



JUNOS® Software

Subscriber Access Configuration Guide

Release 9.4

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, California 94089
USA

408-745-2000

www.juniper.net

Part Number: 530-028713-01, Revision 1

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

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

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

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

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

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

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

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

JUNOS® Software Subscriber Access Configuration Guide

Release 9.4

Copyright © 2009, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Writing: Mark Barnard, Bruce Gillham, Sarah Lesway-Ball, Donna Ono, Brian Wesley Simmons

Editing: Ben Mann

Illustration: Nathaniel Woodward

Cover Design: Edmonds Design

Revision History

15 January 2009—Revision 1

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Table of Contents

	About This Guide	xxix
	Objectives	xxix
	Audience	xxix
	Supported Routing Platforms	xxx
	Using the Indexes	xxx
	Using the Examples in This Manual	xxx
	Merging a Full Example	xxxi
	Merging a Snippet	xxxi
	Documentation Conventions	xxxii
	List of Technical Publications	xxxiv
	Documentation Feedback	xl
	Requesting Technical Support	xli
Part 1	Managing Access Networks	
Chapter 1	Subscriber Access Overview	3
	Subscriber Access Overview	3
	Subscriber Access Terms and Acronyms	4
	Subscriber Access Environment	4
	Relationship Between Subscribers and Interfaces in an Access Network	5
	Subscriber Access Support Limitations	5
	Platform Support	5
	Interface Support	5
	Subscriber Access Licensing Overview	6
	Subscriber Access Operation Flow	6
	Activating Subscribers and Managing Services in an Access Network	7
	Components of a Dynamic Profile	8
	Router Internal Variables Used by Dynamic Profiles	8
	Configuring Subscriber Access	8
Part 2	Subscriber Management	
Chapter 2	Subscriber Management Overview	15
	Subscriber Access Management Overview	15

Chapter 3 Configuring the AAA Service Framework for Subscriber Access 17

AAA Service Framework Overview	17
Router Interaction with RADIUS Servers Overview	18
Configuring Authentication and Accounting Parameters for Subscriber Access	19
Specifying the Authentication and Accounting Methods for Subscriber Access	19
Configuring How Accounting Statistics Are Collected for Subscriber Access	20
Configuring RADIUS Server Parameters for Subscriber Access	21
Specifying the RADIUS Authentication and Accounting Servers for Subscriber Access	21
Configuring RADIUS Server Options for Subscriber Access	21
Configuring How RADIUS Attributes Are Used for Subscriber Access	23
Using RADIUS Dynamic Requests for Subscriber Access Management	25
Dynamic Service Activation During Login Overview	25
RADIUS-Initiated Change of Authorization (CoA) Overview	26
CoA Messages	26
Qualifications for Change of Authorization	26
Message Exchange	26
RADIUS-Initiated Disconnect Overview	27
Disconnect Messages	27
Qualifications for Disconnect	27
Message Exchange	27
Configuring RADIUS-Initiated Dynamic Request Support	28
Verifying and Managing the RADIUS Dynamic-Request Feature	28
RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework	29
RADIUS IETF Attributes Supported by the AAA Service Framework	29
Juniper Networks VSAs Supported by the AAA Service Framework	32
Error-Cause Codes (RADIUS Attribute 101) for Dynamic Requests	36
Attaching Access Profiles	37
Verifying and Managing Subscriber Information	37

Chapter 4 Configuring Address-Assignment Pools for Subscriber Access 39

DHCP and Address Assignment Pools Overview	39
Configuring Address-Assignment Pools	39
Configuring an Address-Assignment Pool Name and Network Address	40
Configuring a Named Address Range for Dynamic Address Assignment	41

Configuring Static Address Assignment	41
Configuring DHCP Client-Specific Attributes	41
DHCP Attributes Table	42
License Requirements for Address-Assignment Pools	43
Tracing Address-Assignment Pool Processes	43
Configuring the Address-Assignment Pool Trace Log Filename	44
Configuring the Number and Size of Address-Assignment Pool Processes Log Files	44
Configuring Access to the Log File	45
Configuring a Regular Expression for Lines to Be Logged	45
Configuring the Trace Operation	45

Chapter 5

Configuring DHCP Local Server for Subscriber Access 47

Extended DHCP Local Server Overview	48
Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools	49
Providing DHCP Client Configuration Information	49
Minimal Configuration for Clients	50
DHCP Local Server and Address-Assignment Pools	51
Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview	52
Multiple DHCP Subscribers Sharing the Same VLAN Logical Interface	52
Primary Dynamic Profile	53
Using External AAA Authentication Services with DHCP	53
Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool To Use	54
Grouping Interfaces with Common DHCP Configurations	55
Group-Specific DHCP Local Server Options	56
Overriding Default DHCP Local Server Configuration Settings	56
Specifying the Maximum Number of DHCP Clients Per Interface	57
Disabling ARP Table Population	58
DHCP Auto Logout Overview	59
Auto Logout Overview	59
How DHCP Identifies and Releases Clients	60
Option 60 and Option 82 Requirements	60
Automatically Logging Out DHCP Clients	61
Attaching Dynamic Profiles to DHCP Subscriber Interfaces	62
Attaching a Dynamic Profile to All DHCP Subscriber Interfaces	62
Attaching a Dynamic Profile to a Group of DHCP Subscriber Interfaces	63
Configuring Passwords for Usernames	63
Creating Unique Usernames for DHCP Clients	64
Verifying and Managing DHCP Local Server Configuration	66
Tracing Extended DHCP Operations	66
Configuring the Extended DHCP Log Filename	68
Configuring the Number and Size of Extended DHCP Log Files	68
Configuring Access to the Extended DHCP Log File	68

Configuring a Regular Expression for Extended DHCP Lines to Be Logged	69
Configuring the Extended DHCP Tracing Flags	69

Chapter 6**Configuring DHCP Relay for Subscriber Access****71**

Extended DHCP Relay Agent Overview	72
Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers	72
Access and Access-Internal Routes	73
DHCP State Persistence	74
Graceful Routing Engine Switchover	74
Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview	75
Multiple DHCP Subscribers Sharing the Same VLAN Logical Interface	75
Primary Dynamic Profile	76
Using External AAA Authentication Services with DHCP	76
Grouping Interfaces with Common DHCP Configurations	77
Group-Specific DHCP Relay Options	78
Overriding the Default DHCP Relay Configuration	79
Overwriting giaddr Information	80
Overriding Option 82 Information	80
Using Layer 2 Unicast Transmission for DHCP Packets	81
Trusting Option 82 Information	81
Disabling ARP Table Population	81
Specifying the Maximum Number of DHCP Clients Per Interface	83
Disabling DHCP Relay	83
DHCP Auto Logout Overview	84
Auto Logout Overview	84
How DHCP Identifies and Releases Clients	84
Option 60 and Option 82 Requirements	85
DHCP Relay Agent Option 82 Value for Auto Logout	85
Automatically Logging Out DHCP Clients	86
Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers	87
Using Matching Option 60 Strings to Process DHCP Client Traffic	88
Using Nonmatching Option 60 Strings to Process DHCP Client Traffic	91
Displaying a Count of Discarded DHCP Packets with Option 60 Information	91
Enabling and Disabling Insertion of Option 82 Information	91
Configuring Agent-Circuit-Id Information	92
Configuring an Option 82 Prefix	93
Configuring Server Groups	94
Configuring Active Server Groups	95

Attaching Dynamic Profiles to DHCP Subscriber Interfaces	95
Attaching a Dynamic Profile to All DHCP Subscriber Interfaces	95
Attaching a Dynamic Profile to a Group of DHCP Subscriber Interfaces	96
Verifying and Managing DHCP Relay Configuration	97
Tracing Extended DHCP Operations	97
Configuring the Extended DHCP Log Filename	98
Configuring the Number and Size of Extended DHCP Log Files	99
Configuring Access to the Extended DHCP Log File	99
Configuring a Regular Expression for Extended DHCP Lines to Be Logged	100
Configuring the Extended DHCP Tracing Flags	100

Chapter 7

Configuring Subscriber Secure Policy Traffic Mirroring 103

Subscriber Secure Policy Overview	104
Subscriber Secure Policy Terms	104
Subscriber Secure Policy Traffic Mirroring Architecture	105
RADIUS Attributes Used for Subscriber Secure Policy	107
RADIUS Attributes Used as Traffic Mirroring Triggers	108
RADIUS-Based Mirroring Attributes	108
Considerations When Using RADIUS Attributes for Subscriber Secure Policy	109
Configuring Subscriber Secure Policy Mirroring Overview	110
Guidelines for Configuring Subscriber Secure Policy Mirroring on the Flow-Tap Service	111
Configuring Flow-Tap Service Support for Subscriber Secure Policy Mirroring	112
Configuring RADIUS Server Support for Subscriber Secure Policy Mirroring	113
Terminating Subscriber Secure Policy Mirroring Sessions	114

Chapter 8

AAA and Remote Subscriber Access Configuration Examples 115

Example: Configuring RADIUS-Based Subscriber Authentication and Accounting	115
Example: Configuring an Address-Assignment Pool	117
Example: Minimum Extended DHCP Local Server Configuration	118
Example: Extended DHCP Local Server Configuration with Optional Pool Matching	118
Example: Minimum DHCP Relay Agent Configuration	118
Example: DHCP Relay Agent Configuration with Multiple Clients and Servers	119
Example: Using Option 60 Strings to Forward DHCP Client Traffic	120
Example: Using Option 60 Strings to Drop DHCP Client Traffic	121

