, Subinterface Configuration

mpls ldp deaggregate

Syntax [no] mpls ldp deaggregate

Release Information Command introduced in JUNOS Release 8.1.0.

Description Configures LDP to bind each prefix to a separate label on the current virtual router. The **no** version enables LDP to aggregate multiple prefixes to be bound to the same label.

Mode Global Configuration

mpls ldp disable

Syntax [no] mpls ldp disable

Release Information Command introduced in JUNOS Release 7.1.0.

Description Disables LDP on the interface. The **no** version reenables LDP on the interface.

Mode Interface Configuration

mpls ldp discovery transport-address

Syntax mpls ldp discovery transport-address *ipAddress*
 no mpls ldp discovery transport-address

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies an arbitrary IP address to be used as the transport address of the local peer advertised in LDP discovery hello messages for interfaces that use the platform label space. The peer router uses the transport address to establish the session TCP connection. By default, the router ID is advertised as the transport address. The **no** version restores the default transport address, the LSR router ID.

Options ■ *ipAddress*—IP address advertised as the transport address

Mode Router Configuration

mpls ldp egress-label

Syntax mpls ldp egress-label { explicit-null | non-null }
 no mpls ldp egress-label

Release Information Command introduced in JUNOS Release 8.1.0.

Description Configures LDP to advertise the explicit null label (label 0) or a non-null label for the LSR that is the egress router for the prefix. This command takes effect immediately. The **no** version restores the default, where the egress router advertises the implicit null label (label 3), which causes the router's upstream neighbor to perform a penultimate hop pop.

Mode Global Configuration

mpls ldp graceful-restart

Syntax mpls ldp graceful-restart [helper]
 no mpls ldp graceful-restart

Release Information Command introduced in JUNOS Release 7.1.0.

Description Enables LDP graceful restart to preserve MPLS forwarding state across a restart, and helper mode, or only helper mode. LDP graceful restart and helper mode are both disabled by default. The **no** version disables both LDP graceful restart and helper mode.

Graceful restart causes the fault tolerant session TLV to be included in LDP initialization messages with a nonzero value for the reconnect timeout. This action announces to neighbors that the router preserves its forwarding state across a restart.

Helper mode causes the fault tolerant session TLV to be included in LDP initialization messages. The reconnect timeout value in the TLV is zero when LDP graceful restart is disabled. This TLV announces to neighbors that the router preserves any label-FEC mapping it has received from a neighbor in the event that the neighbor performs an LDP graceful restart.

Options ■ helper—Configures only helper mode to preserve label-FEC mappings from a neighbor in the event the neighbor gracefully restarts

Mode Global Configuration

mpls ldp graceful-restart reconnect-time

Syntax mpls ldp graceful-restart reconnect-time [*seconds*]
 no mpls ldp graceful-restart reconnect-time

Release Information Command introduced in JUNOS Release 7.1.0.

Description Specifies the length of time you want neighbors to wait for the gracefully restarting router to resume sending LDP messages to neighbors after the restart. The **no** version restores the default value, 120 seconds.

Options ■ *seconds*—Number of seconds in the range 60–300

Mode Global Configuration

mpls ldp graceful-restart recovery-time

Syntax mpls ldp graceful-restart recovery-time [*seconds*]
 no mpls ldp graceful-restart recovery-time

Release Information Command introduced in JUNOS Release 7.1.0.

Description Specifies the length of time the router retains its MPLS forwarding state across a restart. The **no** version restores the default value, 120 seconds.

Options ■ *seconds*—Number of seconds in the range 120–600

Mode Global Configuration

mpls ldp graceful-restart timers max-recovery

Syntax mpls ldp graceful-restart timers max-recovery *seconds*
 no mpls ldp graceful-restart timers max-recovery

Release Information Command introduced in JUNOS Release 7.1.0.

Description Specifies the maximum length of time that the router waits for its neighbor to complete a graceful LDP restart after the LDP session is reestablished. The **no** version restores the default value, 120 seconds.

Options ■ *seconds*—Number of seconds in the range 15–600

Mode Global Configuration

mpls ldp graceful-restart timers neighbor-liveness

Syntax mpls ldp graceful-restart timers neighbor-liveness *seconds*
 no mpls ldp graceful-restart timers neighbor-liveness

Release Information Command introduced in JUNOS Release 7.1.0.

Description Specifies the maximum length of time that the router waits for its neighbor to reestablish an LDP session. The **no** version restores the default value, 120 seconds.

Options ■ *seconds*—Number of seconds in the range 5–300

Mode Global Configuration

mpls ldp igp sync holddown

Syntax mpls ldp igp sync holddown *holdDownValue*
 no mpls ldp ldp igp sync holddown

Release Information Command introduced in JUNOS Release 8.1.0.

Description Configures the LDP-IGP synchronization holddown timer. The **no** version restores the default condition, where the IGP waits for LDP to be operational on the interface indefinitely.

Options ■ *holdDownValue*—Number of milliseconds in the range 1–65535

Mode Global Configuration

mpls ldp independent-control

Syntax [no] mpls ldp independent-control

Release Information Command introduced in JUNOS Release 8.1.0.

Description Specifies independent control as the method used by LDP for label distribution. This command takes effect immediately. The **no** version restores the default method, ordered control.

Mode Global Configuration

mpls ldp ip-forwarding

Syntax [no] mpls ldp ip-forwarding [{ access-list | prefix-list } *listName*)] [host-only]

Release Information Command introduced in JUNOS Release 7.1.0.

Description Specifies LSPs to be put into the IP routing table for forwarding plain IP traffic. The **no** version removes the listed LSPs or all LSPs from the IP routing table.



NOTE: This command replaces the deprecated **mpls topology-driven-lsp ip-interfaces** command.



NOTE: Although the carriage return, <cr>, option is displayed when you type a question mark (?) after entering the **mpls ldp ip-forwarding** command, this command takes effect only if the **access-list**, **host-only**, or **prefix-list** keyword, or a combination of them is specified. Otherwise, although the command is configured successfully and no error is displayed, labels are not used in the IP routing table for forwarding plain IP traffic. This behavior for this command began in JUNOS Release 7.1.0, in which the command was introduced.

- Options**
- access-list—Specifies that *listName* is an access list
 - prefix-list—Specifies that *listName* is a prefix list
 - *listName*—Name of access list or prefix list that specifies LSPs over which IP interfaces are created
 - host-only—Specifies that IP interfaces are created only over LSPs to host addresses

Mode Global Configuration

mpls ldp link-hello disable

Syntax [no] mpls ldp link-hello disable

Release Information Command introduced before JUNOS Release 7.1.0.

Description Suppresses the transmission of LDP link hello messages. This command requires the use of targeted hello messages to form LDP peer adjacencies. The **no** version restores the default condition, where the LSR sends multicast link hello messages.

Mode Interface Configuration

mpls ldp neighbor password

Syntax mpls ldp neighbor *ipAddress* password *passwordString*
 [no] mpls ldp neighbor *ipAddress* password

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the password used to compute MD5 checksums for authenticating the specified LDP neighbor when the peer attempts to establish a TCP connection. The **no** version deletes the password for the peer.

- Options** ■ *ipAddress*—IP address of remote peer
 ■ *passwordString*—Password; alphanumeric string in the range 1–40 characters

Mode Global Configuration

mpls ldp profile

Syntax In Global Configuration mode:

mpls ldp [interface] profile [*profileName*]

no mpls ldp interface profile *profileName*

In Interface Configuration mode:

mpls ldp profile *profileName*

no mpls ldp profile

Release Information Command introduced before JUNOS Release 7.1.0.

Description In Global Configuration mode, creates or modifies a configuration profile for LDP. Places the CLI in LDP Configuration mode. The implicit default LDP profile specifies a value of 0 for hello hold-time; this value signifies 15 seconds for link hellos and 45 seconds for targeted hello messages.

Any change to a profile affects all interfaces that use the profile; changes are effective the next time the interface comes up.

In Interface Configuration mode, creates or enables LDP on the interface with the factory default profile or the specified profile. The **no** version reverts to the default profile on the interface.

In both modes, if you specify a profile not previously configured, it is created with the factory default settings. If you do not specify a profile name, the factory default profile is assumed. The no version deletes the specified profile.

- Options**
- *interface*—Keyword required for the no version in Global Configuration mode
 - *profileName*—Name of a profile to be created or modified (Global Configuration mode), applied to an interface (Interface Configuration mode), or deleted (both modes); the profile sets the values for the protocol parameters; until you modify the profile settings, the values match those of the implicit default profile

Mode Global Configuration, Interface Configuration

mpls ldp redistribute

Syntax `mpls ldp redistribute protocol [route-map mapName]`
 `no mpls ldp redistribute protocol [route-map mapName]`

Release Information Command introduced in JUNOS Release 7.1.0.

Description Enables redistribution of routes from the specified IGP to LDP, enabling LDP to advertise labeled BGP routes for the inter-AS option C two-stack scenario. The **no** version halts redistribution from the specified IGP or according to the specified route map.

You can specify a route map to redistribute more specific routes to LDP. Only routes that pass the maps clauses are redistributed. If you do not use a route map for fine-grained control of route distribution, and you do not want to redistribute BGP routes, then you do not need to issue this command.

For backward compatibility, if you do not issue this command, LDP continues to advertise labels for IGP routes—including connected, static, IS-IS, OSPF, and RIP routes, but excluding BGP routes. That is, IGP routes other than BGP are redistributed to LDP by default.

- Options**
- *protocol*—Protocol from which routes are redistributed to LDP: BGP, connected, IS-IS, OSPF, RIP, or static
 - *mapName*—Name of the route map used to redistribute more specific routing information from an IGP to LDP

Mode Global Configuration

mpls ldp session holdtime

Syntax mpls ldp session holdtime *holdTime*
 no mpls ldp session holdtime

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the LDP session hold time, the period that an LSR maintains a session without receipt of a message from an LDP peer. Each LSR peer sends the session hold time in its initialization message; peers negotiate to use the minimum of the session hold times proposed by the pair of LSRs. This negotiated session hold time is used by the keepalive timer to maintain the session.

The keepalive timer is reset with the receipt of any session message from the peer. In the absence of other LDP protocol messages are being sent, peers periodically send a keepalive message to maintain the LDP session.

The LDP session is terminated when the timer expires. The **no** version restores the default value, 180.

Options ■ *holdTime*—Number of seconds in the range 15–65535

Mode Global Configuration

mpls ldp session keepalive interval

Syntax mpls ldp session keepalive interval *seconds*
 no mpls ldp session keepalive interval

Release Information Command introduced in JUNOS Release 8.1.0.

Description Sets the transmission interval at which LDP sends session keepalive messages to maintain the LDP session. Keepalive messages are sent to LDP peers at this interval in the absence of any other LDP traffic over the session. This command takes effect immediately. The **no** version restores the default interval, 20 seconds.

Options ■ *seconds*—Number of seconds, in the range 1–65535

Mode Global Configuration

mpls ldp session retries

Syntax mpls ldp session retries *retryNum*
 no mpls ldp session retries

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the number of attempts that will be made to set up an LDP session. The **no** version restores the default value, 0, meaning that the attempts will be made until successful.

Options ■ *retryNum*—Number of attempts in the range 0–65535

Mode Global Configuration

mpls ldp session retry-time

Syntax mpls ldp session retry-time *retryTime*
 no mpls ldp session retry-time

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the interval in seconds between attempts to set up an LDP session. The **no** version restores the default value, 30 seconds.

Options ■ *retryTime*—Interval in the range 0–60

Mode Global Configuration

mpls ldp strict-security

Syntax [no] mpls ldp strict-security

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures strict LDP authentication mode, which enables sessions to be formed only by peers with configured passwords. The **no** version enables sessions to be formed by peers without configured passwords.

Mode Global Configuration

mpls ldp sync

Syntax From Interface Configuration mode and Subinterface Configuration mode:

```
[ no ] mpls ldp { isis | ospf } sync
```

From Router Configuration mode for IS-IS:

```
mpls ldp sync [ level-1 | level-2 | level-1-2 ]
```

```
no mpls ldp sync
```

From Router Configuration mode for OSPF:

```
mpls ldp sync [ areaId | areaIdInt ]
```

```
no mpls ldp sync
```

Release Information Command introduced in JUNOS Release 8.1.0.

Description In Interface Configuration mode, synchronizes LDP with the IGP on the current interface. The **no** version removes the configuration for the interface.

In Router Configuration mode, synchronizes LDP with the IGP on all of the protocol's interfaces, on all interfaces in the specified level (IS-IS), or on all interfaces in the specified area (OSPF). The **no** version removes the configuration for all qualifying interfaces.

By default, LDP synchronization is not configured.

LDP—IGP synchronization must be configured on both sides of a link to be effective and avoid asymmetric link costs. In addition, LDP-IGP synchronization is effective only when alternate links with adequate bandwidth are available in the network.

- Options**
- **level-1**—Enables synchronization with LDP on all IS-IS level 1 interfaces
 - **level-1-2**—Enables synchronization with LDP on all IS-IS level 1-2 interfaces
 - **level-2**—Enables synchronization with LDP on all IS-IS level-2-only interfaces
 - ***areaId***—OSPF area ID in IP address format
 - ***areaIdInt***—OSPF area ID as a decimal value in the range 1–4294967295

Mode Interface Configuration, Router Configuration, Subinterface Configuration

mpls ldp targeted-hello holdtime

Syntax mpls ldp targeted-hello holdtime *seconds*
 no mpls ldp targeted-hello holdtime

Release Information Command introduced in JUNOS Release 8.1.0.

Description Configures the LDP targeted-hello hold time, the period for which a sending LSR maintains a record of targeted hello messages from the receiving LSR without receipt of another targeted hello message from that LSR. Each LSR peer sends the hold time in its targeted hello messages; peers negotiate to use the minimum of the hold times proposed by the pair of LSRs.

The hold timer is restarted whenever the LSR receives a targeted hello from the peer in the targeted hello adjacency. The timer expires if no targeted hello is received from the peer within the hold time. The LSR deletes the targeted hello adjacency when the timer expires. If all targeted hello adjacencies are deleted for an LDP session, then the LSR terminates the LDP session.

This command takes effect immediately. The **no** version restores the default value, 45 seconds.

Options ■ *seconds*—Number of seconds, in the range 1–65535

Mode Global Configuration

mpls ldp targeted-hello interval

Syntax mpls ldp targeted-hello interval *seconds*
 no mpls ldp targeted-hello interval

Release Information Command introduced in JUNOS Release 8.1.0.

Description Configures the the interval between targeted hello packets sent by LDP. This command takes effect immediately. The **no** version restores the default value, 15 seconds.

Options ■ *seconds*—Number of seconds, in the range 1–65535

Mode Global Configuration

mpls ldp targeted-hello receive list

Syntax [no] mpls ldp targeted-hello receive list
 { access-list *accessListName* | *ipAddress* [*ipAddress*]* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the list of peer addresses from which MPLS accepts targeted hello messages. When you configure a receive list, hello messages are accepted only from list members. If no list is configured, hello messages are accepted from all addresses. The **no** version removes the list of peer addresses.



NOTE: This command is unnecessary if you configure the **mpls ldp targeted-hello send list** command.

- Options**
- *accessListName*—String of up to 32 alphanumeric characters that identifies an access list
 - *ipAddress*—IP address of a peer
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

mpls ldp targeted-hello send list

Syntax [no] mpls ldp targeted-hello send list
{ access-list *accessListName* | *ipAddress* [*ipAddress*]* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures the list of peer addresses to which MPLS sends targeted hello messages and from which MPLS accepts targeted hello messages. The **no** version removes the list of peer addresses.

- Options**
- *accessListName*—String of up to 32 alphanumeric characters that identifies an access list
 - *ipAddress*—IP address of a peer
 - *—Indicates that one or more parameters can be repeated multiple times in a list in the command line

Mode Global Configuration

mpls ldp vpls neighbor

Syntax [no] mpls ldp vpls *vplsName* neighbor *ipAddress*

Release Information Command introduced in JUNOS Release 8.2.0.

Description Configures the remote VPLS edge (VE) device address of a neighbor in the VPLS domain in which the VPLS instance participates. The specified VPLS instance must use LDP as the signaling protocol. If either or both LDP or MPLS are not configured on the current virtual router, issuing this command creates the LDP and MPLS configurations automatically. The **no** version deletes the neighbor from the VPLS domain.

The **mpls ldp vpls neighbor** command is not valid for a VPLS instance that uses BGP as the signaling protocol. To configure a VPLS instance with BGP signaling, use the **bridge vpls rd**, **bridge vpls route-target**, **bridge vpls site-name site-id**, and **bridge vpls site-range** commands.