Chapter 9 **Summary of AAA and Remote Subscriber Access Statements** **123**

accounting	123
accounting-port	124
accounting-server	125
accounting-session-id-format	125
accounting-stop-on-access-deny	126
accounting-stop-on-failure	126
active-server-group	127
address-assignment	128
always-write-giaddr	129
always-write-option-82	130
attributes	131
authentication	132
authentication	133
authentication-order	134
authentication-server	134
boot-file	135
boot-server	135
circuit-id	136
circuit-id	137
circuit-type	138
circuit-type	139
client-discover-match	140
client-discover-match	141
default-local-server-group	142
default-relay-server-group	143
delimiter	144
delimiter	145
dhcp-attributes	146
dhcp-local-server	147
dhcp-relay	149
disable-relay	152
domain-name	152
domain-name	153
domain-name	154
drop	155
dynamic-profile	157
dynamic-profile	158
ethernet-port-type-virtual	159
exclude	160
forwarding-class	162
grace-period	163
group	164
group	165
hardware-address	167
host	167
ignore	168
immediate-update	168
interface	169
interface	170

interface-client-limit	171
interface-client-limit	172
interface-description-format	173
interfaces	173
ip-address	174
ip-address-first	175
layer2-unicast-replies	176
local-server-group	177
logical-system-name	178
logical-system-name	179
mac-address	180
mac-address	181
maximum-lease-time	181
name-server	182
nas-identifier	182
nas-port-extended-format	183
netbios-node-type	184
network	184
no-arp	185
no-arp	186
option	187
option-60	188
option-60	189
option-82	190
option-82	191
option-82	192
option-82	193
option-match	194
options	195
order	196
override-nas-information	196
overrides	197
overrides	198
password	199
password	200
pool	200
pool-match-order	201
port	201
prefix	202
profile	205
radius	208
radius-flow-tap	209
radius-server	210
range	211
relay-option-60	212
relay-option-82	213
relay-server-group	214
remote-id	215
retry	215
revert-interval	216
router	216

routing-instance	217
routing-instance-name	218
routing-instance-name	219
secret	219
server-group	220
source-address	221
source-ipv4-address	221
statistics	222
tftp-server	223
timeout	223
traceoptions	224
traceoptions	227
traceoptions	230
trust-option-82	232
update-interval	233
username-include	234
username-include	235
user-prefix	236
user-prefix	237
vendor-option	238
vlan-nas-port-stacked-format	239
wins-server	239

Part 3

Mobile IP Access

Chapter 10

Mobile IP Overview 243

Mobile IP Home Agent Elements and Behavior	243
Mobile IP Registration	244
Home Address Assignment	244
Authentication	244
Re-authentication	245
AAA Authentication	245
Local Authentication	246
Accounting	247
Mobile IP Routing and Forwarding	248

Chapter 11

Configuring Mobile IP 249

Configuring Mobile IP	249
Tracing Mobile IP Operations	250
Configuring the Mobile IP Trace Log Filename	251
Configuring the Number and Size of Mobile IP Log Files	251
Configuring Access to the Mobile IP Log File	251
Configuring a Regular Expression for Mobile IP Lines to Be Logged	252
Configuring the Mobile IP Tracing Flags	252
Configuring the Mobile IP Authentication Method	253
Configuring the Mobile IP Home Agent	253

Configuring the Local Authentication Attributes for the Mobile Node	254
Configuring Accounting for Mobile IP Subscribers	254
Configuring Dynamic Home Assignment for the Mobile Node	255

Chapter 12**Summary of Mobile IP Statements 257**

algorithm	257
authenticate	257
dynamic-home-assignment	258
enable-service	258
entity-type	259
home-agent	259
home-agent	260
home-agent-address	260
key	261
mobile-ip	262
nai	263
order	264
peer	265
registration-lifetime	266
revocation-required	266
replay-method	267
spi	268
statistics	269
timestamp-tolerance	270
traceoptions	271
virtual-network	272

Part 4**Dynamic Profiles for Access and Services****Chapter 13****Dynamic Profiles Overview 275**

Dynamic Profiles Overview	275
Dynamic Profile Interface Support	275
What Dynamic Profiles Do	275
How Dynamic Profiles Work	276
Dynamic Variables Overview	276
How Dynamic Variables Work	276
JUNOS Predefined Internal Variables	277
User-Defined Variables	281

Chapter 14**Configuring Dynamic Profiles 283**

Configuring a Basic Dynamic Profile	283
Configuring Predefined Internal Dynamic Variables in Dynamic Profiles	284
Configuring User-Defined Dynamic Variables in Dynamic Profiles	285
Configuring a Dynamic Profile for Client Access	287

	Configuring a Dynamic Profile for Various Levels of Services	288
	Modifying Dynamic Profiles	289
Chapter 15	Dynamic Profile Examples	293
	Example: IGMP Dynamic Profile	293
	Example: Firewall Dynamic Profile	294
Chapter 16	Summary of Dynamic Profile Statements	297
	attribute	297
	default-value	297
	dynamic-profiles	298
	mandatory	300
	radius	300
	tag	301
	variables	301
	vendor-id	302
Part 5	Subscriber Interfaces	
Chapter 17	Subscriber Interface Overview	305
	Subscriber Interface Overview	305
	Statically Identifying Subscribers	305
	Dynamically Identifying Subscribers	306
	Static Subscriber Interfaces and VLAN Overview	306
	Subscriber Interfaces and IP Demux Overview	307
	Interface Sets of Static Demux Interfaces	307
	Dynamic Demux Interfaces	308
	Guidelines for Configuring IP Demux Interfaces for Subscriber Access	308
	MAC Address Validation for Subscriber Interfaces Overview	309
	Supported Types of Subscriber Interfaces	309
	Trusted Addresses	309
	Types of MAC Address Validation	309

Chapter 18	Configuring Subscriber Interfaces for Dynamic Profiles	311
	Configuring Static Subscriber Interfaces in Dynamic Profiles	311
	Configuring a Subscriber Interface with a Static VLAN Interface	312
	Associating Dynamic Profiles with Statically Created Interfaces	312
	Configuring a Subscriber Interface Using a Set of Static IP Demux Interfaces	313
	Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles	314
	Configuring MAC Address Validation for Subscriber Interfaces	315
	Configuring MAC Address Validation for Static Subscriber Interfaces	316
	Configuring MAC Address Validation for Dynamic Subscriber Interfaces	317
Chapter 19	Subscriber Interface Examples	319
	Example: Configuring a Static Subscriber Interface on a Gigabit Ethernet VLAN Interface (Multiple Logical Units)	319
	Example: Configuring a Static Subscriber Interface on a Gigabit Ethernet VLAN Interface	319
	Example: Configuring a Static Subscriber Interface on a Gigabit Ethernet VLAN Interface (No Autonegotiation)	320
	Example: Configuring a Static Subscriber Interface with a Loopback	320
	Example: Configuring Dynamic Subscriber Interfaces on IP Demux Interfaces	320
Chapter 20	Subscriber Interfaces over Aggregated Ethernet Overview	323
	Static VLAN Subscriber Interfaces over Aggregated Ethernet Overview	323
	Guidelines for Configuring a Static VLAN Subscriber Interface over Aggregated Ethernet for Static or Dynamic CoS Support	324
	Guidelines for Configuring an Aggregated Ethernet Logical Interface to Support a Static VLAN Subscriber Interface	324
	Static or Dynamic IP Demux Subscriber Interfaces over Aggregated Ethernet Overview	325
	Relationship Between an IP Demux Subscriber Interface and the Underlying Aggregated Ethernet Logical Interface	325
	Options for Aggregated Ethernet Logical Interfaced That Support IP Demux Subscriber Interfaces	326
	Features Supported with Static or Dynamic IP Demux Subscriber Interfaces over Aggregated Ethernet	326

Chapter 21	Configuring Subscriber Interfaces over Aggregated Ethernet	329
	Configuring a Static VLAN Subscriber Interface over Aggregated Ethernet ...	329
	Configuring a Static or Dynamic IP Demux Subscriber Interface over Aggregated Ethernet	331
	Configuring the Number of Aggregated Ethernet Logical Interfaces on the Router	332
	Configuring Ethernet Links as Members of an Aggregated Ethernet Logical Interface for a Static or Dynamic IP Demux Subscriber Interface	332
	Configuring an Aggregated Ethernet Logical Interface to Support a Static or Dynamic IP Demux Subscriber Interface	333
	Configuring a Static IP Demux Subscriber Interface over an Aggregated Ethernet Logical Interface	334
	Configuring a Dynamic IP Demux Subscriber Interface over an Aggregated Ethernet Logical Interface	335
	Displaying Configuration Information About IP Demux Interfaces over Aggregated Ethernet	336
Chapter 22	Subscriber Interfaces over Aggregated Ethernet Examples	337
	Example: Configuring a Static Subscriber Interface on a VLAN Interface over Aggregated Ethernet	337
	Example: Configuring a Static Subscriber Interface on an IP Demux Interface over Aggregated Ethernet	340
Chapter 23	Summary of Subscriber Interface Statements	343
	address	343
	demux0	344
	demux-options	345
	demux-source	346
	family	347
	family	348
	filter	349
	interfaces	350
	interfaces	351
	mac-validate	352
	precedence	353
	preferred-source-address	354
	underlying-interface	355
	unit	356
	unit	357
	unnumbered-address	358
	vlan-id	359
	vlan-tagging	360

Part 6	Dynamic Firewall Services for Subscriber Access	
Chapter 24	Dynamic Firewall Services Overview	363
	Dynamic Firewall Filters Overview	363
	Firewall Filter Types	363
	Firewall Filter Components	364
	Firewall Filter Processing	364
	Guidelines for Creating and Applying Filters for Subscriber Interfaces	365
	Basic Filter Syntax	365
Chapter 25	Configuring Filters for Dynamic Profiles	367
	Dynamically Attaching Statically Created Filters	367
	Dynamically Attaching Filters Using RADIUS Variables	368
	Defining Dynamic Filter Processing Order	369
Chapter 26	Firewall Filter Examples	371
	Static Filter Examples	371
Part 7	Class of Service for Subscriber Access	
Chapter 27	Class of Service for Subscriber Access Overview	377
	CoS for Subscriber Access Overview	377
	Hardware Requirements for CoS for Dynamic Subscriber Access	377
	CoS and Static IP Demux Interface Set Overview	378
	Subscriber Interfaces that Provide Initial CoS Parameters Dynamically	
	Obtained from RADIUS Overview	378
	Dynamic Configuration of Initial CoS in Client Profiles	379
	Internal Variables for Dynamic Configuration of Initial Traffic	
	Shaping	379
	Internal Variables for Dynamic Configuration of Initial Scheduling and	
	Queuing	381
	Changing CoS Services Overview	385
	Types of CoS Variables Used in a Dynamic Service Profile	386
	Static and Dynamic CoS Configurations	386
	Scenarios for Static and Dynamic Configuration of CoS Parameters	386
	Guidelines for Configuring CoS for Subscriber Access	388

Chapter 28	Configuring Class of Service for Subscriber Access	389
	Configuring Static Scheduling and Queuing in a Dynamic Profile for Subscriber Access	389
	Configuring Dynamic Scheduling and Queuing in a Dynamic Profile for Subscriber Access	391
	Configuring Traffic Shaping and Scheduling in a Dynamic Profile	392
	Configuring Schedulers in a Dynamic Profile	393
	Configuring a Subscriber Interface to Provide Initial CoS Parameters	
	Dynamically Obtained from RADIUS	394
	Configuring RADIUS With Initial CoS Values for CoS Parameters	394
	Configuring a Subscriber Interface That Supports Hierarchical CoS	395
	Associate a Client Dynamic Profile with the Subscriber Interface	395
	Configuring Initial Traffic-Shaping Parameters to be Obtained from RADIUS	395
	Configuring Static Forwarding Classes and Scheduler Maps	396
	Configuring Initial Scheduling and Queuing Parameters to be Obtained from RADIUS	396
	Associating RADIUS-obtained CoS Parameters to the Subscriber Interface	397
	Configuring User-Defined CoS Variables in a Dynamic Service Profile	397
	Applying CoS to an Interface in a Dynamic Profile	400
	Configuring CoS on a Set of Static IP Demux Interfaces	400
Chapter 29	Class of Service for Subscriber Access Examples	403
	Example: Configuring Static Scheduling and Queuing for Subscriber Access	403
	Example: Configuring Aggregate Scheduling of Queues for Residential Subscribers on Static IP Demux Interfaces	404
	Example: Configuring Dynamic Scheduling and Queuing for Subscriber Access	406
	Example: Configuring a Subscriber Interface to Provide Initial CoS Parameters Dynamically Obtained from RADIUS	410
Chapter 30	Class of Service Shaping-Rate Adjustments Overview	413
	Hierarchical CoS Shaping-Rate Adjustments Overview	413
	CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview	414
	Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops	415
Chapter 31	Configuring Class of Service Shaping-Rate Adjustments	417
	Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops	417
	Configuring Static Logical Interface Sets to Serve as CoS Hierarchical Scheduler Nodes for Subscriber Loops	417
	Configuring the Logical Interfaces That Compose the Static Logical Interface Sets	418

	Configuring Hierarchical CoS on the Static Logical Interface Sets That Serve as Hierarchical Scheduler Nodes for Subscriber Local Loops	419
	Configuring ANCP Functionality That Supports and Drives Shaping-Rate Adjustments for Subscriber Local Loops	421
	Displaying Configuration Information About ANCP	422
	Displaying Configuration Information About Shaping-Rate Adjustments for Subscriber Local Loops	422
	Disabling CoS Shaping-Rate Adjustments for Subscriber Local Loops	423
Chapter 32	Class of Service Shaping-Rate Adjustments Examples	425
	Example: Configuring Hierarchical CoS Shaping-Rate Adjustments for Subscriber Local Loops	425
Chapter 33	Summary of Class of Service for Subscriber Access Statements	429
	buffer-size	430
	class-of-service	431
	delay-buffer-rate	432
	drop-profile	433
	drop-profile-map	434
	forwarding-class	435
	guaranteed-rate	436
	interfaces	437
	loss-priority	438
	output-traffic-control-profile	438
	priority	439
	protocol	440
	scheduler	440
	scheduler-map	441
	scheduler-maps	442
	schedulers	443
	shaping-rate	444
	traffic-control-profiles	445
	transmit-rate	446
	unit	447
Part 8	Dynamic Protocols for Subscriber Access	
Chapter 34	Dynamic Protocol Configuration Overview	451
	Dynamic IGMP Configuration Overview	451

Chapter 35	Summary of IGMP Dynamic Profile Statements	453
	accounting	453
	disable	454
	group	455
	group-policy	456
	igmp	457
	immediate-leave	458
	interface	459
	no-accounting	460
	promiscuous-mode	460
	protocols	461
	source	462
	ssm-map	462
	static	463
	version	464
Chapter 36	ANCP Overview	465
	ANCP Topology Discovery and Traffic Monitoring Overview	465
Chapter 37	Configuring ANCP	467
	Configuring ANCP	467
	Configuring ANCP Neighbors	468
	Tracing ANCP Operations	468
	Configuring the ANCP Trace Log Filename	469
	Configuring the Number and Size of ANCP Log Files	469
	Configuring Access to the ANCP Log File	470
	Configuring a Regular Expression for ANCP Lines to Be Logged	470
	Configuring the ANCP Tracing Flags	471
	Associating an Access Node with Subscribers for ANCP Operations	471
	Specifying the Interval Between ANCP Adjacency Messages	472
	Specifying How Long Processes Wait for ANCP Restart to Complete	472
	Configuring ANCP for Backwards Compatibility	473
	Configuring ANCP to Adjust CoS Traffic Shaping	473
Chapter 38	Summary of ANCP Statements	475
	ancp	475
	access-identifier	476
	adjacency-timer	476
	interfaces	477
	interface-set	477
	maximum-helper-restart-time	478
	neighbor	478
	pre-ietf-mode	479
	qos-adjust	479
	traceoptions	480

Part 9	Subscriber Access Examples	
Chapter 39	Service Profile Examples	485
	Example: Configuring a Tiered Service Profile for Subscriber Access	485
Part 10	Complete Configuration Statement Hierarchy for Subscriber Access	
Chapter 40	Subscriber Access Statement Hierarchy	491
	[edit access address-assignment] Hierarchy Level	491
	[edit access profile] Hierarchy Level	491
	[edit dynamic-profiles] Hierarchy Level	493
	[edit forwarding-options dhcp-relay] Hierarchy Level	494
	[edit-protocols ancp] Hierarchy Level	496
	[edit services mobile-ip] Hierarchy Level	496
	[edit services radius-flow-tap] Hierarchy Level	497
	[edit system services dhcp-local-server] Hierarchy Level	497
Part 11	Index	
	Index	501
	Index of Statements and Commands	509

List of Figures

Figure 1: Subscriber Access Network Example	5
Figure 2: Subscriber Access Operation Flow	6
Figure 3: Subscriber Access Configuration Workflow	11
Figure 4: Subscriber Secure Policy Architecture	106
Figure 5: VLAN Subscriber Interfaces	307
Figure 6: IP Demux Subscriber Interface	307

List of Tables

Table 1: Notice Icons	xxxii
Table 2: Text and Syntax Conventions	xxxii
Table 3: Technical Documentation for Supported Routing Platforms	xxxiv
Table 4: JUNOS Software Network Operations Guides	xxxviii
Table 5: JUNOS Software for J-series Services Routers and SRX-series Services Gateways Documentation	xxxix
Table 6: Additional Books Available Through http://www.juniper.net/books	xl
Table 7: Subscriber Access Terms and Acronyms	4
Table 8: Supported RADIUS IETF Attributes	29
Table 9: Supported Juniper Networks VSAs	32
Table 10: Error-Cause Codes (RADIUS Attribute 101)	37
Table 11: DHCP-Attributes Statements	42
Table 12: ARP Table in Trusted Environment	58
Table 13: ARP Table in Distrusted Environment	58
Table 14: ARP Table in Trusted Environment	82
Table 15: ARP Table in Distrusted Environment	82
Table 16: DHCP Relay Agent Option 82 Value for Auto Logout	86
Table 17: Subscriber Secure Policy Terms	104
Table 18: Subscriber Secure Policy Configuration Steps	106
Table 19: RADIUS-Initiated Mirroring at Subscriber Login	106
Table 20: RADIUS-Initiated Mirroring for Current Subscriber	107
Table 21: RADIUS Attributes Used as Traffic Mirroring Triggers	108
Table 22: RADIUS-Based Mirroring Attributes	108
Table 23: LI-Action VSA Action	109
Table 24: Juniper VSAs used by Mobile IP	246
Table 25: JUNOS Predefined Internal Variables and Definitions	277
Table 26: Features Supported with Static or Dynamic IP Demux Subscriber Interfaces	326
Table 27: Scheduler Mapping for Interface Sets	378
Table 28: JUNOS Internal Variables for Dynamic Configuration of Initial Traffic Shaping	380
Table 29: JUNOS Internal Variables for Dynamic Configuration of Initial Scheduling and Queuing	381
Table 30: CoS Services and Variables	387
Table 31: Initial CoS Values for Subscriber Login	407
Table 32: Upgraded CoS Values for the Video Service	410

About This Guide

This preface provides the following guidelines for using the *JUNOS® Software Subscriber Access Configuration Guide*:

- Objectives on page xxix
- Audience on page xxix
- Supported Routing Platforms on page xxx
- Using the Indexes on page xxx
- Using the Examples in This Manual on page xxx
- Documentation Conventions on page xxxii
- List of Technical Publications on page xxxiv
- Documentation Feedback on page xl
- Requesting Technical Support on page xli

Objectives

This guide provides an overview of the subscriber access management features of the JUNOS software and describes how to configure and manage remote subscriber access on the routing platform.



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

Audience

This guide is designed for network administrators who are configuring and monitoring a Juniper Networks MX-series routing platform.