- Options**
- *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command
 - *ipAddress*—IP address of a neighbor in the VPLS domain

Mode Global Configuration

- Related Topics**
- *Configuring LDP Signaling for VPLS in the JUNOS BGP and MPLS Configuration Guide*

mpls ldp vpls vpls-id

Syntax `mpls ldp vpls vplsName vpls-id vplsId`
 `no mpls ldp vpls vplsName vpls-id`

Release Information Command introduced in JUNOS Release 8.2.0.

Description Configures the globally unique VPLS identifier of a VPLS instance that uses LDP as the signaling protocol. All VEs that participate in the same VPLS domain must use the same VPLS identifier. The VPLS identifier configured for a VPLS instance must not be the same as the PWid for Martini configurations for Ethernet layer 2 services over MPLS. The **no** version deletes the VPLS identifier from the VPLS instance.

The **mpls ldp vpls vpls-id** command is not valid for a VPLS instance that uses BGP as the signaling protocol. To configure a VPLS instance with BGP signaling, use the **bridge vpls rd**, **bridge vpls route-target**, **bridge vpls site-name site-id**, and **bridge vpls site-range** commands.

- Options** ■ *vplsName*—Name of a VPLS instance created with the **bridge vpls transport-virtual-router** command
- *vplsId*—VPLS identifier for the VPLS instance, in the range 1–4294967295

Mode Global Configuration

Related Topics ■ *Configuring LDP Signaling for VPLS in the JUNOS BGP and MPLS Configuration Guide*

mpls lsp no-route retries

Syntax mpls lsp no-route retries *retryNum*
 no mpls lsp no-route retries

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the number of attempts that will be made to set up an LSP for RSVP-TE after a failure due to no available route. The **no** version restores the default value, 0, which means the attempts will be made until successful.

Options ■ *retryNum*—Number of retry attempts in the range 0–65535

Mode Global Configuration

mpls lsp no-route retry-time

Syntax mpls lsp no-route retry-time *retryTime*
 no mpls lsp no-route retry-time

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the interval in seconds between attempts to set up an LSP for RSVP-TE after a failure due to no available route. The **no** version restores the default value, 5 seconds.

Options ■ *retryTime*—Interval in the range 1–60

Mode Global Configuration

mpls lsp retries

Syntax mpls lsp retries *retryNum*
 no mpls lsp retries

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the number of attempts that will be made to set up an LSP for RSVP-TE after a failure other than one due to no available route. The **no** version restores the default value, 0, which means the attempts will be made until successful.

Options ■ *retryNum*—Number of retry attempts in the range 0–65535

Mode Global Configuration

mpls lsp retry-time

Syntax mpls lsp retry-time *retryTime*
 no mpls lsp retry-time

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the interval in seconds between attempts to set up an LSP for RSVP-TE after a failure other than one due to no available route. The **no** version restores the default value, 5 seconds.

Options ■ *retryTime*—Interval in the range 1–60

Mode Global Configuration

mpls match exp-bits

Syntax mpls match exp-bits *bitValue* set traffic-class *className* color { green
| yellow | red }

no mpls match exp-bits *bitValue*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the traffic class and color for incoming MPLS packets whose EXP bits in the MPLS shim header match the specified EXP bits value. The **no** version reverts to the default behavior for traffic matching the specified EXP bits value, setting neither traffic class nor color.

- Options**
- *bitValue*—Value in the range 0–7 that matches the corresponding binary value (000–111) for the three EXP bits
 - *className*—Name of a traffic class; the router supports up to eight traffic classes
 - green—Sets packet color to green, indicating a low drop preference
 - yellow—Sets packet color to yellow, indicating a medium drop preference
 - red—Sets packet color to red, indicating a high drop preference

Mode Global Configuration

mpls match traffic-class

Syntax mpls match traffic-class *className* color { green | yellow | red } set exp-bits *bitValue*
 no mpls match traffic-class *className* color { green | yellow | red }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the EXP bits in the MPLS shim header of outgoing MPLS packets that match the specified combination of traffic class and color. The **no** version reverts to the default behavior for traffic matching the specified traffic class and color combination. The default behavior sets the EXP bits to 000 for traffic entering an LSP and has no effect on the EXP bits for transit traffic.

- Options**
- *className*—Name of a traffic class; the router supports up to eight traffic classes
 - green—Sets packet color to green, indicating a low drop preference
 - yellow—Sets packet color to yellow, indicating a medium drop preference
 - red—Sets packet color to red, indicating a high drop preference
 - *bitValue*—Value in the range 0–7 that sets the corresponding binary value (000–111) for the three EXP bits

Mode Global Configuration

mpls policy

Syntax `mpls policy { input | output } policyName`
`[statistics { enabled [baseline { enabled | disabled }] [preserve | merge] |`
`disabled [merge] } | merge]`

`no mpls policy { input | output } [policyName]`

Release Information Command introduced before JUNOS Release 7.1.0.
merge keyword added in JUNOS Release 7.2.0.

Description Assigns a policy list to the ingress or egress of an MPLS layer 2 transport interface. If you enter this command when the policy list does not exist, the router will create a policy list with a filter rule as the default. Attaching this policy list to an interface filters all packets on that interface. You must specify the **input** or **output** keyword to assign the policy list to the ingress or egress of the interface. The **no** version removes the association between a policy list and an interface.

- Options**
- **input**—Applies policy to data arriving at this interface
 - **output**—Applies policy to data leaving this interface
 - ***policyName***—Name of the policy; a maximum of 40 characters
 - **statistics**—Enables or disables collection of policy routing statistics
 - **enabled**—Enables collection of policy routing statistics
 - **baseline enabled**—Enables baselining of policy routing statistics
 - **baseline disabled**—Disables baselining of policy routing statistics
 - **preserve**—Preserves existing statistics for any classifier-list that is the same for both the new and old policy attachments when you attach a new policy to an interface
 - **disabled**—Disables collection of policy routing statistics
 - **merge**—Enables merging of multiple policies to form a single policy

Mode Interface Configuration

- Related Topics**
- *Configuring HDLC Layer 2 Services in the JUNOS BGP and MPLS Configuration Guide*
 - Setting a Statistics Baseline for Policies

mpls policy-list

Syntax [no] mpls policy-list *policyName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates the specified policy list and accesses Policy List Configuration mode. If you enter the **mpls policy-list** command and the policy list does not exist, the router creates a policy list with no rules, the default. When a policy list does not have rules, the router inserts a default filter rule. Attaching this policy list to an interface filters all packets on that interface. The **no** version deletes the policy list.

Options ■ *policyName*—Name of a policy list; string of up to 40 alphanumeric characters

Mode Global Configuration

Related Topics ■ Creating Policy Lists for MPLS

mpls policy-parameter hierarchical

Syntax mpls policy-parameter hierarchical *parameterName* { *nodeValue* | atm | atm-vc | atm-vp *vpValue* | ethernet | fr-vc | forwarding | svlan *svlanValue* | vlan }

no policy-parameter *parameterName*

Release Information Command introduced in JUNOS Release 8.0.0.

Description Specifies a parameter value for MPLS interfaces. The **no** version removes the policy parameter and its contents.

- Options**
- *parameterName*—Name of policy parameter
 - *nodeValue*—Aggregation node number in the range 1–65535
 - *vpValue*—ATM VPI number in the range 0–255
 - *svlanValue*—SVLAN ID number in the range 0–4095

Mode Interface Configuration

Related Topics

- Creating a Classifier Group for a Policy List

mpls policy-parameter reference-rate

Syntax mpls policy-parameter reference-rate *parameterName* [increase] *value*
 no mpls policy-parameter reference-rate *parameterName* [increase *value*]

Release Information Command introduced in JUNOS Release 8.1.0.

Description Creates an MPLS policy parameter for a reference rate; creates a global parameter if it does not exist. The **no** version removes the policy parameter and its contents; if used with the **increase** keyword, decreases the value.

- Options**
- *parameterName*—Name of policy parameter up to 40 characters
 - increase—Increments the existing reference rate value
 - *value*—Value of the reference rate parameter, in the range 0–4292967295

Mode Interface Configuration

Related Topics

- Creating a Classifier Group for a Policy List

mpls policy-statistics

Syntax mpls { enable | disable } policy-statistics *tunnelName*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables policy statistics to be collected for the specified tunnel or LSP. Statistics collection is disabled by default. There is no **no** version.

- Options**
- enable—Enables the collection of policy statistics
 - disable—Disables the collection of policy statistics; this is the default setting
 - *tunnelName*—Name of a tunnel or LSP; string of up to 20 alphanumeric characters

Mode Privileged Exec, User Exec

mpls preserve-vpn-exp

Syntax [no] mpls preserve-vpn-exp

Release Information Command introduced before JUNOS Release 7.1.0.

Description Prevents the value of the EXP bits for a VPN label from being modified by either a per-LSP policy for the outer labels or per-VR traffic class/color rules. In the default condition, per-LSP policies or per-VR rules modify all labels in a given label stack to have the same value for the EXP bits. The **no** version restores the default condition.

Mode Global Configuration

mpls-relay

Syntax `mpls-relay remoteIpAddress [vc-id] vcidValue [group-id groupIdValue]`
`[control-word | no-control-word] [sequencing | no-sequencing]`
`[relay-format { ethernet | frame-relay | ppp | vlan | ethernet-raw-mode }]`

`no mpls-relay`

Release Information Command introduced before JUNOS Release 7.1.0.
control-word, **no-control-word**, **no-sequencing**, and **vlan** keywords added in JUNOS Release 7.1.0.
frame-relay keyword added in JUNOS Release 9.1.0.
ethernet-raw-mode keyword added in JUNOS Release 10.0.0.

Description Routes layer 2 traffic to the specified router by creating an MPLS shim interface on the layer 2 interface. The router can use any MPLS LSP to the remote destination address that you specify. You must issue this command in the virtual router where the remote address can be reached; that is, in the virtual router providing core connections. The **no** version removes the shim interface. See also the route interface command.



NOTE: This command is supported for configuration on an ATM port (ATM Adaptation Layer 5 [AAL5] over an ATM major interface). Before you can specify VPI/VCI ranges and cell concatenation parameters on the ATM port to enable transmission of multiple ATM virtual circuits over a single pseudowire, you must associate the ATM port with the corresponding pseudowire using the **mpls-relay** or **router interface tunnel** command. For more information about the support for multiple VCs over a single pseudowire, see *Multiple ATM Virtual Circuits over a Single Pseudowire Overview* in the *JUNOS BGP and MPLS Configuration Guide*

Options

- *remoteIpAddress*—IP address of the router on the remote end of the layer 2 circuit
- *vcidValue*—Integer in the range 1–4294967295 that identifies the virtual connection; the two ends across the MPLS core must match inside each VC type



NOTE: The VLAN ID, DLCI, or ATM VPI/VCI are not related to the VC ID and can be different on each end of the connection.

-
- *groupIdValue*—Integer in the range 0–4294967295 that identifies a group of virtual connections; not currently used
 - *control-word*—Indicates that the local preference is to use the control word for the layer 2 packets encapsulated in MPLS packets sent to the remote PE router. The default preference is determined by the interface stack on which the MPLS interface is stacked.

- **no-control-word**—Indicates that the local preference is to not use the control word for the layer 2 packets encapsulated in MPLS packets sent to the remote PE router. The default preference is determined by the interface stack on which the MPLS interface is stacked.
- **sequencing**—Specifies that the local preference is to include nonzero sequence numbers with the control word; enabling the remote PE to detect out-of-order packets; has no effect if no control word is sent in the packets. The router always accepts zero sequence numbers and checks the order of nonzero sequence numbers of MPLS packets received from the remote PE; any out of order packets are dropped, regardless of whether sequencing is configured.
- **no-sequencing**—Specifies that the sequencing number in the control word is set to zero, instructing the remote PE router to not attempt to detect out-of-order packets; has no effect if no control word is sent in the packets.
- **relay-format ethernet**—Specifies that the router uses Ethernet signaling and encapsulation, which causes the VLAN interface to appear as an Ethernet interface to the other side of the connection; enables a VLAN interface on one side of an MPLS tunnel to communicate with an Ethernet or a bridged Ethernet interface on the other side of an MPLS tunnel. The VLAN tag is not included in the MPLS encapsulation. This option is not available on serial or POS interfaces for HDLC layer 2 circuits. It is available only on VLAN interfaces
- **relay-format frame-relay**—Specifies that the router uses legacy (pre-RFC 4619) Frame Relay pseudowire type value for signaling and encapsulation. Enables a router running JUNOS software that supports the pseudowire type value defined in RFC 4619, Encapsulation methods for transport of Frame Relay over MPLS Networks, to interoperate with a router that uses the legacy (pre-RFC 4619) pseudowire type value. This option is available on serial or POS interfaces for Frame Relay layer 2 circuits. It is not supported on E120 and E320 routers.
- **relay-format ppp**—Specifies that the router uses VC-type PPP signaling and PPP encapsulation instead of VC-type HDLC signaling and HDLC encapsulation. The router uses VC-type HDLC signaling and HDLC encapsulation by default. This option is available only on serial and POS interfaces for HDLC layer 2 circuits.
- **relay-format vlan**—Specifies that the router uses VLAN signaling and encapsulation. This option is not available on serial or POS interfaces for HDLC layer 2 circuits. It is available for VLAN interfaces.
- **relay-format ethernet-raw-mode**—Specifies that the router uses Ethernet raw mode encapsulation for packets entering and leaving pseudowires. This service corresponds to PW type 0x0005 "Ethernet" [IANA]. When configured on an S-VLAN subinterface, enables the provider edge (PE) device to strip the S-VLAN tags from all packets entering the Martini circuit (MPLS packet switched network). It is supported on ES2 4G, ES2 10G, and ES2 10G Uplink LMs on E120 and E320 routers. You can enable the raw mode configuration only for MPLS shim interfaces stacked on SVLAN interfaces.



NOTE: The **relay-format** keyword determines the pseudowire PW Type value that is used in LDP protocol messages. For a complete list of pseudowire Type values, see <http://www.iana.org/assignments/pwe3-parameters>.

If you do not specify the **relay-format** keyword in the **mpls-relay** or **route interface** command, the pseudowire Type value is chosen based on the type of the interface. For Ethernet interfaces, the pseudowire Type value is chosen as Ethernet (0x0005). For VLAN interfaces, the pseudowire Type value is chosen as Ethernet Tagged Mode (0x0004).

Mode Interface Configuration, Subinterface Configuration

Related Topics ■ *Configuring an MPLS Pseudowire with VCC Cell Relay, Configuring Ethernet/VLAN Layer 2 Services, Configuring Frame Relay Layer 2 Services, Configuring HDLC Layer 2 Services, Configuring Local ATM Cross-Connects Between Ethernet/VLAN Interfaces, Configuring Ethernet Raw Mode Encapsulation for Martini Layer 2 Transport, and Configuring S-VLAN Tunnels for Layer 2 Services in the JUNOS BGP and MPLS Configuration Guide*

mpls-relay atm cell-packing mcpt-timer

Syntax mpls-relay atm cell-packing *maxCellsPerPacket* mcpt-timer *timerIdentifier*
 no mpls-relay atm cell-packing

Release Information Command introduced in JUNOS Release 10.2.0.

Description Configures cell concatenation parameters for an ATM port to calculate the maximum number of ATM cells that the router can concatenate in a single packet and the unique identifier of the ATM Martini cell packing timer that you want to use to detect timeout of the cell collection threshold. You can configure this command on the ATM port only after you associated a pseudowire with the port by using the mpls-relay or route interface tunnel command. You can use this command only on an ATM port (ATM AAL5 over ATM major interface). The **no** version disables cell concatenation, which is the default behavior.

- Options**
- atm—Configures ATM interface parameters for MPLS cross-connect
 - *maxCellsPerPacket*—Maximum number of ATM cells in the range 1–190 that the router can concatenate in a single VCC cell relay-encapsulated packet and transmit on an MPLS pseudowire connection; default value is 1 cell per packet
 - *timerIdentifier*—Integer in the range 1–3 that identifies which of the three ATM Martini cell packing timers (timer 1, timer 2, or timer 3) you want to use to detect timeout of the cell collection time threshold; default value is 1. When the timer expires, the router forwards the packet even if the number of concatenated ATM cells in the packet is fewer than the specified maximum number of cells per packet.

Mode Interface Configuration

- Related Topics**
- *Multiple ATM Virtual Circuits over a Single Pseudowire Overview* and *Multiple ATM Virtual Circuits over a Single Pseudowire Example* in the *JUNOS BGP and MPLS Configuration Guide*

mpls-relay atm vpi-range vci-range

Syntax [no] mpls-relay atm vpi-range *vpiStart vpiEnd* vci-range *vciStart vciEnd*

Release Information Command introduced in JUNOS Release 10.2.0.