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

- Border Gateway Protocol (BGP)
- Distance Vector Multicast Routing Protocol (DVMRP)

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

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

Supported Routing Platforms

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

- MX-series

Using the Indexes

This reference contains two indexes: a complete index that includes topic entries, and an index of statements and commands only.

In the index of statements and commands, an entry refers to a statement summary section only. In the complete index, the entry for a configuration statement or command contains at least two parts:

- The primary entry refers to the statement summary section.
- The secondary entry, usage guidelines, refers to the section in a configuration guidelines chapter that describes how to use the statement or command.

Using the Examples in This Manual

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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


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

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

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

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

Documentation Conventions

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

Table 1: Notice Icons





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

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

Table 2: Text and Syntax Conventions

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

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

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

List of Technical Publications

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

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

Table 3: Technical Documentation for Supported Routing Platforms

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

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

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

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

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

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

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

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

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

Table 4: JUNOS Software Network Operations Guides

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

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

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

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

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

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

Documentation Feedback

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

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

Part 1

Managing Access Networks

- Subscriber Access Overview on page 3

Chapter 1

Subscriber Access Overview

- Subscriber Access Overview on page 3
- Subscriber Access Environment on page 4
- Relationship Between Subscribers and Interfaces in an Access Network on page 5
- Subscriber Access Support Limitations on page 5
- Subscriber Access Licensing Overview on page 6
- Subscriber Access Operation Flow on page 6
- Activating Subscribers and Managing Services in an Access Network on page 7
- Configuring Subscriber Access on page 8

Subscriber Access Overview

The JUNOS subscriber access feature provides subscriber access, authentication, and service creation, activation, and deactivation. You can also collect accounting information and statistics for subscriber service sessions.

The subscriber access feature supports both CLI and AAA-based configuration (such as RADIUS) for subscribers. Access and services start when the router receives a message from a client (such as a DHCP discover message). For RADIUS clients, RADIUS Access-Accept messages and Change-of-Authorization-Request (CoA-Request) messages can create, modify, and delete subscriber sessions as well as activate and deactivate service sessions. You can use CLI commands to create a dynamic profile, which act as a template of user attributes.

A subscriber service is based on the combination of a defined dynamic profile and attributes configured through authentication. Dynamic profiles can include dynamic firewall filters, class of service (CoS) settings, and protocol (IGMP) settings that define access limits for subscribers and the scope of a service granted to the subscriber once access is obtained.

The subscriber access feature provides the following convenience and flexibility to service providers and subscribers:

- Service providers can separate services and access technology and eliminate unprofitable flat-rate billing. They gain the ability to efficiently design, manage, and deliver services that subscribers want, and then bill subscribers based on connect time, bandwidth, and the actual service used.

- Subscribers benefit by gaining access to multiple simultaneous services. Depending on the service provider configuration, subscribers can dynamically connect to and disconnect from various services when they want and for however long they want. Subscribers can be billed based on the service level and usage, rather than being charged a set rate regardless of usage.

Subscriber Access Terms and Acronyms

Table 7 on page 4 defines terms and acronyms that are used in this discussion of subscriber access.

Table 7: Subscriber Access Terms and Acronyms

Term	Definition
Dynamic profile	A template that defines a set of characteristics that are combined with authorization attributes and are dynamically assigned to static interfaces to provide dynamic subscriber access and services for broadband applications.
AAA method for subscriber authentication	The AAA method that uses authentication (for example, including RADIUS VSAs in the Access-Accept packet) to verify a subscriber and activate a service when the subscriber logs in.
RADIUS CoA method	The method that uses RADIUS CoA-Request messages and VSAs to activate a service for a subscriber that is already logged in.

Related Topics

- Subscriber Access Environment on page 4
- Subscriber Access Licensing Overview on page 6
- Subscriber Access Operation Flow on page 6
- Configuring Subscriber Access on page 8

Subscriber Access Environment

A subscriber access environment can include various components, including subscriber access and authentication protocols.

The subscriber access protocols include:

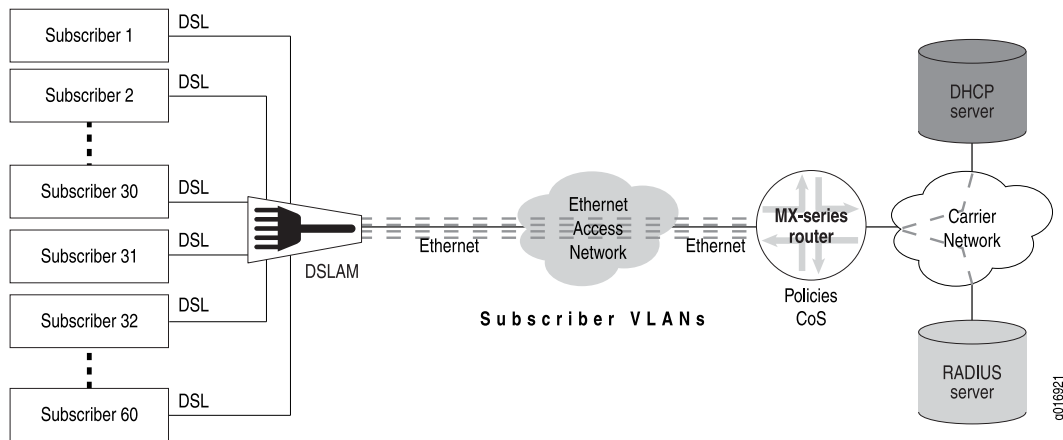
- Dynamic Host Configuration Protocol (DHCP) server
 - Local DHCP server
 - External DHCP server

The subscriber authentication protocols include the RADIUS server.

In addition to these components, a subscriber access environment would also include various access protocols (for example, DHCP) and might use local authentication instead of authenticating clients through a RADIUS server.

Figure 1 on page 5 shows an example of a basic subscriber access network.

Figure 1: Subscriber Access Network Example



Related Topics ■ Subscriber Access Overview on page 3

Relationship Between Subscribers and Interfaces in an Access Network

To the router, a subscriber is an authenticated user. This release supports configurations of only one subscriber per logical interface. However, a subscriber can be either an individual, authenticated client or a group of clients on a single, authenticated VLAN.

Related Topics ■ Subscriber Interface Overview on page 305

Subscriber Access Support Limitations

The subscriber access feature is limited to MX-series routers and the interfaces you can use when configuring dynamic profiles.

Platform Support

Even though many statements appear in the CLI for various other platforms, Juniper Networks supports subscriber access configuration only on MX-series routers.

Interface Support

In this release, you can use dynamic profiles to configure only statically created interfaces. To do so, you must first configure the interfaces on the router to which you expect clients to connect.

The subscriber access feature supports the following device types:

- GE -- Gigabit Ethernet

- XE -- 10-Gigabit Ethernet
- AE -- Aggregated Ethernet

Subscribers can be identified through a VLAN or a static IP demux interface on a supported device.

- Related Topics**
- Relationship Between Subscribers and Interfaces in an Access Network on page 5
 - Configuring Subscriber Access on page 8

Subscriber Access Licensing Overview

To enable some JUNOS software features or router scaling levels, you might have to purchase, install, and manage separate software license packs. The presence on the router of the appropriate software license keys (passwords) determines whether you can configure and use certain features or configure a feature to a predetermined scale.

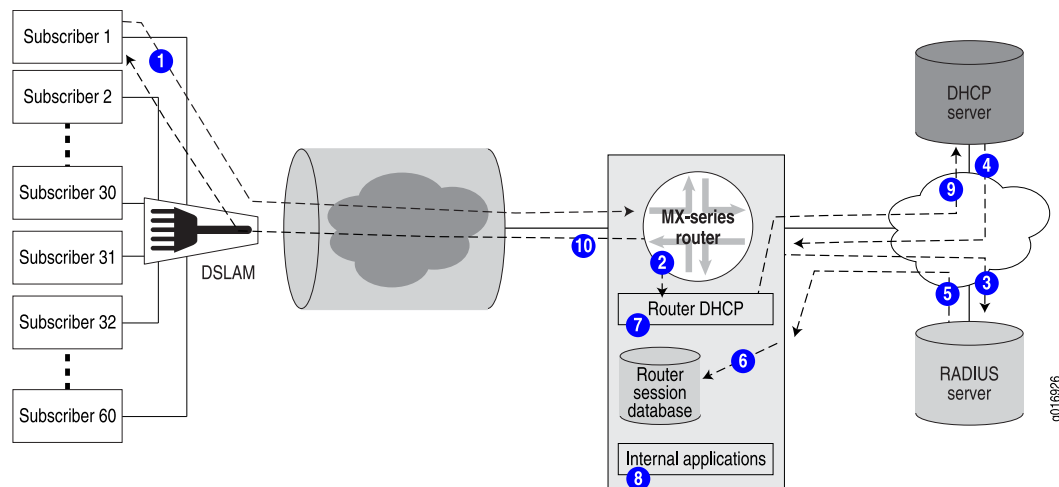
- Related Topics**
- For information about installing and managing JUNOS licenses, see the *JUNOS Software Installation and Upgrade Guide*

Subscriber Access Operation Flow

The subscriber access feature requires that a DHCP client send a DHCP discover message to the router interface to initialize dynamic configuration of that interface.

Figure 2 on page 6 shows the flow of operations that occur when the router is using DHCP relay to enable access for a subscriber.

Figure 2: Subscriber Access Operation Flow



The following general sequence occurs during access configuration for a DHCP client:

1. The client issues a DHCP discover message.
2. The router DHCP component recognizes the DHCP message and adds the client to the router session database.
3. If configured, the router issues an authorization request to the RADIUS server.
4. The DHCP server issues an IP address for the client. When the address is relayed, the address is added to the router session database.
5. RADIUS issues an authorization response to the router.
6. The router adds RADIUS authorization information to the router session database.
7. The router combines the dynamic profile with the RADIUS authorization information.
8. The router alerts all internal applications involved with the subscriber access (for example, routing protocols, dynamic firewall, and dynamic Class of Service).
9. The router passes the message through to the DHCP server.
10. The router DHCP component sends an acknowledgement back to the client.

The subscriber now has access to the network and the authorized service.

- Related Topics**
- Subscriber Access Overview on page 3
 - Configuring Subscriber Access on page 8

Activating Subscribers and Managing Services in an Access Network

The subscriber access feature uses dynamic profiles to activate subscribers and manage services.

A dynamic profile is a set of characteristics, defined in a template, that the router uses to provide dynamic subscriber access and services.

By using dynamic profiles you can:

- Define access for your network
- Define different service levels for subscribers
- Preprovision services that you can activate later

Using AAA-based login (RADIUS-based login or RADIUS CoA) you can:

- Provide subscribers with dynamic activation and deactivation based on service selection
- Provide greater flexibility and efficient management for a large number of subscribers and services

Components of a Dynamic Profile

You can use dynamic profiles to define various router components for subscriber access.

These components include the following:

- Dynamic firewall filters—Includes input and output filters to enforce rules that define whether to permit or deny packets that are transmitting an interface on the router. To apply dynamic firewall filters to the subscriber interface, you configure static input and output firewall filters and reference those filters in dynamic profiles.
- Dynamic Class of Service (CoS)—Includes CoS values that define a service for a subscriber. For example, you can configure the the shaping rate for traffic in a video service by referencing CoS statements in a dynamic profile.
- Dynamic signaling protocol—Includes dynamic IGMP configuration for host to router signaling for IPv4 to support IP multicasting.

Router Internal Variables Used by Dynamic Profiles

The router contains several internal variables that enable dynamic association of interfaces and logical units to incoming subscriber requests. You must specify these internal variables in certain statements within a dynamic profile. When a client accesses the router, the dynamic profile configuration replaces the internal variable with the actual interface name or unit value for the interface the client is accessing.

The internal variables include:

- `$junos-interface-ifd-name`—Replaced with the actual interface device name.
- `$junos-underlying-interface-unit`—Replaced with the actual logical unit number.

Related Topics

- Dynamic Profiles Overview on page 275
- Subscriber Interface Overview on page 305

Configuring Subscriber Access

To configure subscriber access, perform the following tasks:

1. Configure the client access protocol.

Configure one of the following DHCP access methods:

- Configure DHCP local server.

See “Extended DHCP Local Server Overview” on page 48.

- Configure DHCP relay.

See “Extended DHCP Relay Agent Overview” on page 72.

2. Configure subscriber authentication, accounting, and addressing.

- a. Configure RADIUS:
 1. Specify the RADIUS servers.

See “Specifying the RADIUS Authentication and Accounting Servers for Subscriber Access” on page 21.
 2. Specify any optional server attributes.

See “Configuring RADIUS Server Options for Subscriber Access” on page 21.
 3. (Optional) Configure the CoA feature for the RADIUS dynamic-request server to change or deactivate the service after login.

See “Configuring RADIUS-Initiated Dynamic Request Support” on page 28.
 4. Configure subscriber accounting (RADIUS accounting).

See “Configuring How Accounting Statistics Are Collected for Subscriber Access” on page 20.
- b. Configure addressing:
 - Configure address-assignment pools.

See “Configuring Address-Assignment Pools” on page 39.
3. Create and manage dynamic profiles for access and service.
 - a. Configure a basic dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 283.
 - b. Configure a dynamic profile for access.

See “Configuring a Dynamic Profile for Client Access” on page 287.
 - c. Configure a dynamic profile for services.

See “Configuring a Dynamic Profile for Various Levels of Services” on page 288.
 - d. Configure the static subscriber interfaces to be referenced in the dynamic profile.

See “Configuring a Subscriber Interface with a Static VLAN Interface” on page 312.
 - e. Specify the interface-name and unit variables that the router uses to dynamically associate to a subscriber’s incoming interface.

See “Associating Dynamic Profiles with Statically Created Interfaces” on page 312.
 - f. Add, modify, or delete dynamic profile values to manage subscriber access and services.

See “Modifying Dynamic Profiles” on page 289.

The router dynamically activates or modifies the subscriber service using the RADIUS configuration.

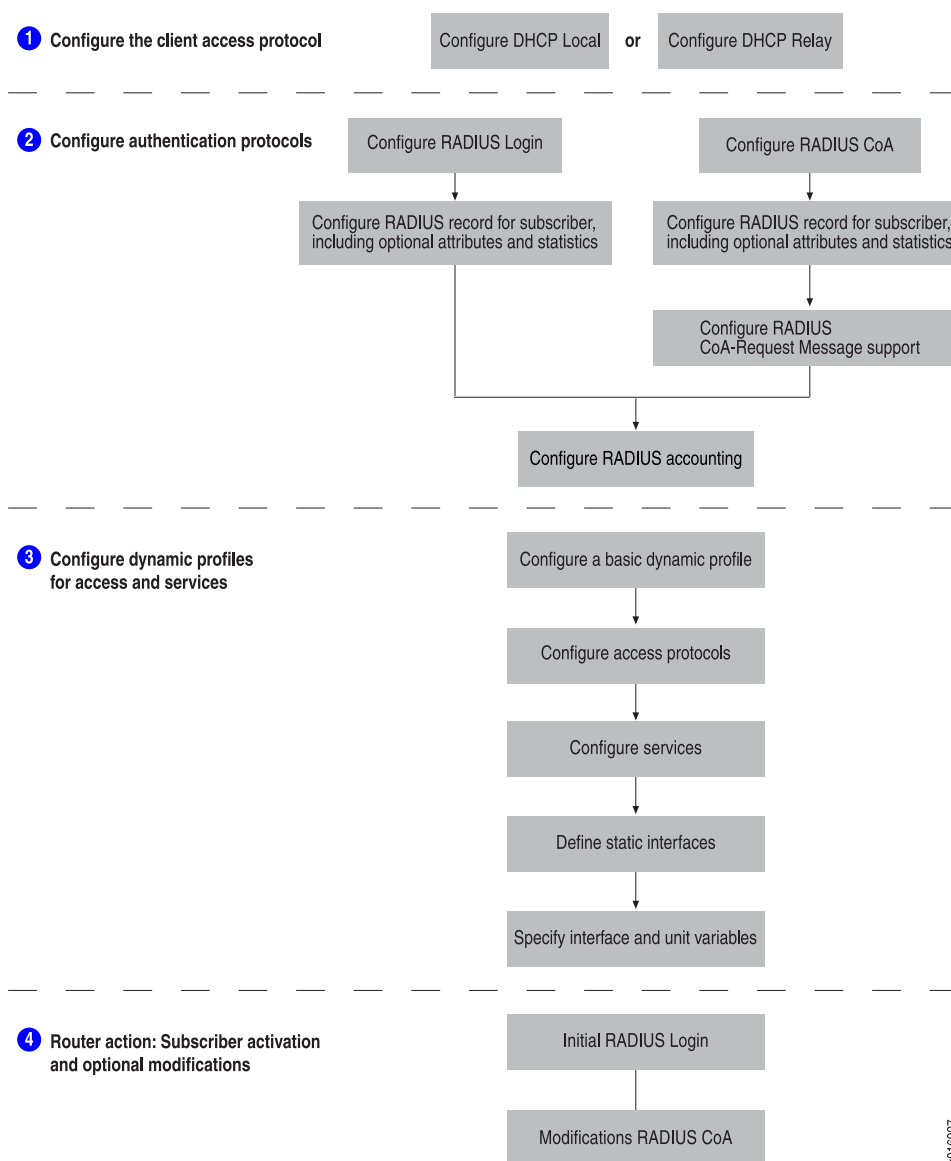
- When the subscriber logs in, the router dynamically activates the service.

See “Dynamic Service Activation During Login Overview” on page 25.

- If RADIUS CoA has been configured, the router can dynamically modify the service for a subscriber.

See “RADIUS-Initiated Change of Authorization (CoA) Overview” on page 26.

Figure 3 on page 11 shows the configuration sequence you perform for subscriber access. It also shows the dynamic configuration performed by the router.

Figure 3: Subscriber Access Configuration Workflow

9016927

- Related Topics**
- Subscriber Access Overview on page 3
 - Subscriber Access Support Limitations on page 5

Part 2

Subscriber Management

- Subscriber Management Overview on page 15
- Configuring the AAA Service Framework for Subscriber Access on page 17
- Configuring Address-Assignment Pools for Subscriber Access on page 39
- Configuring DHCP Local Server for Subscriber Access on page 47
- Configuring DHCP Relay for Subscriber Access on page 71
- Configuring Subscriber Secure Policy Traffic Mirroring on page 103
- AAA and Remote Subscriber Access Configuration Examples on page 115
- Summary of AAA and Remote Subscriber Access Statements on page 123

Chapter 2

Subscriber Management Overview

- Subscriber Access Management Overview on page 15

Subscriber Access Management Overview

The subscriber access management feature enables you to manage the subscribers that are allowed access to the network server, the services that authorized subscribers can use, and how accounting statistics are collected. The subscriber access management feature uses the AAA Service Framework to support the configuration and management of broadband subscriber access. You can statically configure different client types, such as DHCP-based subscribers, and specify the authentication, accounting, and service for the subscribers.