Description Configures a single virtual path identifier (VPI)/virtual circuit identifier (VCI) range of ATM VCs whose cells need to be transported on the single pseudowire. You can configure this command on the ATM port only after you associated a pseudowire with the port by using the **mpls-relay** or **route interface tunnel** command. When you run the **mpls-relay** or **route interface tunnel** command, no default VPI/VCI range is configured. You must specifically configure the VPI/VCI ranges. You can use this command only on an ATM port (ATM AAL5 over ATM major interface). The VPI/VCI values that are not part of the specified range can be used for other existing applications. The **no** version removes the configured VPI/VCI range.



NOTE: The total number of VCs configured with the **mpls-relay atm vpi-range vci-range** command cannot exceed the maximum ATM VC capacity of the line module you are using. For details about the ATM VC capacity of supported line modules, see *JUNOS Release Notes, Appendix A, System Maximums*.

- Options**
- **atm**—Configures ATM interface parameters for MPLS cross-connect. A local cross-connect enables the router to function as a layer 2 switch. It operates with any supported layer 2 service
 - **vpiStart**—Starting virtual path identifier (inclusive) of the VC subrange you are configuring; number in the range 0–255
 - **vpiEnd**—Ending virtual path identifier (inclusive) of the VC subrange you are configuring; number in the range 0–255
 - **vciStart**—Starting virtual circuit identifier (inclusive) of the VC subrange you are configuring; number in the range 1–65535
 - **vciEnd**—Ending virtual circuit identifier (inclusive) of the VC subrange you are configuring; number in the range 1–65535

Mode Interface Configuration

- Related Topics**
- *Multiple ATM Virtual Circuits over a Single Pseudowire Overview* and *Multiple ATM Virtual Circuits over a Single Pseudowire Example* in the *JUNOS BGP and MPLS Configuration Guide*

mpls-relay disable

Syntax [no] mpls-relay disable

Release Information Command introduced in JUNOS Release 7.1.0.

Description Administratively disables the MPLS shim interface. The MPLS shim interface must exist before this command can be issued. MPLS shim interfaces are administratively enabled by default. The **no** version restores the default condition.

Mode Interface Configuration

mpls reoptimize

Syntax mpls [traffic-eng] reoptimize [*interfaceType interfaceSpecifier*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Performs an immediate check for better paths for all existing LSPs. There is no **no** version.

- Options**
- traffic-eng—Specifies optional keyword for compatibility with non-E Series implementations
 - *interfaceType*—Interface type; see “Interface Types and Specifiers” on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Privileged Exec, User Exec

mpls reoptimize timers frequency

Syntax mpls [traffic-eng] reoptimize timers frequency *seconds*
 no mpls [traffic-eng] reoptimize timers frequency

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the frequency at which existing LSPs are checked for better paths. RSVP-TE adds a random number in the range 0–60 seconds to the specified value to prevent all LSPs from being reoptimized simultaneously. The **no** version restores the default value, 3600 seconds.



NOTE: Low timer values lead to frequent reoptimization of LSPs, which is undesirable for the following reasons:

- Frequent changes to the LSPs increases packet loss.
 - Frequent reoptimization increases the load on the router, especially when the router acts as the LSP head end. The load is particularly noticeable in a scaled network, resulting in high CPU utilization on the router.
-

- Options**
- *traffic-eng*—Specifies optional keyword for compatibility with non-E Series implementations
 - *seconds*—Number of seconds in the range 0–604800; a value of zero means that no reoptimization is performed

Mode Global Configuration

mpls rsvp

Syntax [no] mpls rsvp

Release Information Command introduced in JUNOS Release 7.1.0.

Description Enables RSVP-TE, as does any RSVP-TE-related command. The **no** version disables RSVP-TE.

Mode Global Configuration

mpls rsvp authentication

Syntax [no] { ip | mpls } rsvp authentication

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables MD5 authentication for RSVP on the interface. Enable authentication after configuring the authentication key. The router generates an error message and discards any RSVP messages if you enable authentication before configuring the authentication key, or remove the key while authentication is still enabled. The **no** version disables authentication.

- Options**
- ip—Specifies alternative keyword for compatibility with non-E Series implementations
 - mpls—Specifies JUNOS MPLS implementation

Mode Interface Configuration

mpls rsvp authentication key

Syntax { ip | mpls } rsvp authentication [key *authkey*]
 no { ip | mpls } rsvp authentication [key [*authkey*]]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Assigns a key to the interface for MD5 authentication between RSVP peers. Assign the key before you enable authentication on the interface. The **no** version deletes the MD5 key.



NOTE: Keys of up to 40 characters are supported for non-Juniper Networks implementations. However, a key with more than 16 characters will cause an authenticated link between E Series and M- or T-series routers to be inoperable.

- Options**
- ip—Specifies alternative keyword for compatibility with non-E Series implementations
 - mpls—Specifies JUNOS MPLS implementation
 - *authkey*—Key used to create MD5 digest for messages sent from this interface and to authenticate messages received on this interface; alphanumeric string in the range 1–40 characters

Mode Interface Configuration

mpls rsvp bfd-liveness-detection

Syntax { ip | mpls } rsvp bfd-liveness-detection [minimum-interval *minInterval* |
[minimum-receive-interval *minRecInterval*]
[minimum-transmit-interval *minTransInterval*]] [multiplier *multValue*]

no { ip | mpls } rsvp bfd-liveness-detection

Release Information Command introduced in JUNOS Release 8.1.0.

Description Enables BFD (bidirectional forwarding detection) on an interface running RSVP-TE and defines BFD values to be negotiated between RSVP-TE neighbors for detection of IP data path failures. The **no** version disables BFD on the RSVP-TE interface.



NOTE: BFD sessions might not be maintained when the multiplier value is 1 and configured intervals are very short. We recommend that you do not use a multiplier value of 1 with very short intervals.

- Options**
- ip—Specifies alternative keyword for compatibility with non-E Series implementations
 - mpls—Specifies JUNOS MPLS implementation
 - *minInterval*—Minimum proposed transmit interval and required receive interval for BFD control packets; has the same effect as configuring the minimum receive interval and the minimum transmit interval to the same value; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *minRecInterval*—Minimum interval at which the local peer must receive BFD control packets sent by the remote peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *minTransInterval*—Minimum interval at which the local peer proposes to transmit BFD control packets to the remote peer; number in the range 100–65535 milliseconds—for ES2 4G LM only, the range is 10–65535 milliseconds; default value is 300 milliseconds
 - *multValue*—Detection multiplier value that the remote peer router multiplies by the local peer's negotiated transmit interval to determine the remote peer's BFD liveness detection interval; equal to the number of BFD packets that can be missed before the BFD session is declared down; number in the range 1–255; default value is 3

Mode Interface Configuration

mpls rsvp disable

Syntax [no] mpls rsvp disable

Release Information Command introduced in JUNOS Release 7.1.0.

Description Administratively disables RSVP-TE on the interface. The **no** version reenables RSVP-TE on the interface.

Mode Interface Configuration

mpls rsvp egress-label

Syntax mpls { rsvp | traffic-eng } egress-label { non-null | explicit-null }
 no mpls { rsvp | traffic-eng } egress-label

Release Information Command introduced in JUNOS Release 7.3.0.

Description Specifies that the egress router advertises the explicit null label or a non-null (real) label by means of RSVP-TE. This advertisement ensures that packets received from upstream include a label and that the egress router performs ultimate hop popping. The **no** version restores the default condition, where the egress router advertises the implicit null label for all tunnels (except those requiring PHB) that terminate on the router.

- Options**
- rsvp—Specifies JUNOS implementation
 - traffic-eng—Specifies keyword for compatibility with non-E Series implementations
 - non-null—Advertises a real label, signaling that the egress router pops the last label and performs the IP lookup; this behavior was the default before this release
 - explicit-null—Advertises the explicit null label, signaling that the egress router pops the last label and performs the IP lookup

Mode Global Configuration

mpls rsvp message-bundling

Syntax [no] mpls rsvp message-bundling

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables RSVP-TE to send bundle messages, each of which includes multiple standard RSVP-TE messages, to reduce the overall message-processing overhead. The **no** version disables RSVP-TE message bundling.

Mode Global Configuration

mpls rsvp profile

Syntax In Global Configuration mode:

```
mpls rsvp [ interface ] profile [ profileName ]
```

```
no mpls rsvp interface profile profileName
```

In Interface Configuration mode:

```
mpls rsvp profile profileName
```

```
no mpls rsvp profile
```

Release Information Command introduced before JUNOS Release 7.1.0.

Description In Global Configuration mode, creates or modifies a configuration profile for RSVP-TE. Places the CLI in RSVP Configuration mode. If you specify a profile not previously configured, it is created with the factory default settings. If you do not specify a profile name, the factory default profile is assumed. The implicit default RSVP-TE profile specifies a value of 30,000 ms (30 seconds) for the refresh period and a value of 3 for the timeout factor.

Any change to a profile affects all interfaces that use the profile; changes are effective the next time the interface comes up. The **no** version deletes the specified profile. The **no** version deletes the specified profile.

In Interface Configuration mode, creates or enables RSVP-TE on the interface with the factory default profile or the specified profile, or disables RSVP-TE on the interface. The **no** version reverts to the default profile on the interface.

In both modes, if you specify a profile not previously configured, it is created with the factory default settings. If you do not specify a profile name, the factory default profile is assumed. The **no** version deletes the specified profile. The **no** version deletes the specified profile.

- Options**
- **interface**—Keyword required for the **no** version in Global Configuration mode
 - **profileName**—Name of a profile to be created or modified (Global Configuration mode), applied to an interface (Interface Configuration mode), or deleted (both modes); the profile sets the values for the protocol parameters; until you modify the profile settings, the values match those of the implicit default profile

Mode Global Configuration, Interface Configuration

mpls rsvp refresh-reduction

Syntax [no] mpls rsvp refresh-reduction

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables RSVP-TE summary refresh and reliability features, including the message ID object, the message ack object, and summary refresh messages. The **no** version disables summary refresh and reliability.

Mode Global Configuration

mpls rsvp signalling hello

Syntax { ip | mpls } rsvp signalling hello
 [refresh { interval *helloInterval* | misses *helloMisses* }]
 { no | default } { ip | mpls } rsvp signalling hello

Release Information Command introduced in JUNOS Release 7.3.0.

Description In Global Configuration mode, turns on or configures RSVP-TE hello support for all RSVP-TE interfaces on the current virtual router. Automatically creates RSVP-TE or MPLS on the current virtual router if they do not yet exist there. The **no** version turns off hello support on the current VR. The **default** version restores the default configuration, in which RSVP hello support is not enabled.

In Interface Configuration mode and Subinterface Configuration mode, turns on or configures RSVP-TE hello support on the current interface, and overrides the global configuration. Automatically creates RSVP-TE or MPLS on the current virtual router if it is not configured there. This command also creates RSVP-TE on the interface if it is not configured there. The **no** version turns off hello support on the current interface. The **default** version restores the default configuration, in which RSVP hello support is not enabled, and also restores inheritance of the configuration values from the global configuration..

- Options**
- ip—Specifies alternative keyword for compatibility with non-E Series implementations
 - *helloInterval*—Number of milliseconds specifying the interval at which hellos are sent, in the range 1000–60000; default value is 10000
 - *helloMisses*—Number of RSVP-TE hello messages from a peer that can be missed before that hello adjacency peer is considered to be down, in the range 4–10; default value is 4

Mode Global Configuration, Interface Configuration, Subinterface Configuration

mpls rsvp signalling hello graceful-restart

Syntax { ip | mpls } rsvp signalling hello graceful-restart [mode help-neighbor]
no { ip | mpls } rsvp signalling hello graceful-restart

Release Information Command introduced in JUNOS Release 8.0.0.

Description Enables RSVP-TE graceful restart as a restarting node or helper node on the current virtual router. The **no** version disables graceful restart on the current VR.

- Options**
- ip—Specifies alternative keyword for compatibility with non-E Series implementations
 - mode help-neighbor—Specifies the current VR acts only as a graceful restart helper node for neighbors that support RSVP-TE graceful restart

Mode Global Configuration

mpls rsvp signalling hello graceful-restart recovery-time

Syntax { ip | mpls } rsvp signalling hello graceful-restart recovery-time *recoveryTime*
no { ip | mpls } rsvp signalling hello graceful-restart recovery-time

Release Information Command introduced in JUNOS Release 8.0.0.

Description Configures the recovery time for RSVP-TE graceful restart for all interfaces that have RSVP-TE enabled. The **no** version restores the default value.

- Options**
- ip—Specifies alternative keyword for compatibility with non-E Series implementations
 - *recoveryTime*—Time in milliseconds within which you want the neighboring routers to resynchronize RSVP-TE state and MPLS forwarding state after a graceful restart, in the range 60000–480000; default value is 120000

Mode Global Configuration

mpls rsvp signalling hello graceful-restart restart-time

Syntax { ip | mpls } rsvp signalling hello graceful-restart restart-time *restartTime*
 no { ip | mpls } rsvp signalling hello graceful-restart restart-time

Release Information Command introduced in JUNOS Release 8.0.0.

Description Configures the restart time for RSVP-TE graceful restart for all interfaces that have RSVP-TE enabled. The **no** version restores the default value.

- Options**
- *ip*—Specifies alternative keyword for compatibility with non-E Series implementations
 - *restartTime*—Total time in milliseconds for the sender to gracefully restart RSVP-TE and to re-establish hello communication with RSVP-TE neighbors; in the range 60000–3600000; default value is 60000

Mode Global Configuration

mpls rsvp signalling node-hello

Syntax { ip | mpls } rsvp signalling node-hello
 [refresh { interval *helloInterval* | misses *helloMisses* }]
 { no | default } { ip | mpls } rsvp signalling node-hello

Release Information Command introduced in JUNOS Release 9.0.0.

Description Turns on or configures RSVP-TE hellos to include node IDs as source and destination addresses in the hello packets for all RSVP-TE interfaces on the current virtual router. RSVP-TE hellos based on node ID enable the JUNOS software to interoperate its RSVP-TE graceful restart capability with routers that cannot support RSVP-TE graceful restart with link-based hellos.

The **no** version turns off node-hello support on the current VR. The **default** version restores the default configuration, in which RSVP node hello support is not enabled.



NOTE: Node hellos are required only for interoperability with some non-E Series implementations. Node hellos are not required for communications between routers running JUNOS software or for interoperability with routers running JUNOS software.

- Options**
- ip—Specifies alternative keyword for compatibility with non-E Series implementations
 - *helloInterval*—Number of milliseconds specifying the interval at which node hellos are sent, in the range 1000–60000; default value is 10000
 - *helloMisses*—Number of RSVP-TE node hello messages from a peer that can be missed before that hello adjacency peer is considered to be down, in the range 4–10; default value is 4

Mode Global Configuration

mpls signaling-interface

Syntax mpls signaling-interface *interfaceType interfaceSpecifier*
 no mpls signaling-interface

Release Information Command introduced in JUNOS Release 7.1.0.

Description Specifies a particular layer 2 interface as the signaling interface for an MPLS major interface that is stacked on an ATM AAL5 interface. MPLS uses the IPv4 or IPv6 interface stacked on the specified interface for signaling. The **no** version restores the default behavior, wherein MPLS nondeterministically selects a layer 2 interface as the signaling interface.



NOTE: You can configure this command only for interfaces that use the interface label space. For interfaces that use the platform label space, the signaling interface is always next to the MPLS major interface, that is, stacked on the same lower interface and is not configurable.

Options ■ *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Interface Configuration

mpls spf-use-any-best-path

Syntax [no] mpls spf-use-any-best-path

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables the SPF calculations to consider both the best IGP (IS-IS or OSPF) paths and the MPLS tunnel to reach the tunnel endpoint. The **no** version restores the default value, which is to always use the MPLS tunnel to reach the tunnel endpoint—the IGP best paths are not considered.

Mode Router Configuration

mpls statistics label

Syntax [no] mpls statistics label { interface *interfaceName* atm *vpi vci* | *labelValue* }

Release Information Command introduced in JUNOS Release 7.1.0.

Description Enables statistics collection for MPLS in labels. By default, statistics are enabled for in labels depending on the protocol that added the in label to the MPLS forwarding table. Statistics are not stored in NVS. The **no** version disables statistics collection.

- Options**
- *interfaceName*—Name of interface for label in interface label space on an ATM AAL5 interface; up to 15 alphanumeric characters
 - *vpi*—Virtual path identifier for a label, a value in the range 0–255
 - *vci*—Virtual circuit identifier for a label, a value in the range 33–65535
 - *labelValue*—Integer identifying a label in the platform label space, a value in the range 16–1048575

Mode Global Configuration

mpls statistics next-hop

Syntax [no] mpls statistics next-hop *nextHopIndex*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Enables statistics collection for MPLS next hops. By default, statistics are enabled for next hops depending on the protocol that created the MPLS next hop. Statistics are not stored in NVS. The **no** version disables statistics collection.

Options ■ *nextHopIndex*—Integer uniquely identifying a next hop; in the range 1–1048575

Mode Global Configuration

mpls statistics policy

Syntax [no] mpls statistics policy *tunnelName*

Release Information Command introduced in JUNOS Release 7.1.0.