Chapter 3

Configuring the AAA Service Framework for Subscriber Access

- AAA Service Framework Overview on page 17
- Router Interaction with RADIUS Servers Overview on page 18
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 19
- Specifying the Authentication and Accounting Methods for Subscriber Access on page 19
- Configuring How Accounting Statistics Are Collected for Subscriber Access on page 20
- Configuring RADIUS Server Parameters for Subscriber Access on page 21
- Using RADIUS Dynamic Requests for Subscriber Access Management on page 25
- Dynamic Service Activation During Login Overview on page 25
- RADIUS-Initiated Change of Authorization (CoA) Overview on page 26
- RADIUS-Initiated Disconnect Overview on page 27
- Configuring RADIUS-Initiated Dynamic Request Support on page 28
- Verifying and Managing the RADIUS Dynamic-Request Feature on page 28
- RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 29
- RADIUS IETF Attributes Supported by the AAA Service Framework on page 29
- Juniper Networks VSAs Supported by the AAA Service Framework on page 32
- Error-Cause Codes (RADIUS Attribute 101) for Dynamic Requests on page 36
- Attaching Access Profiles on page 37
- Verifying and Managing Subscriber Information on page 37

AAA Service Framework Overview

The AAA Service Framework provides a single point of contact for all the authentication, authorization, accounting, address assignment, and dynamic request services that the router supports for network access. The framework supports authentication and authorization through external servers, such as RADIUS. The framework also supports accounting and dynamic-request CoA and disconnect

operations through external servers, and address assignment through a combination of local address-assignment pools and RADIUS.

When interacting with external back-end RADIUS servers, the AAA Service Framework supports standard RADIUS attributes and Juniper Networks vendor specific attributes (VSAs). The AAA Service Framework also includes an integrated RADIUS client that is compatible with RADIUS servers that conform to RFC-2865, RFC-2866, and RFC-3576, and which can initiate requests.

You create the following types of configurations to manage subscriber access.

- Authentication—Authentication parameters defined in the access profile determine the authentication component of the AAA processing. For example, subscribers can be authenticated using an external authentication service such as RADIUS.
- Accounting—Accounting parameters in the access profile specify the accounting part of the AAA processing. For example, the parameters determine how the router collects and uses subscriber statistics.
- RADIUS-initiated dynamic requests—A list of authentication server IP addresses in the access profile specify the RADIUS servers that can initiate dynamic requests to the router. Dynamic requests include CoA requests, which specify VSA modifications and service changes, and disconnect requests, which terminate subscriber sessions. The list of authentication servers also provide RADIUS-based dynamic service activation and deactivation during subscriber login.
- Address assignment—The AAA Service Framework assigns addresses to subscribers based on the configuration of local address-assignment pools. For example, the AAA framework collaborates with RADIUS servers to assign addresses from the specified pools.
- Subscriber secure policy—RADIUS VSAs and attributes provide RADIUS-initiated traffic mirroring on a per-subscriber basis.

- Related Topics**
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 19
 - Configuring Address-Assignment Pools on page 39

Router Interaction with RADIUS Servers Overview

To identify the RADIUS servers that the router can use and to configure how the router interacts with the servers, you include the `radius-server` statement at the `[edit access]` hierarchy level. You can specify multiple RADIUS servers on the network.

```
[edit access]
radius-server server-address {
  accounting-port port-number;
  port port-number;
  retry attempts;
  secret password;
  source-address source-address;
  timeout seconds;
}
```


The following list describes the **radius-server** configuration statements:

- **server-address**—The address of the RADIUS server to use. To configure more than one RADIUS server, include multiple **server-address** entries.
- **accounting-port**—The RADIUS server accounting port number. The default accounting port number is 1813.
- **port-number**—The port number used to contact the RADIUS server. The default is port number 1812.
- **retry**—The number of times that the router attempts to contact a RADIUS accounting server. You can configure the router to retry from 1 through 16 times. The default setting is 3 retry attempts.
- **secret**—The required secret (password) that the local router passes to the RADIUS client. Secrets can contain spaces.
- **source-address**—A source address for the RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address. The source address is a valid IPv4 address configured on one of the router interfaces.
- **timeout**—The length of time that the local router waits to receive a response from a RADIUS server. By default, the router waits 3 seconds. You can configure the timeout to be from 1 through 90 seconds.

Configuring Authentication and Accounting Parameters for Subscriber Access

You use an access profile to configure authentication and accounting support for the subscriber access management feature. The access profile enables you to specify the type of methods used for authentication and accounting. You can also configure how subscriber access management collects and uses accounting statistics.

- Related Topics**
- Specifying the Authentication and Accounting Methods for Subscriber Access on page 19
 - Configuring How Accounting Statistics Are Collected for Subscriber Access on page 20

Specifying the Authentication and Accounting Methods for Subscriber Access

To specify the authentication and accounting methods that subscriber access management uses, you include the **authentication-order** statement and **accounting order** statements at the **[edit access profile *profile-name*]** hierarchy level.

```
[edit access profile profile-name]
authentication-order [ authentication-methods ]
}
accounting {
    order [ accounting-methods ];
}
```

You can configure multiple authentication and accounting methods—the **authentication-order** and **accounting order** statements specify the order in which the subscriber access management feature uses the methods. For example, an

authentication entry of **radius password** specifies that RADIUS authentication is performed first and, if it fails, local authentication (**password**) is done.

```
[edit access profile profile-name]  
authentication-order radius password;
```

You can specify the following authentication methods:



NOTE: The **password** keyword is not supported by the subscriber access management feature in this release.

- **password**—Local authentication
- **radius**—RADIUS-based authentication

You can specify the following accounting methods:

- **radius**—RADIUS-based accounting

Configuring How Accounting Statistics Are Collected for Subscriber Access

Include the **accounting** statement at the [edit access profile *profile-name*] hierarchy level to specify how the subscriber access management feature collects and uses accounting statistics.

```
[edit access profile profile-name]  
accounting {  
    accounting-stop-on-access-deny;  
    accounting-stop-on-failure;  
    order [ accounting-method ];  
    statistics (time | volume-time);  
    update-interval minutes;  
}
```

The following list describes the accounting statements:

- **accounting-stop-on-access-deny**—Configures AAA to issue an Acct-Stop message if the AAA server denies access to the subscriber.
- **accounting-stop-on-failure**—Configures the AAA servers to send an Acct-Stop message if the subscriber fails AAA but is granted access by the AAA-server.
- **order**—The order in which multiple accounting methods are used. For example, an entry of **radius** specifies that the router use RADIUS accounting and, if that fails, no accounting is performed.
- **statistics**—The types of statistics to gather. You can specify that the router collect both volume and time statistics or only time statistics for subscriber sessions. When you change the type of statistics being collected, current subscribers

continue to use the previous collection specification—subscribers who log in after the change use the new specification.

- **update-interval**—Configures the number of minutes between accounting updates. You can configure an interval from 10 through 1440 minutes. If you specify an interval of 10 through 15, the interval is rounded up to 15.

Configuring RADIUS Server Parameters for Subscriber Access

Include the **radius** statement at the [edit access profile *profile-name*] hierarchy level to specify the RADIUS parameters for the subscriber access manager feature. You can specify the IP addresses of the RADIUS servers used for authentication and accounting, options that provide configuration information for the RADIUS servers, and how RADIUS attributes are used.

- Specifying the RADIUS Authentication and Accounting Servers for Subscriber Access on page 21
- Configuring RADIUS Server Options for Subscriber Access on page 21
- Configuring How RADIUS Attributes Are Used for Subscriber Access on page 23

Specifying the RADIUS Authentication and Accounting Servers for Subscriber Access

To specify one or more RADIUS authentication or accounting servers to use for subscriber access management, include the **authentication-server** and **accounting-server** statements at the [edit access profile *profile-name* radius] hierarchy level. You must specify the IP address for the authentication or accounting server.

```
[edit access profile profile-name radius]
authentication-server [ ip-address ];
accounting-server [ ip-address ];
```

To configure multiple RADIUS authentication or accounting servers, include multiple *ip-address* entries, for example:

```
[edit access profile profile-name radius]
authentication-server 192.168.1.1 192.168.1.2 192.168.1.3;
accounting-server 192.168.1.1 192.168.1.3 192.168.1.4;
```

Configuring RADIUS Server Options for Subscriber Access

Include the **options** statement at the [edit access profile *profile-name* radius] hierarchy level to specify the options used by the RADIUS authentication and accounting servers.

```
[edit access profile profile-name radius]
options {
  accounting-session-id-format (decimal | description);
  ethernet-port-type-virtual;
  interface-description-format [sub-interface | adapter];
  nas-identifier identifier-value;
  nas-port-extended-format {
    adapter-width width;
    port-width width;
```



```

        slot-width width;
        stacked-vlan-width width;
        vlan-width width;
    }
    override-nas-information;
    revert-interval interval;
    vlan-nas-port-stacked-format;
}

```

The following list describes the accounting options:

- **accounting-session-id-format**—The format the router uses to identify the accounting session. The identifier can be in one of the following formats. The router uses decimal format by default.
 - **decimal**—For example, 435264
 - **description**—In the format, *jnpr interface-specifier:subscriber-session-id*. For example, *jnpr fastEthernet 3/2.6:1010101010101*
- **ethernet-port-type-virtual**—The physical port type the router uses to authenticate clients. The port type is passed in RADIUS attribute 61 (NAS-Port-Type). This statement specifies a port type of *virtual*; by default the router passes a port type of *ethernet* in RADIUS attribute 61.
- **interface-description-format**—The information that is included in or omitted from the interface description that the router passes to RADIUS for inclusion in the RADIUS attribute 87 (NAS-Port-Id). By default, the router includes both the subinterface and the adapter in the interface description.
- **nas-identifier**—The value for the client RADIUS attribute 32 (NAS-Identifier), which is used for authentication and accounting requests. You can specify a string in the range 1 to 64 characters.
- **nas-port-extended-format**—Configures the RADIUS client to use the extended format for RADIUS attribute 5 (NAS-Port) and specify the width of the fields in the NAS-Port attribute.
 - **adapter-width *width***—Number of bits in the adapter field.
 - **port-width *width***—Number of bits in the port field.
 - **slot-width *width***—Number of bits in the slot field.
 - **stacked-vlan-width *width***—Number of bits in the SVLAN ID field.
 - **vlan-width *width***—Number of bits in the VLAN ID field.
- **revert-interval**—The amount of time that the router waits after a server has become unreachable. The router rechecks the connection to the server when the revert-interval expires. If the server is then reachable, it is used in accordance with the order of the server list.
- **vlan-nas-port-stacked-format**—Configures RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.

Configuring How RADIUS Attributes Are Used for Subscriber Access

Include the `attributes` statement at the `[edit access profile profile-name radius]` hierarchy level to specify attributes that are ignored in RADIUS Access-Accept messages, or that are excluded from particular RADIUS message types.

```
[edit access profile profile-name radius]
attributes {
  ignore {
    framed-ip-netmask;
    input-filter;
    logical-system:routing-instance;
    output-filter;
  }
  exclude
    accounting-authentic [ accounting-on | accounting-off ];
    accounting-delay-time [ accounting-on | accounting-off ];
    accounting-session-id [ access-request | accounting-on | accounting-off |
      accounting-stop ];
    accounting-terminate-cause [ accounting-off ];
    called-station-id [ access-request | accounting-start | accounting-stop ];
    calling-station-id [ access-request | accounting-start | accounting-stop ];
    class [ accounting-start | accounting-stop ];
    dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
    dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
    output-filter [ accounting-start | accounting-stop ];
    event-timestamp [ accounting-on | accounting-off | accounting-start |
      accounting-stop ];
    framed-ip-address [ accounting-start | accounting-stop ];
    framed-ip-netmask [ accounting-start | accounting-stop ];
    input-filter [ accounting-start | accounting-stop ];
    input-gigapackets [ accounting-stop ];
    input-gigawords [ accounting-stop ];
    interface-description [ access-request | accounting-start | accounting-stop ];
    nas-identifier [ access-request | accounting-on | accounting-off | accounting-start
      | accounting-stop ];
    nas-port [ access-request | accounting-start | accounting-stop ];
    nas-port-id [ access-request | accounting-start | accounting-stop ];
    nas-port-type [ access-request | accounting-start | accounting-stop ];
    output-gigapackets [ accounting-stop ];
    output-gigawords [ accounting-stop ];
  }
}
```

The following list describes the ignore and exclude statements:

- Use the `ignore` statement to configure the router to ignore a particular attribute in RADIUS Access-Accept messages. By default, the router processes the attributes received from the external AAA server. You can specify that the following attributes are ignored:
 - `framed-ip-netmask`—Framed-Ip-Netmask, RADIUS attribute 9
 - `input-filter`—Ingress-Policy-Name, VSA 26-10

- `logical-system:routing-instance`—Virtual-Router, VSA 26-1
- `output-filter`—Egress-Policy-Name, VSA 26-11
- Use the `exclude` statement to configure the router to exclude the specified attributes from the specified type of RADIUS message. Not all attributes appear in all types of RADIUS messages—the CLI indicates the RADIUS message type. By default, the router includes the specified attributes in RADIUS Access-Request, Acct-On, Acct-Off, Acct-Start, and Acct-Stop messages. You can configure the router to exclude the following attributes:
 - `accounting-authentic`—RADIUS attribute 45, Acct-Authentic
 - `accounting-delay-time`—RADIUS attribute 41, Acct-Delay-Time
 - `accounting-session-id`—RADIUS attribute 44, Acct-Session-Id
 - `accounting-terminate-cause`—RADIUS attribute 49, Acct-Terminate-Cause
 - `called-station-id`—RADIUS attribute 30, Called-Station-Id
 - `calling-station-id`—RADIUS attribute 31, Calling-Station-Id
 - `class`—RADIUS attribute 25, Class
 - `dhcp-gi-address`—Juniper VSA 26-57, DHCP-GI-Address
 - `dhcp-mac-address`—Juniper VSA 26-56, DHCP-MAC-Address
 - `event-timestamp`—RADIUS attribute 55, Event-Timestamp
 - `framed-ip-address`—RADIUS attribute 8, Framed-IP-Address
 - `framed-ip-netmask`—RADIUS attribute 9, Framed-IP-Netmask
 - `input-filter`—Juniper VSA 26-10, Ingress-Policy-Name
 - `input-gigapackets`—Juniper VSA 26-42, Acct-Input-Gigapackets
 - `input-gigawords`—RADIUS attribute 52, Acct-Input-Gigawords
 - `interface-description`—Juniper VSA 26-53, Interface-Desc
 - `nas-identifier`—RADIUS attribute 32, NAS-Identifier
 - `nas-port`—RADIUS attribute 5, NAS-Port
 - `nas-port-id`—RADIUS attribute 87, NAS-Port-Id
 - `nas-port-type`—RADIUS attribute 61, NAS-Port-Type
 - `output-filter`—Juniper VSA 26-11, Egress-Policy-Name
 - `output-gigapackets`—Juniper VSA 25-43, Acct-Output-Gigapackets
 - `output-gigawords`—RADIUS attribute 53, Acct-Output-Gigawords

Using RADIUS Dynamic Requests for Subscriber Access Management

RADIUS dynamic requests provide an efficient way to centrally manage subscriber sessions. The AAA Service Framework's RADIUS dynamic request support allows RADIUS servers to initiate user-related operations, such as a termination operation, by sending unsolicited request messages to the router. Without the RADIUS dynamic request feature, the only way to disconnect a RADIUS user is from the router, which can be cumbersome and time-consuming in large networks.

In a typical client-server RADIUS environment, the router functions as the client and initiates requests sent to the remote RADIUS server. However, when using RADIUS dynamic requests, the roles are reversed. For example, during a disconnect operation, the remote RADIUS server performs as the client and initiates the request (the disconnect action) — the router functions as the server in the relationship.

You create an access profile to configure the router to support RADIUS dynamic requests. This configuration enables the router to receive and act on the following types of messages from remote RADIUS servers:

- Access-Accept messages—Dynamically activate services based on attributes in RADIUS Access-Accept messages received when a subscriber logs in.
- Change-of-Authorization (CoA) messages—Dynamically modify active sessions based on attributes in CoA messages. CoA messages can include service creation requests, deletion requests, RADIUS attributes, and Juniper Networks VSAs.
- Disconnect messages—Immediately terminate specific subscriber sessions.

Related Topics

- Dynamic Service Activation During Login Overview on page 25
- RADIUS-Initiated Change of Authorization (CoA) Overview on page 26
- RADIUS-Initiated Disconnect Overview on page 27
- Configuring RADIUS-Initiated Dynamic Request Support on page 28
- RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 29
- Error-Cause Codes (RADIUS Attribute 101) for Dynamic Requests on page 36

Dynamic Service Activation During Login Overview

The AAA Service Framework enables the router to dynamically activate subscriber services as part of a subscriber login operation.

The framework sets up the subscriber session and then completes the service action specified by the Juniper Networks VSA 26–65 that is received in the Access-Accept message. If the service request is unsuccessful, the framework logs out the subscriber.

RADIUS-Initiated Change of Authorization (CoA) Overview

The AAA Service Framework uses CoA messages to dynamically modify active subscriber sessions. For example, RADIUS attributes in CoA messages might instruct the framework to create, modify, or terminate a subscriber service.

CoA Messages

Dynamic request support enables the router to receive and process unsolicited CoA messages from external RADIUS servers. RADIUS-initiated CoA messages use the following codes in request and response messages:

- CoA-Request (43)
- CoA-ACK (44)
- CoA-NAK (45)

Qualifications for Change of Authorization

To complete the change of authorization for a user, the CoA-Request must contain the two RADIUS attributes shown in the following list to uniquely identify subscribers. The request must also include the appropriate VSA shown in the following list to perform the required operation. The AAA Service Framework handles the actual request.

- User-Name [attribute 1]
- Acct-Session-ID [attribute 44]
- Activate-Service [VSA 26–65]
- Deactivate-Service [VSA 26–66]



NOTE: If only the User-Name attribute is included in the CoA-Request, the router uses the first match for the username.

Message Exchange

The RADIUS server and the AAA Service Framework on the router exchange messages using UDP. The CoA-Request message sent by the RADIUS server has the same format as the Disconnect-Request packet that is sent for a disconnect operation.

The response is either a CoA-ACK or a CoA-NAK message:

- If the AAA Service Framework successfully changes the authorization, the response is a RADIUS-formatted packet with a CoA-ACK message, and the data filter is applied to the session.
- If AAA Service Framework is unsuccessful, the request is malformed, or attributes are missing, the response is a RADIUS-formatted packet with a CoA-NAK message.



NOTE: The AAA Service Framework processes one dynamic request at a time per subscriber. If the framework receives a second dynamic request (either another CoA or a Disconnect-Request) while processing a previous request for the same subscriber, the framework responds with a CoA-NAK message.

RADIUS-Initiated Disconnect Overview

This section describes the AAA Service Framework's support for RADIUS-initiated disconnect dynamic requests. The AAA Service Framework uses disconnect messages to dynamically terminate active subscriber sessions.

Disconnect Messages

To centrally control the disconnection of remote access subscribers, the RADIUS dynamic request feature on the router receives and processes unsolicited messages from RADIUS servers.

The dynamic request feature uses the existing format of RADIUS disconnect request and response messages. RADIUS-initiated disconnect uses the following codes in its RADIUS request and response messages:

- Disconnect-Request (40)
- Disconnect-ACK (41)
- Disconnect-NAK (42)

Qualifications for Disconnect

For the AAA Service Framework to disconnect a user, the Disconnect-Request message must contain an attribute with an accounting session ID. The Disconnect-Request message can contain an Acct-Session-Id (44) attribute or an Acct-Multi-Session-Id (50) attribute for the session ID or both. If both the Acct-Session-Id and Acct-Multi-Session-Id attributes are present in the request, the router uses both attributes. If the User-Name (1) attribute is also present in the request, the username and accounting session ID are used to perform the disconnection. The AAA Service Framework handles the actual request.

Message Exchange

The RADIUS server and the AAA Service Framework exchange messages using UDP. The Disconnect-Request message sent by the RADIUS server has the same format as the CoA-Request packet that is sent for a change of authorization operation.