Description Enables statistics collection for policies attached to an MPLS tunnel. Statistics are not stored in NVS. The **no** version disables statistics collection.

Options ■ *tunnelName*—Name of the MPLS tunnel

Mode Global Configuration

mpls topology-driven-lsp

Syntax [no] mpls topology-driven-lsp

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables topology-driven LSP creation on the virtual router where the LSR automatically creates LSPs when it learns a new IGP route. In the context of the VRF virtual router, enables carrier-of-carriers support on the provider carrier's PE router.

The router advertises labels for new routes immediately to all peers without waiting for a label request message from an upstream peer or a label mapping message from a downstream peer. This mode is downstream-unsolicited, independent control.

The **no** version disables topology-driven LSPs on the virtual router.

Mode Global Configuration

mpls topology-driven-lsp ip-interfaces

Syntax [no] mpls topology-driven-lsp ip-interfaces [egress | ingress]
 [{ access-list | prefix-list } *listName*] [host-only]

no mpls topology-driven-lsp ip-interfaces [egress | ingress] [host-only]
 [policy-list]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies LSPs to be put into the IP routing table for forwarding plain IP traffic. The **no** version removes the LSPs from the table.



NOTE: This command is deprecated and may be removed completely in a future release. The function provided by this command has been replaced by the **ldp ip-forwarding** command.

- Options**
- egress—Has no effect
 - ingress—Has no effect
 - access-list—Specifies that *listName* is an access list
 - prefix-list—Specifies that *listName* is a prefix list
 - *listName*—Name of access list or prefix list that specifies LSPs over which IP interfaces are created
 - host-only— Specifies that only LSPs to host addresses are added to the IP routing table
 - policy-list—Removes previously applied access lists or prefix lists

Mode Global Configuration

mpls traffic-class

Syntax [no] mpls traffic-class *className* [scheduler-profile *profileName*]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies traffic class for which LSP-level queues are created. The **no** version deletes the traffic class.

- Options**
- *className*—Name of a traffic class; the router supports up to eight traffic classes
 - *profileName*—Name of a scheduler profile to associate with the traffic class

Mode Global Configuration

mpls traffic-eng

Syntax mpls traffic-eng level-1 | level-2
 no mpls traffic-eng level-1 | level-2

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables flooding of MPLS traffic-engineering link information into the specified IS-IS level. Flooding is disabled by default. The **no** version disables flooding.

- Options** ■ level-1—Floods IS-IS level 1
 ■ level-2—Floods IS-IS level 2

Mode Router Configuration

mpls traffic-eng administrative-weight

Syntax mpls traffic-eng administrative-weight *weight*
 no mpls traffic-eng administrative-weight

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the administrative weight for the interface. The **no** version restores the default value, which matches the IGP-determined weight (cost).

Options ■ *weight*—Administrative weight, a value in the range 0–4294967295 supersedes any weight conferred upon the link by the IGP

Mode Interface Configuration, Subinterface Configuration

mpls traffic-eng area

Syntax [no] mpls traffic-eng area { *areaId* | *areaIdInt* }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Enables flooding of MPLS traffic-engineering link information into the specified OSPF area. Flooding is disabled by default. The **no** version disables flooding.

- Options**
- *areaId*—OSPF area ID in IP address format
 - *areaIdInt*—OSPF area ID as a decimal value in the range 0–4294967295

Mode Router Configuration

mpls traffic-eng attribute-flags

Syntax mpls traffic-eng attribute-flags *bitmask*
 no mpls traffic-eng attribute-flags

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies attributes for the interface for traffic engineering. The attributes are compared with tunnel affinity bits to determine links eligibility for the tunnel. The **no** version restores the default value, 0x0.

Options ■ *bitmask*—Mask that sets the attributes, a value in the range 0x0–0xFFFFFFFF

Mode Interface Configuration, Subinterface Configuration

mpls traffic-eng egress-label

Syntax mpls { rsvp | traffic-eng } egress-label { non-null | explicit-null }
 no mpls { rsvp | traffic-eng } egress-label

Description Specifies that the egress router advertises the explicit null label or a non-null label by means of RSVP-TE. See the **mpls rsvp egress-label** command for a complete description and syntax.

Mode Global Configuration

mpls traffic-eng flood thresholds

Syntax mpls traffic-eng flood thresholds { up | down } *percentage* [*percentage*]*
 no mpls traffic-eng flood thresholds { up | down }

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies thresholds for the flooding of the current reservable bandwidth throughout the network. You can configure a set of thresholds for increases or decreases in bandwidth. Flooding is triggered when the reservable bandwidth increases past any up threshold or decreases past any down threshold. The **no** version restores the following default values:

- For increases in bandwidth (up changes)—15, 30, 45, 60, 75, 80, 85, 90, 95, 97, 98, 99, 100
- For decreases in bandwidth (down changes)—100, 99, 98, 97, 96, 95, 90, 85, 80, 75, 60, 45, 30, 15

Options ■ up—Specifies that an increase in bandwidth past the threshold triggers flooding
 ■ down—Specifies that a decrease in bandwidth past the threshold triggers flooding
 ■ *percentage*—Percentage of reservable bandwidth, a value from 1 to 100 percent for increasing bandwidth and from 0 to 99 percent for decreasing bandwidth
 ■ *—Indicates that the percentage can be repeated multiple times in a list in the command line

Mode Interface Configuration, Subinterface Configuration

mpls traffic-eng link-management timers periodic-flooding

Syntax mpls traffic-eng link-management timers periodic-flooding *frequency*
 no mpls traffic-eng link-management timers periodic-flooding

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies the interval at which bandwidth values are flooded to the entire network. Configuring a value of 0 turns off flooding. The **no** version restores the default value, 180.

Options ■ *frequency*—Interval in seconds, a value in the range 0–3600

Mode Global Configuration

mpls traffic-eng multicast-intact

Syntax [no] mpls traffic-eng multicast-intact

Release Information Command introduced in JUNOS Release 7.1.0.

Description Enables a multicast network and MPLS traffic engineering (TE) network to interoperate on a router running OSPF. The **no** version disables interoperability between multicast protocols and MPLS-TE.

Mode Router Configuration

mpls traffic-eng router-id

Syntax [no] mpls traffic-eng router-id *interfaceType interfaceSpecifier*

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies a stable interface to be used as a router ID for MPLS traffic engineering with IS-IS or OSPF, typically a loopback interface. The interface acts as the destination node for tunnels originating at other nodes. The **no** version removes the interface as a router ID.

- Options**
- *interfaceType*—Interface type; see Interface Types and Specifiers on page 5
 - *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5

Mode Router Configuration

mpls tunnel-model

Syntax mpls tunnel-model { pipe | uniform }
 no mpls tunnel-model

Release Information Command introduced before JUNOS Release 7.1.0.

Description Specifies whether MPLS employs the pipe or uniform tunnel model for differentiated services. The **no** version restores the default, the pipe model.

- Options** ■ pipe-model—Specifies that the pipe model is followed
 ■ uniform-model—Specifies that the uniform model is followed

Mode Global Configuration

mpls tunnels profile

Syntax [no] mpls tunnels profile *profileName* [disable]

Release Information Command introduced before JUNOS Release 7.1.0.

Description Creates or disables a tunnel profile for MPLS. The **no mpls tunnels profile** version deletes the tunnel profile. The **no mpls tunnels profile disable** version reenables tunnels previously disabled.

- Options**
- *profileName*—Name of a tunnel configuration profile used for MPLS tunnels
 - **disable**—Disables all tunnels associated with the profile

Mode Global Configuration

mrout port admission-bandwidth-limit

Syntax `mrout port portNumber admission-bandwidth-limit limitValue`
 `[priority-bandwidth-limit priorityBandwidthValue] [hysteresis hysteresisValue]`
 `no mrout port portNumber admission-bandwidth-limit`

Release Information Command introduced in JUNOS Release 7.1.0.
 hysteresis and **priority-bandwidth limit** keywords and *hysteresisValue* and *priorityBandwidthValue* variables added in JUNOS Release 8.2.0.

Description Configures a limit on the admission bandwidth of outgoing interfaces (OIFs) containing IPv4 or IPv6 mroutes, across different virtual routers, on a port. The **no** version removes any OIF admission bandwidth limits.

- Options**
- *portNumber*—Port number in the form *slot/port*.
 - *limitValue*—Limit on the admission bandwidth (in bits per second) of outgoing interfaces containing IPv4 or IPv6 mroutes, across different virtual routers, on a port. The default is no limit.
 - *priorityBandwidthValue*— Minimum value of admitted priority bandwidth in bps. The default is no limit.
 - *hysteresisValue*—Minimum priority bandwidth limit before the system evaluates mroutes and admits any blocked OIFs; in the range 0-100 percent.

Mode Global Configuration

mroute port limit

Syntax mroute port *portNumber* limit *limitValue*
 no mroute port *portNumber* limit

Release Information Command introduced before JUNOS Release 7.1.0.

Description Configures a limit on the number of outgoing interfaces (OIFs) containing IPv4 or IPv6 mroutes, across different virtual routers, on a port. The **no** version removes any OIF port limits.

- Options** ■ *portNumber*—Port number in the form *slot/port*.
 ■ *limitValue*—Limit on the number of outgoing interfaces containing IPv4 or IPv6 mroutes, across different virtual routers, on a port. The default is no limit.

Mode Global Configuration

mru

Syntax `mru mruSize`

`no mru`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Sets the maximum allowable size in bytes of the maximum receive unit for interfaces on cOCx/STMx, COCX-F3, CT3, and POS modules. The **no** version restores the default value, which varies according to module type.

- Options** ■ *mruSize*—Maximum allowable size of the MRU; default and range varies with module type:
- Interfaces on cOCx/STMx, CT3, and COCX-F3 modules—Number in the range 4–9996; default value is 1600
 - Interfaces on POS modules—Number in the range 1–9996; default value is 4470

Mode Interface Configuration

mtrace

Syntax `mtrace sourceAddress [destinationAddress [groupAddress [responseAddress]]]`
`[maxHops] [detailed]`

Release Information Command introduced before JUNOS Release 7.1.0.

Description Discovers the routes that multicast packets follow when travelling to their destinations. There is no **no** version.

- Options**
- *sourceAddress*—DNS name or unicast IP address of the multicast-capable device at the beginning of the path.
 - *destinationAddress*—DNS name or unicast address of the device at the end of the path. The default destination is the router from which you type the command.
 - *groupAddress*—DNS name or multicast address of the group for which you want to trace routes. The default address is 224.2.0.1 (the group used for MBONE Audio).
 - *responseAddress*—IP address that receives the results of the trace
 - *maxHops*—Maximum number of hops allowed for the trace; default value is 64.
 - *detailed*—Provides a detailed description of the trace, rather than a summary

Mode Privileged Exec, User Exec

mtu

Syntax `mtu mtuSize``no mtu`**Release Information** Command introduced before JUNOS Release 7.1.0.**Description** Sets the maximum allowable size in bytes of the maximum transmission unit for interfaces on cOCx/STMx, CT3, COCX-F3, Ethernet, or POS modules. The **no** version restores the default value, which varies according to module type. This command is not available for the Ethernet interface on the SRP module.

- Options**
- *mtuSize*—Maximum allowable size of the MTU; default and range varies with interface type:
 - Interfaces on cOCx/STMx, CT3, and COCX-F3 modules—Number in the range 4–9996; default value is 1600
 - Interfaces on Ethernet modules—Number in the range 64–9188, except on the FE-2 and FE-8 I/O modules, where the range is 64–9042; you cannot configure MTU on Ethernet interfaces on the SRP module; default value is 1518
 - Interfaces on POS modules—Number in the range 1–9996; default value is 4470

Mode Interface Configuration

multicast

Syntax multicast { permit | deny }

no multicast

Release Information Command introduced before JUNOS Release 7.1.0.

Description Modifies the subscriber policy for the multicast protocol to define whether the subscriber (client) interfaces that belong to a bridge group or to a VPLS instance forward (permit) or filter (deny) multicast packets. The **no** version restores the default value, permit multicast packets.

You cannot change the default subscriber policy values for trunk (server) interfaces that belong to a bridge group or to a VPLS instance. You also cannot change the default subscriber policy values for a VPLS virtual core interface, which acts as a trunk interface. The VPLS virtual core interface represents all of the MPLS tunnels from the router to the remote VPLS edge (VE) devices.

- Options**
- permit—Specifies that the subscriber interface associated with the bridge group or VPLS instance forwards multicast packets
 - deny—Specifies that the subscriber interface associated with the bridge group or VPLS instance filters multicast packets

Mode Subscriber Policy Configuration

multicast group port limit

Syntax multicast group port *interfaceSpecifier* limit *groupLimit*
 no multicast group port *interfaceSpecifier* limit

Release Information Command introduced before JUNOS Release 7.1.0.

Description Limits the number of IGMP or MLD groups that a port can accept. The **no** version restores the default situation, in which there is no limit to the number of IGMP or MLD groups the port can accept.

- Options** ■ *interfaceSpecifier*—Particular interface; format varies according to interface type; see Interface Types and Specifiers on page 5
- *groupLimit*—Maximum number of IGMP or MLD groups that an interface can accept in the range 0–64,000

Mode Global Configuration

Part 2

Index

- Index on page 1445

Index

Symbols

10-Gigabit Ethernet interface.....	18
802.3ad Link Aggregation	
minimum member links.....	1321
802.3ah OAM link-fault management	
enabling on an interface.....	581

A

AAA commands

aaa accounting acct-stop on-aaa-failure.....	22
aaa accounting acct-stop on-access-deny.....	23
aaa accounting broadcast.....	24
aaa accounting commands.....	25
aaa accounting default.....	26
aaa accounting duplication.....	27
aaa accounting exec.....	28
aaa accounting immediate-update.....	29
aaa accounting interval.....	30
aaa accounting statistics.....	31
aaa accounting suppress null-username.....	32
aaa accounting vr-group.....	33
aaa authentication default.....	34
aaa authentication enable default.....	35
aaa authentication login.....	36
aaa authorization.....	37
aaa authorization config-commands.....	38
aaa delimiter.....	39
aaa dns.....	41
aaa duplicate-address-check.....	43
aaa intf-desc-format include.....	44
aaa ipv6-dns.....	45
aaa local database.....	47
aaa local select database.....	48
aaa local username.....	49
aaa new-model.....	50
aaa parse-direction.....	51
aaa parse-order.....	52
aaa qos downstream rate.....	54
aaa route-download.....	55
aaa route-download now.....	56
aaa route-download suspend.....	57
aaa service accounting interval.....	58
aaa subscriber limit per-port.....	59

aaa subscriber limit per-vr.....	60
aaa timeout.....	61
aaa tunnel assignment-id-format.....	62
aaa tunnel calling-number-format.....	63
aaa tunnel calling-number-format-fallback.....	66
aaa tunnel client-name.....	68
aaa tunnel ignore.....	70
aaa tunnel nas-port-method.....	71
aaa tunnel password.....	72
aaa tunnel switch-profile.....	73
aaa tunnel tx-connect-speed-method.....	74
aaa tunnel-group.....	69
aaa user accounting interval.....	75
aaa virtual-router.....	76
aaa wins.....	77
accounting.....	80
authorization.....	200
baseline aaa.....	216
baseline aaa route-download.....	217
clear ip routes download.....	406
login authentication.....	1253
AAA domain map commands	
aaa domain-map.....	42
auth-router-name.....	201
ip-router-name.....	935
ipv6-local-interface.....	1034
local-interface.....	1233
AAA profile commands	
aaa profile.....	53
allow.....	112
deny.....	508
ANCP commands	
adjustment-factor.....	107
baseline l2c.....	347
clear l2c discovery-table.....	424
clear l2c neighbor.....	425
gsmpp-syn-timeout.....	678
id.....	696
l2c.....	1150
l2c end-user-id.....	1151
l2c ip listen.....	1152
l2c ip oif.....	1153
l2c line-configuration.....	1154
l2c max-branches.....	1155
l2c peer-attachment-id.....	1157

max-branches.....	1293
max-discovery-table-entries.....	1294
APS/MSP commands	
aps force.....	116
aps group.....	117
aps lockout.....	118
aps manual.....	119
aps protect.....	120
aps revert.....	121
aps unidirectional.....	122
aps working.....	123
ARP commands	
arp.....	142
arp spoof-check.....	144
arp timeout.....	145
clear arp.....	363
ip proxy-arp.....	918
ATM 1483 subinterface.....	6, 14
ATM commands	
atm.....	147
atm aal5 description.....	148
atm aal5 shutdown.....	149
atm aal5 snmp trap link-status.....	150
atm atm1483 advisory-rx-speed.....	151
atm atm1483 auto-configure.....	152
atm atm1483 description.....	153
atm atm1483	
export-subinterface-description.....	154
atm atm1483 mtu.....	155
atm atm1483 profile.....	156
atm atm1483 shutdown.....	157
atm atm1483 snmp trap link-status.....	158
atm atm1483 subscriber.....	159
atm auto-configuration.....	160
atm bulk-config.....	161
atm bulk-config modify.....	162
atm bulk-config shutdown.....	163
atm cac.....	164
atm cell-packing.....	165
atm class-vc.....	168
atm clock internal.....	169
atm description.....	170
atm framing.....	172
atm ilmi-enable.....	173
atm ilmi-keepalive.....	174
atm lbo.....	175
atm mcpt-timers.....	176
atm oam.....	177
atm oam flush.....	178
atm oam loopback-location.....	179
atm pvc.....	182
atm shutdown.....	185
atm snmp trap link-status.....	186
atm sonet stm-1.....	187
atm uni-version.....	188
atm vc-per-vp.....	189

atm vp-description.....	190
atm vp-tunnel.....	193
atm-vp qos-parameter.....	191
atm-vp qos-profile.....	192
auto-configure.....	203
auto-configure atm1483.....	204
baseline atm vp interface.....	218
baseline interface atm.....	228
cbr.....	353
class-int.....	359
class-vc.....	360
ds3-scramble.....	549
e3-scramble.....	556
encapsulation.....	563
inarp.....	709
interface atm.....	719
ip atm-vc.....	747
load-interval.....	1230
loopback.....	1255
map-group.....	1264
map-list.....	1265
monitor atm vc.....	1331
monitor atm vp.....	1332
ATM interface.....	6, 14

B

B-RAS commands

aaa accounting acct-stop on-aaa-failure.....	22
aaa accounting acct-stop on-access-deny.....	23
aaa accounting broadcast.....	24
aaa accounting commands.....	25
aaa accounting default.....	26
aaa accounting duplication.....	27
aaa accounting exec.....	28
aaa accounting immediate-update.....	29
aaa accounting interval.....	30
aaa accounting statistics.....	31
aaa accounting suppress null-username.....	32
aaa accounting vr-group.....	33
aaa authentication default.....	34
aaa delimiter.....	39
aaa dhcpv6-delegated-prefix	
delegated-ipv6-prefix.....	40
aaa dns.....	41
aaa domain-map.....	42
aaa duplicate-address-check.....	43
aaa intf-desc-format include.....	44
aaa ipv6-dns.....	45
aaa ipv6-nd-ra-prefix framed-ipv6-prefix.....	46
aaa local database.....	47
aaa local select database.....	48
aaa local username.....	49
aaa parse-direction.....	51
aaa parse-order.....	52
aaa profile.....	53

aaa qos downstream rate.....	54
aaa route-download.....	55
aaa route-download now.....	56
aaa route-download suspend.....	57
aaa service accounting interval.....	58
aaa subscriber limit per-port.....	59
aaa subscriber limit per-vr.....	60
aaa timeout.....	61
aaa tunnel assignment-id-format.....	62
aaa tunnel calling-number-format.....	63
aaa tunnel calling-number-format-fallback.....	66
aaa tunnel client-name.....	68
aaa tunnel ignore.....	70
aaa tunnel nas-port-method.....	71
aaa tunnel password.....	72
aaa user accounting interval.....	75
aaa virtual-router.....	76
aaa wins.....	77
accounting.....	80
address.....	85
address-pool-name.....	101
allow.....	112
auth-router-name.....	201
authorization change.....	201
backup-address-pool-name.....	212
baseline aaa.....	216
baseline aaa route-download.....	217
baseline cops.....	223
baseline dhcp.....	224
baseline local pool.....	254
baseline radius.....	263
baseline radius dynamic-request.....	264
baseline radius relay.....	265
baseline ssc.....	269
baseline tacacs.....	271
bridge1483 service-profile.....	311
clear ip demux.....	385
clear ip routes download.....	406
deadtime.....	478
deny.....	508
dhcp delete-binding.....	510
dhcp-external delete-binding.....	513
dhcp-external duplicate-mac-address.....	514
dhcpv6 delete-binding.....	515
domain.....	537
grace-period.....	671
include circuit-identifier.....	710
include dhcp-option 82.....	711
include hostname.....	712
include ip-address.....	713
include mac-address.....	714
include virtual-router-name.....	715
ip address-pool.....	740
ip auto-configure ip-subscriber.....	748
ip auto-detect ip-subscriber.....	749
ip dhcp-capture.....	762
ip dhcp-external auto-configure.....	763
ip dhcp-external disregard-giaddr-next-hop.....	764
ip dhcp-external	
recreate-subscriber-interface.....	765
ip dhcp-external server-address.....	766
ip dhcp-external server-sync.....	767
ip dhcp-server.....	779
ip inactivity-timer.....	842
ip local alias.....	846
ip local pool.....	847
ip local pool snmpTrap.....	848
ip local pool warning.....	849
ip local shared-pool.....	850
ip re-authenticate-auto-detect ip-subscriber.....	919
ip route-map ip-subscriber.....	932
ip service-profile.....	945
ip use-framed-routes ip-subscriber.....	968
ip-hint.....	808
ip-router-name.....	935
ipv6-prefix-pool-name.....	1108
ipv6-router-name.....	1112
key.....	1146
l2tp rx-connect-speed-when-equal.....	1186
license b-ras.....	1213
logout subscribers.....	1254
loopback.....	1255
max-sessions.....	1301
medium ipv4.....	1310
BFD commands	
address bfd-liveness-detection.....	92
clear ipv6 bfd session.....	409
ip ospf bfd-liveness-detection.....	884
ip pim bfd-liveness-detection.....	895
ip rip bfd-liveness-detection.....	925
ip route.....	929
ipv6 ospf bfd-liveness-detection.....	1080
ipv6 pim bfd-liveness-detection.....	1090
isis bfd-liveness-detection.....	1123
license bfd.....	1212
mpls rsvp bfd-liveness-detection.....	1406
BGP commands	
address-family.....	95
aggregate-address.....	109
auto-summary.....	208
baseline ip bgp.....	230
bgp advertise-best-external-to-internal.....	275
bgp advertise-inactive.....	276
bgp always-compare-med.....	277
bgp bestpath med confed.....	278
bgp bestpath missing-as-worst.....	279
bgp client-to-client reflection.....	280
bgp cluster-id.....	281
bgp confederation identifier.....	282
bgp confederation peers.....	283
bgp dampening.....	284
bgp default ipv4-unicast.....	285

bgp default local-preference.....	286
bgp default route-target filter.....	287
bgp enforce-first-as.....	288
bgp fast-external-fallover.....	289
bgp graceful-restart.....	290
bgp graceful-restart	
path-selection-defer-time-limit.....	291
bgp graceful-restart restart-time.....	292
bgp graceful-restart stalepaths-time.....	293
bgp log-neighbor-changes.....	294
bgp maxas-limit.....	295
bgp redistribute-internal.....	296
bgp router-id.....	297
bgp shutdown.....	298
bgp wait-on-end-of-rib.....	299
check-vpn-next-hops.....	356
clear access-list.....	362
clear bgp ipv6.....	366
clear bgp ipv6 dampening.....	367
clear bgp ipv6 dynamic-peers.....	369
clear bgp ipv6 redistribution.....	370
clear bgp ipv6 wait-end-of-rib.....	370
clear ip bgp.....	378
clear ip bgp dampening.....	380
clear ip bgp dynamic-peers.....	382
clear ip bgp redistribution.....	383
clear ip bgp wait-end-of-rib.....	384
clear ip routes.....	405
clear ip tunnel-routes.....	407
clear ipv6 access-list.....	408
clear ipv6 routes.....	419
clear ipv6 tunnel-routes.....	420
debug ip bgp.....	482
debug ip mbgp.....	484
default-fields peer.....	497
default-fields route.....	499
default-information originate.....	501
disable-dynamic-redistribute.....	521
distance bgp.....	529
exit-address-family.....	616
export map.....	620
external-paths.....	623
global export map.....	664
global import map.....	665
import map.....	708
ip as-path access-list.....	745
ip bgp-community new-format.....	750
ip bgp-confed-as-set new-format.....	751
ip community-list.....	757
ip extcommunity-list.....	797
ip fallback global.....	798
ip route parent-router.....	929
ip route vrf.....	929
ip route-type.....	933
ip vrf.....	970
ip vrf forwarding.....	971
match as-path.....	1276
match community.....	1277
match distance.....	1277
match extcommunity.....	1279
match ip address.....	1280
match ip next-hop.....	1281
match level.....	1285
match metric.....	1286
match metric-type.....	1287
match mpls-label.....	1288
match policy-list.....	1289
match route-type.....	1290
match tag.....	1292
maximum routes.....	1296
maximum-paths.....	1295
bgp commands	
match description.....	1442
BGP/MPLS VPN commands	
address-family.....	95
bgp default route-target filter.....	287
bgp wait-on-end-of-rib.....	299
check-vpn-next-hops.....	356
clear ip routes vrf.....	405
clear ip tunnel-routes vrf.....	407
clear ipv6 routes vrf.....	419
clear ipv6 tunnel-routes vrf.....	420
debug ip mbgp.....	484
default-information originate.....	501
domain-id.....	540
domain-tag.....	545
dont-install-routes.....	546
exit-address-family.....	616
export map.....	620
global export map.....	664
global import map.....	665
import map.....	708
ip dynamic-interface-prefix.....	795
ip fallback global.....	798
ip mpls forwarding-mode label-switched.....	861
ip route parent-router.....	929
ip route vrf.....	929
ip share-interface.....	946
ip share-nexthop.....	947
ip vrf.....	970
ip vrf forwarding.....	971
ipv6 share-interface.....	1118
match mpls-label.....	1288
maximum routes.....	1296
maximum-paths.....	1295
mpls topology-driven-lsp.....	1422
neighbor activate.....	299
BGP/MPLS VPNs commands	
external-paths.....	623
booting commands	
boot backup.....	301
boot config.....	302

- boot force-backup.....303
- boot hotfix.....304
- boot revert-tolerance.....305
- boot revert-tolerance never.....306
- boot subsystem.....307
- boot system.....308
- check-disk.....355
- delete.....506
- flash-disk compare.....631
- flash-disk duplicate.....632
- flash-disk initialize.....633
- flash-disk scan.....634
- mount.....1336
- bridged Ethernet commands
 - bridge1483 mtu.....310
 - bridge1483 service-profile.....311
 - encapsulation bridge1483.....564
 - ip mac-validate.....851
- bridged IP commands
 - encapsulation bridge1483.....564
- bridging commands
 - arp.....142
 - baseline bridge.....219
 - baseline bridge interface.....220
 - bridge.....312
 - bridge acquire.....313
 - bridge address.....314
 - bridge aging-time.....316
 - bridge crb.....317
 - bridge learn.....319
 - bridge route.....320
 - bridge snmp-trap link-status.....321
 - bridge subscriber-policy.....322
 - bridge-group.....318
 - broadcast.....330
 - clear bridge.....372
 - clear bridge address.....373
 - clear bridge interface.....374
 - ip.....735
 - mpls.....1337
 - multicast.....1441
- C**
- Cisco HDLC commands
 - baseline hdlc interface.....227
 - encapsulation hdlc.....566
 - hdlc down-when-looped.....683
 - hdlc keepalive.....684
 - hdlc shutdown.....685
- CLI commands. *See* user interface commands
- CLNS commands
 - clns configuration-time.....434
 - clns holding-time.....435
 - clns host.....436
- COCX-F3 commands
 - interface serial.....731
- cOCx/STMx commands
 - baseline path interface sonet.....260
 - baseline section interface sonet.....266
 - controller sonet.....462
 - crc.....472
 - interface serial.....731
 - loopback.....1255
 - mru.....1438
 - mtu.....1440
- cOCx/STMx commands and OCx/STMx commands
 - description.....509
- conventions
 - notice icons.....xxxix
 - text and syntax.....xl
- CT3 commands
 - bert.....273
 - crc.....472
 - description.....509
 - equipment loopback.....577
 - idle-character.....698
 - invert data.....734
 - loopback.....1255
 - mdl carrier.....1303
 - mdl string.....1304
 - mdl transmit.....1305
 - mru.....1438
 - mtu.....1440
- customer support.....xli
 - contacting JTAC.....xli
- D**
- default commands vs. no commands.....3
- deprecated commands.....4
- DHCP commands
 - clear ip dhcp-local binding.....386
 - ip dhcp-capture.....762
 - ip dhcp-local auth domain.....768
 - ip dhcp-local auth include.....769
 - ip dhcp-local auth password.....770
 - ip dhcp-local auth user-prefix.....771
- DHCP external server commands
 - dhcp-external duplicate-mac-address.....514
 - ip dhcp-external recreate-subscriber
 - interface.....765
- DHCP local server commands
 - ip dhcp-local
 - auto-configureagent-circuit-identifier.....772
 - ip dhcp-local cable-modem.....773
 - ip dhcp-local snmp Traps.....777
 - link.....1224
- DHCPv6 local server commands
 - ipv6 dhcpv6-local delegated-prefix.....1022
 - ipv6 dhcpv6-local dns-domain-search.....1023

ipv6 dhcpv6-local dns-server.....	1024
ipv6 dhcpv6-local prefix-lifetime.....	1025
Diagnostic commands	
diag.....	516
diag-level.....	517
Digital certificate commands	
common-name.....	451
country.....	471
crl.....	473
domain-name.....	543
enrollment retry-limit.....	574
enrollment retry-period.....	575
enrollment url.....	576
ike crl.....	702
ipsec ca authenticate.....	991
ipsec ca enroll.....	992
ipsec ca identity.....	993
ipsec certificate-database refresh.....	994
ipsec certificate-request generate.....	995
ipsec crl	997
ipsec identity.....	998
ipsec key generate	1001
ipsec key pubkey-chain rsa.....	1003
ipsec key zeroize.....	1004
issuer-identifier.....	1139
key-string.....	1148
DNS commands	
ip domain-lookup.....	782
ip domain-name.....	783
ip name-server.....	870
documentation set	
comments on.....	xli
DoS protection group commands	
atm dos-protection-group.....	171
bridge1483 dos-protection-group.....	309
dos-protection-group.....	547
ethernet dos-protection-group.....	580
frame-relay dos-protection-group.....	643
hdlc dos-protection-group.....	682
ip dos-protection-group.....	784
ipv6 dos-protection-group.....	1026
lag dos-protection-group.....	1210
DVMRP commands	
baseline ip dvmrp.....	233
clear ip dvmrp routes.....	387
disable.....	519
disable-dynamic-redistribute.....	521
dvmrp destination profile.....	554
ip dvmrp.....	785
ip dvmrp accept-filter.....	786
ip dvmrp announce-filter.....	787
ip dvmrp auto-summary.....	788
ip dvmrp disable.....	789
ip dvmrp metric-offset.....	790
ip dvmrp route-limit.....	792
ip dvmrp routehog-notification.....	791

ip dvmrp summary-address.....	793
ip dvmrp unicast-routing.....	794
dynamic interface commands	
atm atm1483 advisory-rx-speed.....	151
atm atm1483 auto-configure.....	152
atm atm1483 description.....	153
atm atm1483 profile.....	156
atm atm1483 subscriber.....	159
atm bulk-config.....	161
atm bulk-config modify.....	162
atm bulk-config shutdown.....	163
atm pvc.....	182
auto-configure.....	203
auto-configure atm1483.....	204
auto-configure vlan.....	205

E

E120 routers	
interface types and specifiers.....	13
E3 commands	
atm framing.....	172
clock source.....	438
controller e3.....	461
crc.....	472
description.....	509
framing.....	658
load-interval.....	1230
loopback.....	1255
mru.....	1438
mtu.....	1440
E320 routers	
interface types and specifiers.....	13
ERX14xx models	
interface types and specifiers.....	5
ERX310 router	
interface types and specifiers.....	5
ERX7xx models	
interface types and specifiers.....	5
Ethernet commands	
baseline interface fastEthernet.....	228
baseline interface gigabitEthernet.....	228
debounce.....	479
debounce-interval.....	480
duplex.....	553
ethernet description.....	579
interface fastEthernet.....	721
interface gigabitEthernet.....	722
interface lag.....	725
interface tenGigabitEthernet.....	732
ip mac-validate.....	851
lacp.....	1208
lacp port-priority.....	1209
link-fault management	
ethernet oam lfm.....	581
ethernet oam lfm high-threshold.....	582

- ethernet oam lfm link-monitor
 - frame-seconds.....583
- ethernet oam lfm link-monitor
 - frame-seconds-summary.....585
- ethernet oam lfm link-monitor
 - symbol-period.....587
- ethernet oam lfm mode.....589
- ethernet oam lfm pdu-lost-threshold.....590
- ethernet oam lfm pdu-transmit-interval
 -591
- ethernet oam lfm remote-failure.....592
- ethernet oam lfm remote-loopback.....594
- ethernet oam lfm remote-loopback
 - supported.....595
- member-interface.....1312
- monitor vlan interface.....1333
- mtu.....1440
- Event Manager commands
 - boolean-test.....300
 - existence-test.....614
- F**
- Fast Ethernet commands
 - load-interval.....1230
- Fast Ethernet interface.....7, 15
- file management commands
 - copy.....465
 - copy running-configuration.....467
 - copy running-configuration
 - startup-configuration.....468
 - copy startup-configuration.....469
 - host.....691
 - hotfix activate.....693
- filtering show commands.....4
- flow statistics commands
 - cache entries.....350
 - cache timeout.....351
 - enabled.....558
 - export destination.....619
 - export source.....621
 - ip flow statistics.....805
 - ip flow-aggregation cache800
 - ip flow-cache entries.....801
 - ip flow-cache timeout.....802
 - ip flow-export.....803
 - ip flow-sampling-mode packet-interval.....804
 - mask destination.....1272
 - mask source.....1274
- Frame Relay commands
 - baseline frame-relay interface.....225
 - encapsulation frame-relay ietf.....565
 - frame-relay class.....640
 - frame-relay description.....642
 - frame-relay fragment.....644
 - frame-relay interface-dlci ietf.....645
 - frame-relay intf-type.....646
 - frame-relay keepalive.....647
 - frame-relay lmi-n391dte.....648
 - frame-relay lmi-n392dce.....649
 - frame-relay lmi-n392dte.....650
 - frame-relay lmi-n393dce.....651
 - frame-relay lmi-n393dte.....652
 - frame-relay lmi-t391dte.....653
 - frame-relay lmi-t392dce.....654
 - frame-relay lmi-type.....655
 - map-class frame-relay.....1263
- FTP client commands
 - ip ftp source-address.....806
 - ip ftp source-interface.....807
- FTP server commands
 - delete.....506
 - ftp-server enable.....660
 - ftp-server flush.....661
- G**
- GE port redundancy commands
 - link failover arp-flush.....1225
 - link failover force.....1226
 - link failover timeout.....1227
 - link selection.....1228
- Gigabit Ethernet interface.....8, 15
- GRE commands
 - gre destination profile.....672
 - gre-tunnel classifier-list.....674
 - gre-tunnel policy.....675
 - gre-tunnel policy-list.....676
- H**
- HDLC commands, Cisco
 - baseline hdlc interface.....227
 - encapsulation hdlc.....566
 - hdlc down-when-looped.....683
 - hdlc keepalive.....684
 - hdlc shutdown.....685
- HTTP local server commands
 - baseline ip http.....234
 - ip http.....809
 - ip http access-class.....810
 - ip http max-connection-time.....811
 - ip http port.....812
 - ip http redirectUrl.....813
 - ip http same-host-limit.....814
 - ip http server.....815
 - ipv6 http.....1029
 - ipv6 http port.....1030
 - ipv6 http redirectUrl.....1031
 - ipv6 http server.....1032

I

ICMP commands	
ip icmp update-source.....	816
ICR commands	
ip vrrp icr-partition.....	978
ip vrrp icr-partition group.....	979
ip vrrp icr-partition svlan-list.....	980
ip vrrp icr-partition vlan-list.....	983
ip vrrp icr-partition vlan-range.....	984
IEEE 802.3ad link aggregation group interface.....	8, 16
IEEE 802.3ah OAM link-fault management	
enabling on an interface.....	581
IGMP commands	
baseline ip igmp.....	235
baseline ip igmp-proxy interface.....	236
igmp disable.....	699
igmp promiscuous.....	700
ip igmp.....	817
ip igmp access-group.....	818
ip igmp access-source-group.....	819
ip igmp apply-oif-map.....	820
ip igmp explicit-tracking.....	820
ip igmp group limit.....	822
ip igmp immediate-leave.....	823
ip igmp last-member query-interval.....	824
ip igmp oif-map.....	825
ip igmp promiscuous.....	826
ip igmp querier.....	830
ip igmp querier-timeout.....	831
ip igmp query-interval.....	832
ip igmp query-max-response-time.....	833
ip igmp robustness.....	834
ip igmp static-exclude.....	837
ip igmp static-group.....	838
ip igmp static-include.....	839
ip igmp version.....	840
ipv6 mld apply-oif-map.....	1039
multicast group port limit.....	1442
show ip igmp ssm-map enable.....	835
show ip igmp ssm-map static.....	836
<i>See also</i> IGMP proxy commands	
IGMP proxy commands	
ip igmp-proxy.....	827
ip igmp-proxy unsolicited-report-interval.....	828
ip igmp-proxy V1-router-present-time.....	829
IKE commands	
ike local-identity.....	703
ike peer-identity.....	707
ike peer-identity distinguished-name.....	704
ike peer-identity domain-name.....	705
ike peer-identity ip address.....	706
interface commands	
baseline interface serial.....	228
baseline ip interface.....	237
baseline ipv6 interface.....	247
clear ip interface.....	389
clear ipv6 interface.....	410
clear ipv6 neighbors.....	412
description.....	509
interface.....	718
interface ip.....	723
interface ipv6.....	724
interface loopback.....	726
interface mlframe-relay.....	727
interface mlppp.....	728
interface null.....	729
interface pos.....	730
interface serial.....	731
interface tunnel.....	733
ip address.....	738
ip alwaysup.....	743
ip broadcast-address.....	753
ip debounce-time.....	758
ip description.....	760
ip dynamic-interface-prefix.....	795
ip redirects.....	920
ip share-interface.....	946
ip share-nexthop.....	947
ip shutdown.....	948
ip tcp adjust-mss.....	963
ipv6 description.....	1021
ipv6 share-interface.....	1118
interface types and specifiers.....	5
E120 routers.....	13
E320 routers.....	13
ERX14xx models.....	5
ERX310 routers.....	5
ERX7xx models.....	5
IP commands	
arp.....	142
arp timeout.....	145
baseline ip.....	229
baseline ip tunnel-reassembly.....	242
baseline ip udp.....	243
baseline ip vrrp.....	244
baseline show-delta-counts.....	267
baseline tcp.....	272
clear access-list.....	362
clear arp.....	363
clear ip ospf database.....	395
clear ip ospf neighbor.....	396
clear ip prefix-list.....	401
clear ip prefix-tree.....	402
clear ip rip dynamic-interfaces.....	403
clear ip rip redistribution.....	404
clear ip routes.....	405
clear ip tunnel-routes.....	407
clear ipv6 access-list.....	408
distance.....	528
forwarding-table route-holddown.....	639
ip access-route table-map.....	737
ip access-routes.....	736

- ip address.....738
- ip address-pool.....740
- ip alwaysup.....743
- ip analyzer.....744
- ip as-path access-list.....745
- ip auto-configure ip-subscriber.....748
- ip auto-detect ip-subscriber.....749
- ip broadcast-address.....753
- ip community-list.....757
- ip debounce-time.....758
- ip demux-type da-prefix.....759
- ip description.....760
- ip destination-prefix.....761
- ip dhcp-capture.....762
- ip dhcp-external auto-configure.....763
- ip dhcp-external server-address.....766
- ip dhcp-external server-sync.....767
- ip dhcp-server.....779
- ip directed-broadcast.....780
- ip disable-forwarding.....781
- ip explicit-path.
 - mpls explicit-path *See* MPLS commands
- ip extcommunity-list.....797
- ip ignore-df-bit.....841
- ip inactivity-timer.....842
- ip initial-sequence-preference.....843
- ip interface.
 - no ip interface *See* Command Reference
 - Guide N to Z, IP commands
- ip irdp.....845
- ip local alias.....846
- ip local pool.....847
- ip local pool snmpTrap.....848
- ip local pool warning.....849
- ip local shared-pool.....850
- ip mac-validate.....851
- ip mask-reply.....852
- ip mirror.....854
- ip mtu.....862
- ip multipath round-robin.....869
- ip prefix-list.....915
- ip prefix-tree.....916, 917
- ip proxy-arp.....918
- ip re-authenticate-auto-detect ip-subscriber.....919
- ip redirects.....920
- ip refresh-route.....921
- ip rip commands. *See* RIP commands
- ip route.....929
- ip route-map ip-subscriber.....932
- ip router-id.....934
- ip rsvp bandwidth.
 - mpls bandwidth *See* MPLS commands
- ip rsvp signalling hello graceful-restart
 - recovery-time.
 - mpls rsvp signalling hello graceful-restart
 - recovery-time *See* MPLS commands
- ip rsvp signalling hello graceful-restart restart-time.
 - mpls rsvp signalling hello graceful-restart
 - restart-time *See* MPLS commands
- ip rsvp signalling hello graceful-restart.
 - mpls rsvp signalling hello graceful-restart *See* MPLS commands
- ip rsvp signalling hello.
 - mpls rsvp signalling hello *See* MPLS commands
- ip rsvp signalling node-hello.
 - mpls rsvp signalling node-hello *See* MPLS commands
- ip sa-validate.....943
- ip sa-validate trap-enable.....944
- ip shutdown.....948
- ip source-prefix.....949
- ip source-route.....950
- ip speed.....951
- ip ssh. *See* SSH commands
- ip static-route table-map.....960
- ip tcp adjust-mss.....963
- ip ttl.....964
- ip tunnel reassembly.....965
- ip unnumbered.....966
- ip unreachable.....967
- ip virtual-router.....969
- ip vrrp.....972
- ip vrrp accept-data.....973
- ip vrrp advertise-interval.....974
- ip vrrp authentication-key.....975
- ip vrrp authentication-type.....976
- ip vrrp enable.....977
- ip vrrp icr-partition.....978
- ip vrrp icr-partition group.....979
- ip vrrp icr-partition svlan-list.....980
- ip vrrp icr-partition svlan-list explicit.....981
- ip vrrp icr-partition svlan-range.....982
- ip vrrp icr-partition vlan-list.....983
- ip vrrp icr-partition vlan-range.....984
- ip vrrp preempt.....986
- ip vrrp priority.....987
- ip vrrp timers-learn.....988
- ip vrrp track.....989
- ip vrrp virtual-address.....990
- ip-hint.....808
- ipv6 initial-sequence-preference.....1033
- IP multicast commands
 - ip block-multicast-sources.....752
 - ip multicast admission-bandwidth-limit.....863
 - ip multicast-routing.....865
 - ip multicast-routing bandwidth-map.....866
 - ip multicast-routing disable-rpf-check.....867
 - ip multicast-routing permanent-mroute.....868
 - ip rpf-route.....937
 - ipv6 multicast admission-bandwidth-limit.....1059

ipv6 multicast-routing bandwidth-map.....	1062	IPv6 commands	
mtrace.....	1439	baseline ipv6 tcp.....	251
ip pim commands		clear bgp ipv6.....	366
ip pim sparse-mode		clear bgp ipv6 dampening.....	367
graceful-restart-duration.....	907	clear bgp ipv6 redistribution.....	370
IP TCP commands. <i>See</i> TCP commands		clear bgp ipv6 wait-end-of-rib.....	370
IPSec commands		clear ipv6 prefix-list.....	418
aggressive-mode.....	111	clear ipv6 routes.....	419
authentication.....	194	clear ipv6 tunnel-routes.....	420
encryption.....	572	ipv6.....	1013
hash.....	681	ipv6 access-route table-map.....	1015
ip address virtual-router.....	742	ipv6 address.....	1016
ipsec ca authenticate.....	991	ipv6 description.....	1021
ipsec ca enroll.....	992	ipv6 enable.....	1027
ipsec ca identity.....	993	ipv6 hop-limit.....	1028
ipsec certificate-database refresh.....	994	ipv6 mtu.....	1058
ipsec certificate-request generate.....	995	ipv6 neighbor.....	1078
ipsec clear sa.....	996	ipv6 route.....	1109
ipsec cri.....	997	ipv6 sa-validate.....	1117
ipsec identity.....	998	ipv6 static-route table-map.....	1119
ipsec ike-policy-rule.....	999	ipv6 unnumbered.....	1120
ipsec isakmp-policy-rule.....	1000	ipv6 virtual-router.....	1121
ipsec key generate.....	1001	license ipv6.....	1215
ipsec key manual pre-share.....	1002	IPv6 local address pool commands	
ipsec key pubkey-chain rsa.....	1003	baseline ipv6 local pool.....	248
ipsec key zeroize.....	1004	dns-domain-search.....	533
ipsec lifetime.....	1005	dns-server.....	535
ipsec local-endpoint.....	1006	exclude-prefix.....	610
ipsec option dpd.....	1007	ipv6 address-pool local.....	1017
ipsec option nat-t.....	1008	ipv6 local pool.....	1035
ipsec option tx-invalid-cookie.....	1009	ipv6-prefix-pool-name.....	1108
ipsec transform-set.....	1010	IPv6 multicast commands	
ipsec transport profile.....	1011	ipv6 block-multicast-sources.....	1018
ipsec tunnel profile.....	1012	ipv6 multicast-routing.....	1061
key.....	1146	ipv6 multicast-routing disable-rpf-check.....	1063
key-string.....	1148	ipv6 multicast-routing permanent-mroute.....	1064
license ipsec-tunnels.....	1214	ipv6 rpf-route.....	1116
license l2tp-session.....	1217	IPv6 neighbor discovery commands	
lifetime.....	1221	ipv6 nd.....	1065
masked-key.....	1273	ipv6 nd active-solicitations.....	1066
IPSec identity commands		ipv6 nd dad attempts.....	1067
common-name.....	451	ipv6 nd managed-config-flag.....	1068
country.....	471	ipv6 nd ns-interval.....	1069
domain-name.....	543	ipv6 nd other-config-flag.....	1070
IPSec transport profile commands		ipv6 nd prefix-advertisement.....	1071
application.....	114	ipv6 nd proxy.....	1072
enable ipsec transport.....	559	ipv6 nd ra-interval.....	1073
ipsec transport profile.....	1011	ipv6 nd ra-lifetime.....	1074
lifetime.....	1221	ipv6 nd reachable-time.....	1075
local ip address.....	1234	ipv6 nd suppress-ra.....	1076
IPSec tunnel commands		ipv6 nd suppress-ra-source-link-layer.....	1077
domain-suffix.....	544	IS-IS commands	
local ip identity.....	1236	area-authentication.....	125
local ip network.....	1237	area-authentication-key.....	126
IPSec tunnel profile commands		area-message-digest-key.....	128
ipsec tunnel profile.....	1012	baseline clns.....	222

clear ip isis redistribution.....	390
clear isis adjacency.....	421
clear isis database.....	422
clear isis ipv6 redistribution.....	423
clns configuration-time.....	434
clns holding-time.....	435
clns host.....	436
debug isis.....	495
default-information originate.....	501
disable-dynamic-redistribute.....	521
distance ip.....	530
distribute-domain-wide.....	531
domain-authentication.....	538
domain-authentication-key.....	539
domain-message-digest-key.....	541
full-spf-always.....	662
ignore-lsp-errors.....	701
ip route-type.....	933
ip router isis.....	935
ipv6 router isis.....	1110
is-type.....	1143
isis authentication-key.....	1122
isis bfd-liveness-detection.....	1123
isis circuit-type.....	1124
isis csnp-interval.....	1125
isis hello-interval.....	1126
isis hello-multiplier.....	1127
isis lsp-interval.....	1129
isis mesh-group.....	1130
isis message-digest-key.....	1131
isis metric.....	1133
isis network point-to-point.....	1134
isis priority.....	1135
isis retransmit-interval.....	1136
isis retransmit-throttle-interval.....	1137
isis tag.....	1138
log-adjacency-changes.....	1239
lsp-gen-interval.....	1257
lsp-mtu.....	1258
lsp-refresh-interval.....	1259
max-lsp-lifetime.....	1299
maximum-paths.....	1295
metric.....	1316
metric-style narrow.....	1317
metric-style transition.....	1318
metric-style wide.....	1319
mpls ldp autoconfig.....	1354
mpls ldp igp sync holddown.....	1364
mpls ldp sync.....	1376
mpls spf-use-any-best-path.....	1418
mpls traffic-eng.....	1425
mpls traffic-eng router-id.....	1433

J

J-Flow commands

clear ip flow stats.....	388
--------------------------	-----

L

L2TP commands

aaa tunnel assignment-id-format.....	62
aaa tunnel calling-number-format.....	63
aaa tunnel calling-number-format-fallback.....	66
aaa tunnel switch-profile.....	73
aaa tunnel tx-connect-speed-method.....	74
aaa tunnel-group.....	69
address.....	85
avp.....	210
bundled-group-id.....	346
bundled-group-id-overrides-mlppp-ed.....	347
client-name.....	433
default-upper-type mlppp.....	505
disable proxy lcp.....	523
disconnect-cause.....	525
enable ipsec-transport.....	559
enable proxy authenticate.....	561
failover-resync.....	629
identification.....	697
l2tp checksum.....	1158
l2tp destination lockout-test.....	1160
l2tp destination lockout-timeout.....	1161
l2tp destination profile.....	1162
l2tp destruct-timeout.....	1163
l2tp dial-out connecting-timer-value.....	1164
l2tp dial-out dormant-timer-value.....	1165
l2tp dial-out max-buffered-triggers.....	1166
l2tp dial-out session delete.....	1167
l2tp dial-out session reset.....	1168
l2tp dial-out target.....	1169
l2tp dial-out target.....	1169
l2tp disable calling-number-avp.....	1170
l2tp disable challenge.....	1171
l2tp disconnect-cause.....	1172
l2tp drain.....	1173
l2tp drain destination.....	1174
l2tp drain tunnel.....	1175
l2tp fail-over-within-preference.....	1177
l2tp failover-resync.....	1176
l2tp ignore-receive-data-sequencing.....	1178
l2tp ignore-transmit-address-change.....	1179
l2tp reject-transmit-address-change.....	1184
l2tp retransmission.....	1185
l2tp shutdown.....	1187
l2tp shutdown destination.....	1188
l2tp shutdown session.....	1189
l2tp shutdown tunnel.....	1190
l2tp switch-profile.....	1191
l2tp tunnel default-receive-window.....	1192
l2tp tunnel idle-timeout.....	1193
l2tp tunnel short-drain-timeout.....	1194

l2tp tunnel test.....	1196
l2tp tunnel-switching.....	1195
l2tp unlock destination.....	1197
l2tp unlock-test destination.....	1198
l2tp weighted-load-balancing.....	1199
local host.....	1232
local ip address.....	1234
max-sessions.....	1301
medium ipv4.....	1310
L2VPN commands	
address-family.....	95
LDP commands	
clear mpls ldp.....	429
hello hold-time.....	686
hello interval.....	687
mpls ldp.....	1352
mpls ldp advertise-labels.....	1353
mpls ldp deaggregate.....	1355
mpls ldp disable.....	1356
mpls ldp discovery transport-address.....	1357
mpls ldp egress-label.....	1358
mpls ldp graceful-restart.....	1359
mpls ldp graceful-restart reconnect-time.....	1360
mpls ldp graceful-restart recovery-timer.....	1361
mpls ldp graceful-restart timers	
max-recovery.....	1362
mpls ldp graceful-restart timers	
neighbor-liveness.....	1363
mpls ldp independent-control.....	1365
mpls ldp ip-forwarding.....	1366
mpls ldp link-hello disable.....	1367
mpls ldp neighbor password.....	1368
mpls ldp profile.....	1369
mpls ldp redistribute.....	1370
mpls ldp session holdtime.....	1371
mpls ldp session keepalive interval.....	1372
mpls ldp session retries.....	1373
mpls ldp session retry-time.....	1374
mpls ldp strict security.....	1375
mpls ldp targeted-hello holdtime.....	1377
mpls ldp targeted-hello interval.....	1378
mpls ldp targeted-hello receive list.....	1379
mpls ldp targeted-hello send list.....	1380
mpls topology-driven-lsp.....	1422
link aggregation commands	
interface lag.....	725
lACP.....	1208
lACP port-priority.....	1209
member-interface.....	1312
link aggregation group interface, IEEE 802.3ad.....	8, 16
link-fault management commands	
ethernet oam lfm.....	581
ethernet oam lfm high-threshold.....	582
ethernet oam lfm link-monitor	
frame-seconds.....	583

ethernet oam lfm link-monitor	
frame-seconds-summary.....	585
ethernet oam lfm link-monitor	
symbol-period.....	587
ethernet oam lfm mode.....	589
ethernet oam lfm pdu-lost-threshold.....	590
ethernet oam lfm pdu-transmit-interval.....	591
ethernet oam lfm remote-failure.....	592
ethernet oam lfm remote-loopback.....	594
ethernet oam lfm remote-loopback	
supported.....	595
local user database commands	
aaa authentication default.....	34
aaa local database.....	47
aaa local select database.....	48
aaa local username.....	49
ip-address.....	739
ip-address-pool.....	741
loopback interface.....	8

M

manuals

comments on.....	xli
mirror commands	
mirror.....	1322
mirror analyzer-ip-address.....	1324
mirror disable.....	1325
mirror trap-enable.....	1328
mirror-enable.....	1327
MLD commands.....	1045
baseline ipv6 mld.....	249
baseline ipv6 mld-proxy interface.....	250
ip mld oif-map.....	1044
ipv6 mld.....	1036
ipv6 mld access-group.....	1037
ipv6 mld access-source-group.....	1038
ipv6 mld explicit-tracking.....	1039
ipv6 mld group limit.....	1041
ipv6 mld immediate-leave.....	1042
ipv6 mld last-member query-interval.....	1043
ipv6 mld querier-timeout.....	1048
ipv6 mld query-interval.....	1049
ipv6 mld query-max-response-time.....	1050
ipv6 mld robustness.....	1051
ipv6 mld ssm-map enable.....	1052
ipv6 mld ssm-map static.....	1053
ipv6 mld static-exclude.....	1054
ipv6 mld static-group.....	1055
ipv6 mld static-include.....	1056
ipv6 mld version.....	1057
ipv6 mld-proxy version.....	1047
ipv6 router mld.....	1111
mld disable.....	1329
<i>See also</i> MLD proxy commands	

- MLD proxy commands
 - ipv6 mld-proxy.....1045
 - ipv6 mld-proxy unsolicited-report-interval.....1046
- MLFR commands
 - baseline frame-relay interface.....225
 - baseline frame-relay multilink interface.....226
 - encapsulation mlframe-relay ietf.....567
 - frame-relay interface-dlci ietf.....645
 - frame-relay intf-type.....646
 - frame-relay keepalive.....647
 - frame-relay lmi-n391dte.....648
 - frame-relay lmi-n392dce.....649
 - frame-relay lmi-n392dte.....650
 - frame-relay lmi-n393dce.....651
 - frame-relay lmi-n393dte.....652
 - frame-relay lmi-t391dte.....653
 - frame-relay lmi-t392dce.....654
 - frame-relay lmi-type.....655
 - interface mlframe-relay.....727
 - member-interface.....1312
- MLPPP commands
 - encapsulation mlppp.....568
 - interface mlppp.....728
 - member-interface.....1312
- Mobile IP commands
 - baseline ip mobile home-agent.....238
 - clear ip mobile binding.....391
 - ip mobile home-agent.....855
 - ip mobile host.....856
 - ip mobile profile.....857
 - ip mobile secure foreign-agent.....858
 - ip mobile secure host.....859
- MPLS commands.....1337
 - append-after.....113
 - bandwidth.....213
 - baseline mpls interface.....256
 - baseline mpls label.....257
 - baseline mpls next-hop.....258
 - baseline mpls tunnel.....259
 - cleanup-timeout-factor.....361
 - clear mpls dynamic-interfaces
 - on-major-interfaces.....428
 - clear mpls ldp.....429
 - clear rsvp authentication.....431
 - hello hold-time.....686
 - hello interval.....687
 - index.....716
 - interface tunnel.....733
 - ip explicit-path. *See* mpls explicit-path
 - ip rsvp authentication key. *See* mpls rsvp authentication key
 - ip rsvp authentication. *See* mpls rsvp authentication
 - ip rsvp bandwidth. *See* mpls bandwidth
 - ip rsvp bfd-liveness-detection. *See* mpls rsvp bfd-liveness-detection
 - ip rsvp signalling hello. *See* mpls rsvp signalling hello
 - list.....1229
 - mark-exp.....1270
 - member interface.....1311
 - mpls.....1337
 - mpls atm vci range.....1339
 - mpls atm vpi range.....1340
 - mpls backup-path.....1341
 - mpls bandwidth.....1342
 - mpls classifier-list.....1343
 - mpls copy-upc-to-exp.....1344
 - mpls create-dynamic-interfaces.....1345
 - mpls diff-serv phb-id traffic-class.....1346
 - mpls disable.....1347
 - mpls explicit-path.....1348
 - mpls ip propagate-ttl.....1349
 - mpls l2transport load-balancing-group.....1350
 - mpls ldp.....1352
 - mpls ldp advertise-labels.....1353
 - mpls ldp autoconfig.....1354
 - mpls ldp deaggregate.....1355
 - mpls ldp disable.....1356
 - mpls ldp discovery transport-address.....1357
 - mpls ldp egress-label.....1358
 - mpls ldp graceful-restart.....1359
 - mpls ldp graceful-restart reconnect-time.....1360
 - mpls ldp graceful-restart recovery-timer.....1361
 - mpls ldp graceful-restart timers
 - max-recovery.....1362
 - mpls ldp graceful-restart timers
 - neighbor-liveness.....1363
 - mpls ldp igp sync holddown.....1364
 - mpls ldp independent-control.....1365
 - mpls ldp ip-forwarding.....1366
 - mpls ldp link-hello disable.....1367
 - mpls ldp neighbor password.....1368
 - mpls ldp profile.....1369
 - mpls ldp redistribute.....1370
 - mpls ldp session holdtime.....1371
 - mpls ldp session keepalive interval.....1372
 - mpls ldp session retries.....1373
 - mpls ldp session retry-time.....1374
 - mpls ldp strict security.....1375
 - mpls ldp sync.....1376
 - mpls ldp targeted-hello holdtime.....1377
 - mpls ldp targeted-hello interval.....1378
 - mpls ldp targeted-hello receive list.....1379
 - mpls ldp targeted-hello send list.....1380
 - mpls lsp no-route retries.....1383
 - mpls lsp no-route retry-time.....1384
 - mpls lsp retries.....1385
 - mpls lsp retry-time.....1386
 - mpls match exp-bits.....1387
 - mpls match traffic-class.....1388
 - mpls policy-list.....1390

mpls policy-statistics.....	1393
mpls preserve-vpn-exp.....	1394
mpls reoptimize.....	1401
mpls reoptimize timers frequency.....	1402
mpls rsvp.....	1403
mpls rsvp authentication.....	1404
mpls rsvp authentication key.....	1405
mpls rsvp bfd-liveness-detection.....	1406
mpls rsvp disable.....	1407
mpls rsvp egress-label.....	1408
mpls rsvp message-bundling.....	1409
mpls rsvp profile.....	1410
mpls rsvp refresh-reduction.....	1411
mpls rsvp signalling hello.....	1412
mpls rsvp signalling hello graceful-restart.....	1413
mpls rsvp signalling hello graceful-restart recovery-time.....	1414
mpls rsvp signalling hello graceful-restart restart-time.....	1415
mpls rsvp signalling node-hello.....	1416
mpls signaling-interface.....	1417
mpls statistics label.....	1419
mpls statistics next-hop.....	1420
mpls statistics policy.....	1421
mpls topology-driven-lsp.....	1422
mpls topology-driven-lsp ip-interfaces.....	1423
mpls traffic-class.....	1424
mpls traffic-eng administrative-weight.....	1426
mpls traffic-eng attribute-flags.....	1428
mpls traffic-eng egress-label. <i>See</i> mpls rsvp egress-label	
mpls traffic-eng flood thresholds.....	1430
mpls traffic-eng link-management timers periodic-flooding.....	1431
mpls tunnel-model.....	1434
mpls tunnels profile.....	1435
mpls-relay.....	1395
mpls-relay atm cell-packing mcpt-timer.....	1398
mpls-relay atm vpi-range vci-range.....	1399
mpls-relay disable.....	1400
<i>See also</i> LDP commands, MPLS (IS-IS) commands, MPLS (OSPF) commands, RSVP-TE commands	
MPLS commands (IS-IS)	
mpls spf-use-any-best-path.....	1418
mpls traffic-eng.....	1425
mpls traffic-eng router-id.....	1433
MPLS commands (OSPF)	
mpls traffic-eng area.....	1427
mpls traffic-eng multicast-intact.....	1432
mpls traffic-eng router-id.....	1433
Multicast command	
mroute port admission-bandwidth-limit.....	1436
mroute port limit.....	1437
Multilink Frame Relay commands. <i>See</i> MLFR commands	
multilink frame relay interface.....	8
multilink PPP interface.....	9
N	
NAT commands	
baseline ip nat.....	239
clear ip nat translation.....	393
ip nat.....	871
ip nat inside source list.....	872
ip nat inside source static.....	873
ip nat outside source list.....	874
ip nat outside source static.....	875
ip nat pool.....	876
ip nat translation.....	877
ip nat translation max-entries.....	878
license nat.....	1219
NFS commands	
host.....	691
ip nfs.....	879
ip nfs host.....	880
no commands vs. default commands.....	3
non-PPP equal access commands	
baseline ip dhcp-local.....	232
baseline ipv6 dhcpv6-local.....	246
default-router	504
dns-server	534
domain-name.....	543
ip dhcp-local excluded-address.....	774
ip dhcp-local limit.....	775
ip dhcp-local pool.....	776
ip dhcp-local unique-client-ids.....	778
lease	1211
notice icons.....	xxxix
NTP commands	
clock set.....	437
clock summer-time date.....	439
clock summer-time recurring.....	440
clock timezone.....	441
null interface.....	9
NVS commands	
check-disk.....	355
flash-disk compare.....	631
flash-disk duplicate.....	632
flash-disk initialize.....	633
flash-disk scan.....	634
mount.....	1336
O	
OCx/STMx commands	
baseline path interface sonet.....	260
baseline section interface sonet.....	266
clock source.....	438
controller sonet.....	462
loopback.....	1255

OSPF commands

address area.....	86
address authentication message-digest.....	89
address authentication-key.....	88
address authentication-none.....	91
address cost.....	93
address dead-interval.....	94
address hello-interval.....	97
address message-digest-key md5.....	98
address network.....	99
address passive-interface.....	100
address priority.....	102
address retransmit-interval.....	104
address transmit-delay.....	106
area default-cost.....	127
area nssa.....	130
area range.....	131
area stub.....	132
area virtual-link.....	133
area virtual-link authentication-key.....	134
area virtual-link authentication-none.....	136
area virtual-link dead-interval.....	137
area virtual-link hello-interval.....	138
area virtual-link message-digest-key md5.....	139
area virtual-link retransmit-interval.....	140
area virtual-link transmit-delay.....	141
area virtual-link authentication message-digest.....	135
area. no area See Command Reference Guide N to Z, OSPF commands	
authentication message-digest.....	197
authentication-key.....	196
authentication-none.....	199
auto-cost reference-bandwidth.....	206
automatic-virtual-link.....	207
baseline ip ospf.....	240
baseline ipv6 ospf.....	251
clear bfd session.....	365
clear ip ospf redistribution.....	397
clear ipv6 ospf counters.....	413
clear ipv6 ospf process.....	414
clear ipv6 ospf redistribution.....	415
cost.....	470
dead-interval.....	477
debug ip ospf.....	486
debug ipv6 ospf.....	491
default-information originate.....	501
disable-dynamic-redistribute.....	521
disable-incremental-external-spf.....	522
distance.....	528
domain-id.....	540
domain-tag.....	545
dont-install-routes.....	546
graceful-restart.....	666
graceful-restart helper.....	667

graceful-restart

helper-abort-topology-change.....	668
graceful-restart notify-duration.....	669
graceful-restart restart-duration.....	670
hello-interval.....	688
ip ospf authentication message-digest.....	882
ip ospf authentication-key.....	881
ip ospf authentication-none.....	883
ip ospf bfd-liveness-detection.....	884
ip ospf cost.....	885
ip ospf dead-interval.....	886
ip ospf hello-interval.....	887
ip ospf message-digest-key md5.....	888
ip ospf network.....	889
ip ospf priority.....	890
ip ospf retransmit-interval.....	891
ip ospf shutdown.....	892
ip ospf transmit-delay.....	893
ip route-type.....	933
ipv6 ospf area.....	1079
ipv6 ospf bfd-liveness-detection.....	1080
ipv6 ospf cost.....	1081
ipv6 ospf dead-interval.....	1082
ipv6 ospf hello-interval.....	1083
ipv6 ospf mtu-ignore.....	1084
ipv6 ospf network.....	1085
ipv6 ospf priority.....	1086
ipv6 ospf retransmit-interval.....	1087
ipv6 ospf shutdown.....	1088
ipv6 ospf transmit-delay.....	1089
ipv6 route-type.....	1115
ipv6 router ospf.....	1113
maximum-paths.....	1295
message-digest-key md5.....	1315
mpls ldp autoconfig.....	1354
mpls ldp igp sync holddown.....	1364
mpls ldp sync.....	1376
mpls traffic-eng area.....	1427
mpls traffic-eng multicast-intact.....	1432
mpls traffic-eng router-id.....	1433

P

PIM commands

clear ip mroute.....	392
clear ip pim auto-rp.....	398
clear ip pim interface count.....	399
clear ip pim remote-neighbor count.....	400
clear ipv6 mroute.....	411
clear ipv6 pim interface.....	416
clear ipv6 pim remote-neighbor.....	417
debug ip pim.....	488
debug ipv6 pim.....	493
ip pim.....	894
ip pim bfd-liveness-detection.....	895
ip pim bsr-candidate.....	896

ip pim data-mdt.....	897	frame-relay policy-list.....	657
ip pim dr-priority.....	898	gre-tunnel policy.....	675
ip pim group-address-pool.....	899	gre-tunnel policy-list.....	676
ip pim join-filter.....	900	green-mark.....	673
ip pim join-prune-interval.....	901	ip classifier-list.....	754
ip pim query-interval.....	902	ip filter-options all.....	799
ip pim rp-address.....	903	ip match-policy-list.....	853
ip pim rp-candidate.....	904	ip policy.....	910
ip pim send rp-announce.....	905	ip policy-list.....	912
ip pim send rp-discovery scope.....	906	ip policy-parameter hierarchical.....	913
ip pim sparse-modegraceful-restart-duration.....	907	ip policy-parameter reference-rate.....	914
ip pim spt-threshold.....	908	ipv6 classifier-list.....	1019
ip pim ssm.....	909	ipv6 policy.....	1102
ipv6 pim bfd-liveness-detection.....	1090	ipv6 policy-list.....	1104
ipv6 pim bsr-candidate.....	1091	ipv6 policy-parameter hierarchical.....	1105
ipv6 pim dr-priority.....	1092	ipv6 policy-parameter reference-rate.....	1106
ipv6 pim join-filter.....	1093	ipv6 prefix-list.....	1107
ipv6 pim join-prune-interval.....	1094	l2tp classifier-list.....	1159
ipv6 pim query-interval.....	1095	l2tp policy.....	1180
ipv6 pim rp-address.....	1096	l2tp policy-list.....	1181
ipv6 pim rp-candidate.....	1097	l2tp policy-parameter hierarchical.....	1182
ipv6 pim sparse-mode.....	1098	l2tp policy-parameter reference-rate.....	1183
ipv6 pim sparse-mode		log.....	1238
graceful-restart-duration.....	1099	mark.....	1266
ipv6 pim spt-threshold.....	1100	mark-clp.....	1268
ipv6 pim ssm.....	1101	mark-de.....	1269
ipv6 router pim.....	1114	mask-val.....	1275
mdt-data-delay.....	1306	mpls policy.....	1389
mdt-data-holddown.....	1307	mpls policy-parameter hierarchical.....	1391
mdt-data-timeout.....	1308	mpls policy-parameter reference-rate.....	1392
mdt-interval.....	1309	POS commands	
policy management commands		baseline interface pos.....	228
aggregation-node.....	110	crc.....	472
atm classifier-list.....	167	encapsulation ppp.....	569
atm policy.....	180	interface pos.....	730
atm policy-list.....	181	loopback.....	1255
atm-cell-mode.....	166	mru.....	1438
clear mirror log.....	427	mtu.....	1440
color.....	442	POS interface.....	10, 17
color-aware.....	443	PPP commands	
color-mark-profile.....	444	baseline ppp interface.....	261
committed-action.....	445	PPPoE commands	
committed-burst.....	446	aaa tunnel calling-number-format.....	63
committed-rate.....	449	aaa tunnel calling-number-format-fallback.....	66
conformed-action.....	454	baseline pppoe interface.....	262
control plane.....	459	encapsulation pppoe.....	570
exceeded-action.....	597	profile command, ip tcp adjust-mss.....	963
exception http-redirect.....	604		
excess-burst.....	609		
exp-mask.....	618		
filter.....	630		
forward.....	635		
forward interface.....	636		
forward next-hop.....	637		
frame-relay classifier-list.....	641		
frame-relay policy.....	656		

Q

QoS commands

aaa qos downstream rate.....	54
adjustment-factor.....	107
assured-rate.....	146
buffer-weight.....	331
clear egress-queue.....	376

- clear fabric-queue.....377
- committed-drop-threshold.....447
- committed-length.....448
- committed-threshold.....450
- conformed-drop-threshold.....455
- conformed-fraction.....456
- conformed-length.....457
- conformed-threshold.....458
- controlled-interface-type.....460
- convergence-factor.....464
- drop-profile.....548
- exceeded-drop-threshold.....598
- exceeded-fraction.....599
- exceeded-length.....600
- exceeded-threshold.....601
- fabric-strict-priority.....626
- fabric-weight.....627
- forwarding-rate-threshold.....638
- gre-tunnel classifier-list.....674
- gre-tunnel policy-list.....676
- instance-interface-type.....717
- load-rebalance.....1231
- mark-exp.....1270
- mark-user-priority.....1271
- maximum-voql.....1297
- minimum-dynamic-rate-percent.....1320
- mpls classifier-list.....1343
- mpls policy-list.....1390
- mpls policy-statistics.....1393
- qos-shaping-mode.....864
- QoS commands,
 - member-interface-type.....1313
- R**
- RADIUS commands
 - aaa intf-desc-format include.....44
 - authorization change.....201
 - baseline radius.....263
 - baseline radius dynamic-request.....264
 - baseline radius relay.....265
 - key.....1146
 - max-sessions.....1301
- redundancy commands
 - clear redundancy history.....430
 - disable-autosync.....520
 - disable-switch-on-error.....524
 - ip initial-sequence-preference.....843
 - ipv6 initial-sequence-preference.....1033
- Response Time Reporter commands
 - frequency.....659
 - hops-of-statistics-kept.....690
 - max-response-failure.....1300
- RIP commands
 - address.....85
 - address authentication key.....87
 - address authentication mode.....90
 - address bfd-liveness-detection.....92
 - address receive version.....103
 - address send version.....105
 - authentication key.....195
 - authentication mode.....198
 - baseline ip rip.....241
 - clear ip rip dynamic-interfaces.....403
 - clear ip rip redistribution.....404
 - debounce-time.....481
 - debug ip rip.....490
 - default-information originate.....501
 - default-metric.....503
 - disable.....519
 - disable-dynamic-redistribute.....521
 - distance.....528
 - distribute-list.....532
 - exit-remote-neighbor.....617
 - interface-event-disable.....720
 - ip rip.....922
 - ip rip authentication key.....923
 - ip rip authentication mode.....924
 - ip rip bfd-liveness-detection.....925
 - ip rip copy-to-dynamic.....926
 - ip rip receive version.....927
 - ip rip send version.....928
 - ip route-type.....933
 - ip split-horizon.....952
 - ip summary-address.....961
 - match-set summary prefix-tree.....1291
- routing policy commands
 - match as-path.....1276
 - match community.....1277
 - match description.....1442
 - match distance.....1277
 - match extcommunity.....1279
 - match ip address.....1280
 - match ip next-hop.....1281
 - match ipv6 address.....1282
 - match ipv6 next-hop.....1283
 - match ipv6 route-source.....1284
 - match level.....1285
 - match metric.....1286
 - match metric-type.....1287
 - match policy-list.....1289
 - match route-type.....1290
 - match tag.....1292
 - match-set summary prefix-tree.....1291
- RSVP-TE commands
 - bandwidth.....213
 - cleanup-timeout-factor.....361
 - clear rsvp authentication.....431
 - mark-exp.....1270
 - mpls backup-path.....1341
 - mpls bandwidth.....1342
 - mpls classifier-list.....1343

mpls diff-serv phb-id traffic-class.....	1346	bulkstats receiver remote-name.....	338
mpls lsp no-route retries.....	1383	bulkstats schema.....	339
mpls lsp no-route retry-time.....	1384	bulkstats schema subtree.....	340
mpls lsp retries.....	1385	bulkstats schema subtree policy.....	341
mpls lsp retry-time.....	1386	bulkstats schema subtree qos.....	342
mpls policy-list.....	1390	bulkstats traps.....	344
mpls policy-statistics.....	1393	bulkstats virtual-router-group.....	345
mpls reoptimize.....	1401	bulkstats.	
mpls reoptimize timers frequency.....	1402	no bulkstats <i>See</i> Command Reference Guide	
mpls rsvp.....	1403	N to Z, SNMP commands	
mpls rsvp authentication.....	1404	SNMP server event manager commands	
mpls rsvp authentication key.....	1405	delta-sampling.....	507
mpls rsvp bfd-liveness-detection.....	1406	SONET/SDH interface.....	12, 17
mpls rsvp disable.....	1407	SSH commands	
mpls rsvp egress-label.....	1408	crypto key dss.....	474
mpls rsvp message-bundling.....	1409	disconnect ssh.....	526
mpls rsvp profile.....	1410	ip ssh authentication-retries.....	953
mpls rsvp refresh-reduction.....	1411	ip ssh crypto.....	954
mpls rsvp signalling hello.....	1412	ip ssh disable-user-authentication.....	955
mpls rsvp signalling hello graceful-restart.....	1413	ip ssh mac.....	956
mpls rsvp signalling hello graceful-restart		ip ssh sleep.....	957
recovery-time.....	1414	ip ssh timeout.....	958
mpls rsvp signalling hello graceful-restart		ip ssh user-authentication-protocol.....	959
restart-time.....	1415	subscriber interface commands	
mpls rsvp signalling node-hello.....	1416	dhcp-external delete-binding.....	513
mpls traffic-class.....	1424	ip auto-configure ip-subscriber.....	748
mpls traffic-eng administrative-weight.....	1426	ip auto-detect ip-subscriber.....	749
mpls traffic-eng attribute-flags.....	1428	ip demux-type da-prefix.....	759
mpls traffic-eng flood thresholds.....	1430	ip destination-prefix.....	761
mpls traffic-eng link-management timers		ip dhcp-external auto-configure.....	763
periodic-flooding.....	1431	ip dhcp-external server-address.....	766
		ip dhcp-external server-sync.....	767
		ip inactivity-timer.....	842
		ip re-authenticate-auto-detect ip-subscriber.....	919
		ip source-prefix.....	949
		subscriber management commands	
		ip service-profile.....	945
		subscriber policy commands	
		arp.....	142
		bridge subscriber-policy.....	322
		broadcast.....	330
		ip.....	735
		mpls.....	1337
		multicast.....	1441
		support, technical <i>See</i> technical support	
		suspicious control flow detection commands	
		baseline	
		suspicious-control-flow-detectioncounts.....	270
		clear suspicious-control-flow-detection	432
		system commands	
		aaa authentication enable default.....	35
		aaa authentication login.....	36
		aaa authorization.....	37
		aaa authorization config-commands.....	38
		aaa new-model.....	50
		access-class in.....	78

S

serial interface.....	10
Service Manager commands	
license service-management.....	1220
show commands, filtering.....	4
SNMP commands	
baseline snmp.....	268
buffer-weight.	
no buffer-weight <i>See</i> Command Reference	
Guide N to Z, SNMP commands	
bulkstats collector.....	333
bulkstats collector collector-mode.....	333
bulkstats collector description.....	333
bulkstats collector interval.....	333
bulkstats collector max-size.....	333
bulkstats collector primary-receiver.....	333
bulkstats collector secondary-receiver.....	333
bulkstats collector single-interval.....	333
bulkstats file-format endOfLine-Lf.....	334
bulkstats interface-type.....	337
bulkstats interfaces description-format	
common.....	335
bulkstats interfaces rfc 1213.....	336

access-list.....	79
bandwidth oversubscription.....	214
banner.....	215
clear line.....	426
copy.....	465
copy running-configuration	
startup-configuration.....	468
copy startup-configuration.....	469
crypto key dss.....	474
data-character-bits.....	476
delete.....	506
description.....	509
dir.....	518
disconnect ssh.....	526
dsr-detect.....	550
enable password.....	560
enable secret.....	562
erase secrets.....	578
exception dump.....	602
exception gateway.....	603
exception monitor.....	605
exception monitor interval.....	606
exception protocol ftp.....	607
exception source.....	608
exclude-subsystem.....	611
exec-banner.....	612
exec-timeout.....	613
halt.....	680
help.....	689
host.....	691
hostname.....	692
hotfix activate.....	693
ip domain-lookup.....	782
ip domain-name.....	783
ip name-server.....	870
ip nfs.....	879
ip nfs host.....	880
ip ssh authentication-retries.....	953
ip ssh crypto.....	954
ip ssh disable-user-authentication.....	955
ip ssh mac.....	956
ip ssh sleep.....	957
ip ssh timeout.....	958
ip ssh user-authentication-protocol.....	959
ipv6 access-list.....	1014
line.....	1223
login.....	1252
login authentication.....	1253
macro.....	1262
memory.....	1314
more.....	1334
motd-banner.....	1335

T

T1 commands	
interface serial.....	731
T3 commands	
atm framing.....	172
bert.....	273
cablelength.....	352
channelized.....	354
controller t3.....	463
description.....	509
dsu bandwidth.....	551
dsu mode.....	552
equipment loopback.....	577
idle-character.....	698
load-interval.....	1230
loopback.....	1255
mru.....	1438
mtu.....	1440
TACACS+ commands	
aaa authentication enable default.....	35
baseline tacacs.....	271
TCP commands	
tcp ack-rst-and-syn.....	962
technical support	
contacting JTAC.....	xl
text and syntax conventions.....	xl
time commands, system	
clock set.....	437
clock summer-time date.....	439
clock summer-time recurring.....	440
clock timezone.....	441
timing command, clock source.....	438
troubleshooting commands	
baseline log.....	255
bgp log-neighbor-changes.....	294
debug ip bgp.....	482
debug ip mbgp.....	484
debug ip ospf.....	486
debug ip pim.....	488
debug ip rip.....	490
debug ipv6 ospf.....	491
debug ipv6 pim.....	493
debug isis.....	495
log.....	1238
log destination.....	1241
log destination syslog source.....	1243
log engineering.....	1244
log fields.....	1245
log filters.	
no log filters <i>See</i> Command Reference Guide	
N to Z, troubleshooting commands	
log here.....	1247
log severity.....	1248
log unlimited.....	1250
log verbosity.....	1251
tunnel interface.....	13

tunnel service command, max-interfaces.....1298

U

unified ISSU commands

issu initialize.....1140
 issu start.....1141
 issu stop.....1142
 license issu.....1216

user interface commands

configure.....452
 confirmations explicit.....453
 disable.....519
 do.....536
 enable.....557
 end.....573
 exit.....615

V

virtual router command

ipv6-virtual-router.....1112

VLAN commands

auto-configure vlan.....205
 encapsulation vlan.....571
 mark-user-priority.....1271
 mask-val.....1275
 monitor vlan interface.....1333

VoIP commands

circuit-id.....474
 circuit-id interface.....474

VPLS commands

address-family.....95
 arp.....142
 baseline bridge.....219
 baseline bridge interface.....220
 baseline bridge interface vpls.....221
 bridge.....312
 bridge acquire.....313
 bridge address.....314
 bridge aging-time.....316
 bridge learn.....319
 bridge snmp-trap link-status.....321
 bridge subscriber-policy.....322
 bridge vpls rd.....323
 bridge vpls route-target.....325
 bridge vpls site-name site-id.....327
 bridge vpls site-range.....328
 bridge vpls transport-virtual-router.....329
 bridge-group.....318
 broadcast.....330
 clear bridge.....372
 clear bridge address.....373
 clear bridge interface.....374
 clear bridge interface vpls.....375
 clear ip bgp.....378

clear ip bgp dampening.....380
 clear ip bgp wait-end-of-rib.....384
 ip.....735
 mpls.....1337
 mpls ldp vpls neighbor.....1381
 mpls ldp vpls vpls-id.....1382
 multicast.....1441

VPN commands

ipv6-router-name.....1112

VPWS commands

clear ip bgp.....378
 clear ip bgp dampening.....380
 clear ip bgp wait-end-of-rib.....384
 l2vpn control-word.....1200
 l2vpn encapsulation-type.....1201
 l2vpn local-site-id remote-site-id.....1202
 l2vpn rd.....1203
 l2vpn route-target.....1204
 l2vpn sequencing.....1205
 l2vpn site-name site-id.....1206
 l2vpn site-range.....1207

VRRP commands

baseline ip vrrp.....244
 ip vrrp.....972
 ip vrrp accept-data.....973
 ip vrrp advertise-interval.....974
 ip vrrp authentication-key.....975
 ip vrrp authentication-type.....976
 ip vrrp enable.....977
 ip vrrp icr-partition.....978
 ip vrrp icr-partition group.....979
 ip vrrp icr-partition svlan-list.....980
 ip vrrp icr-partition vlan-list.....983
 ip vrrp icr-partition vlan-range.....984
 ip vrrp preempt.....986
 ip vrrp priority.....987
 ip vrrp timers-learn.....988
 ip vrrp track.....989
 ip vrrp virtual-address.....990

VRRP ICR commands

ip vrrp icr-partition svlan-list explicit.....981
 ip vrrp icr-partition svlan-range.....982