The disconnect response is either a Disconnect-ACK or a Disconnect-NAK message:

- If the AAA Service Framework successfully disconnects the user, the response is a RADIUS-formatted packet with a Disconnect-ACK message.

- If the AAA Service Framework cannot disconnect the user, the request is malformed, or attributes are missing from the request, the response is a RADIUS-formatted packet with a Disconnect-NAK message.



NOTE: The AAA Service Framework processes one dynamic request at a time per subscriber. If the framework receives a second dynamic request while processing a previous request (either a CoA or another Disconnect-Request) for the same subscriber, the framework responds with a Disconnect-NAK message.

Configuring RADIUS-Initiated Dynamic Request Support

To configure RADIUS dynamic request support, include the `authentication-server` statement at the `[edit access profile profile-name radius]` hierarchy level. The router uses this list of specified servers for both authentication and dynamic request operations. The router listens on UDP port 3799 for dynamic requests.

```
[edit access profile profile-name radius]
authentication-server [ ip-address ]
```

To configure the router to support dynamic requests from more than one RADIUS server, include multiple *ip-address* entries, for example:

```
authentication-server 192.168.1.3 192.168.10.15;
```

- Related Topics**
- Using RADIUS Dynamic Requests for Subscriber Access Management on page 25
 - Dynamic Service Activation During Login Overview on page 25
 - RADIUS-Initiated Change of Authorization (CoA) Overview on page 26
 - RADIUS-Initiated Disconnect Overview on page 27
 - RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 29
 - Error-Cause Codes (RADIUS Attribute 101) for Dynamic Requests on page 36

Verifying and Managing the RADIUS Dynamic-Request Feature

To display statistics for RADIUS dynamic requests on the router, use the following operational command:

- `show network-access aaa statistics dynamic-requests`

For information about using this operational command, see the *JUNOS System Basics and Services Command Reference*.

RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework

The AAA Service Framework supports RADIUS attributes and vendor-specific attributes (VSAs)—this support provides tunable parameters that the subscriber access management feature uses when creating subscribers and services.

RADIUS attributes are carried as part of standard RADIUS request and reply messages. The subscriber management access feature uses the RADIUS attributes to exchange specific authentication, authorization and accounting information. VSAs allow the subscriber access management feature to pass implementation-specific information that provide extended capabilities, such as service activation or deactivation, and enabling and disabling filters.

The following tables list the RADIUS attributes and Juniper Networks VSAs that the AAA service frameworks supports:

- RADIUS IETF Attributes Supported by the AAA Service Framework on page 29
- Juniper Networks VSAs Supported by the AAA Service Framework on page 32

RADIUS IETF Attributes Supported by the AAA Service Framework

Table 8 on page 29 describes the RADIUS IETF attributes supported by the JUNOS software AAA Service Framework.

Table 8: Supported RADIUS IETF Attributes

Attribute Number	Attribute Name	Description
1	User-Name	<ul style="list-style-type: none"> ■ Name of user to be authenticated ■ Configurable username override
2	User-Password	<ul style="list-style-type: none"> ■ Password of user to be authenticated Password Authentication Protocol (PAP) ■ Configurable password override ■ Password Authentication Protocol (PAP)
4	NAS-IP-Address	IP address of the network access server (NAS) that is requesting authentication of the user
5	NAS-Port	Physical port number of the NAS that is authenticating the user
6	Service-Type	Type of service the user has requested or the type of service to be provided
8	Framed-IP-Address	<ul style="list-style-type: none"> ■ IP address to be configured for the user ■ 0.0.0.0 or absence is interpreted as 255.255.255.254

Table 8: Supported RADIUS IETF Attributes (*continued*)

Attribute Number	Attribute Name	Description
9	Framed-IP-Netmask	<ul style="list-style-type: none"> ■ IP network to be configured for the user when the user is a router to a network ■ Absence implies 255.255.255.255
11	Filter-ID	<ul style="list-style-type: none"> ■ Name of the filter list for the user ■ Interpreted as input policy name
18	Reply-Message	<ul style="list-style-type: none"> ■ Text that may be displayed to the user ■ Only the first instance of this attribute is used
22	Framed-Route	String that provides routing information to be configured for the user on the NAS; in the format: <code><addr>[/<maskLen>] [<nexthop> [<cost>]] (tag <tagValue>) [distance <distValue>]</code>
25	Class	An arbitrary value that the NAS includes in all accounting packets for the user if supplied by the RADIUS server
27	Session-Timeout	Maximum number of consecutive seconds of service to be provided to the user before termination of the session
31	Calling-Station-ID	Allows the NAS to send the phone number from which the call originated
32	NAS-Identifier	Identifies the NAS originating the request
40	Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (Start), the end (Stop), or the interim (Interim-Update)
41	Acct-Delay-Time	Indicates how many seconds the client has been trying to send a particular record
42	Acct-Input-Octets	Indicates how many octets have been received from the port during the time this service has been provided
43	Acct-Output-Octets	Indicates how many octets have been sent to the port during the time this service has been provided
44	Acct-Session-ID	<p>Unique accounting identifier that makes it easy to match start and stop records in a log file. The identifier can be in one of the following formats:</p> <ul style="list-style-type: none"> ■ decimal—For example, 435264 ■ description—In the generic format, <code>jnpr interface-specifier:subscriber-session-id</code>; For example, <code>jnpr fastEthernet 3/2.6:1010101010101</code>
45	Acct-Authentic	Indicates how the user was authenticated: whether by RADIUS, the NAS itself, or another remote authentication protocol

Table 8: Supported RADIUS IETF Attributes *(continued)*

Attribute Number	Attribute Name	Description
46	Acct-Session-Time	Indicates how long in seconds that the user has received service
47	Acct-Input-Packets	Indicates how many packets have been received from the port during the time this service has been provided to a framed user
48	Acct-Output-Packets	Indicates how many packets have been sent to the port in the course of delivering this service to a framed user
49	Acct-Terminate-Cause	<p>Contains the reason the service (a PPP session) was terminated. The service can be terminated for the following reasons:</p> <ul style="list-style-type: none"> ■ User Request (1)—User initiated the disconnect (log out) ■ Idle Timeout (4)—Idle timer has expired ■ Session Timeout (5)—Client reached the maximum continuous time allowed on the service or session ■ Admin Reset (6)—System administrator terminated the session ■ Port Error (8)—PVC failed; no hardware or no interface ■ NAS Error (9)—Negotiation failures, connection failures, or address lease expiration ■ NAS Request (10)—PPP challenge timeout, PPP request timeout, tunnel establishment failure, PPP bundle failure, IP address lease expiration, PPP keep-alive failure, Tunnel disconnect, or an unaccounted-for error
52	Acct-Input-Gigawords	Indicates how many times the Acct-Input-Octets counter has wrapped around 2^{32} during the time this service has been provided. Can be present in Accounting-Request records only where the Acct-Status-Type is set to Stop or Interim-Update
53	Acct-Output-Gigawords	Indicates how many times the Acct-Output-Octets counter has wrapped around 2^{32} in the course of delivering this service. Can be present in Accounting-Request records only where the Acct-Status-Type is set to Stop or Interim-Update
55	Event-Timestamp	Records the time that this event occurred on the NAS, in seconds, since January 1, 1970 00:00 UTC
61	NAS-Port-Type	Indicates the type of physical port the NAS is using to authenticate the user
85	Acct-Interim-Interval	Number of seconds between each interim accounting update for this session
87	NAS-Port-ID	Text string that identifies the physical interface of the NAS that is authenticating the user

Table 8: Supported RADIUS IETF Attributes (*continued*)

Attribute Number	Attribute Name	Description
88	Framed-Pool	Name of an assigned address pool that should be used to assign an address for the user

Juniper Networks VSAs Supported by the AAA Service Framework

Table 9 on page 32 describes Juniper Networks VSAs supported by the JUNOS software AAA Service Framework. The AAA Service Framework uses vendor ID 4874, which is assigned to Juniper Networks by the Internet Assigned Numbers Authority (IANA).

Table 9: Supported Juniper Networks VSAs

Attribute Number	Attribute Name	Description	Value
26-4	Primary-DNS	Client DNS address negotiated during IPCP	integer: 4-byte primary-dns-address
26-5	Secondary-DNS	Client DNS address negotiated during IPCP	integer: 4-byte secondary-dns-address
26-6	Primary-WINS	Client WINS (NBNS) address negotiated during IPCP	integer: 4-byte primary-wins-address
26-7	Secondary-WINS	Client WINS (NBNS) address negotiated during IPCP	integer: 4-byte secondary-wins-address
26-10	Ingress-Policy-Name	Input policy name to apply to client interface	string: input-policy-name
26-11	Egress-Policy-Name	Output policy name to apply to client interface	string: output-policy-name
26-12	Ingress-Statistics	Enable or disable input statistics on client interface	integer: ■ 0 = disable ■ 1 = enable
26-13	Egress-Statistics	Enable or disable output statistics on client interface	integer: ■ 0 = disable ■ 1 = enable
26-23	IGMP-Enable	Enable or disable IGMP on a client interface	integer: ■ 0 = disable ■ 1 = enable

Table 9: Supported Juniper Networks VSAs (continued)

Attribute Number	Attribute Name	Description	Value
26-34	Framed-IP-Route-Tag	Route tag to apply to returned framed-ip-address	integer: 4-octet
26-42	Input-Gigapackets	Number of times input-packets attribute rolls over its 4-octet field	integer
26-43	Output-Gigapackets	Number of times output-packets attribute rolls over its 4-octet field	integer
26-56	DHCP-MAC-Address	Client MAC address	string: mac-address
26-57	DHCP-GI-Address	DHCP relay agent IP address	integer: 4-octet
26-58	LI-Action	Traffic mirroring action	0 = stop mirroring 1 = start mirroring 2 = no action
26-59	Med-Dev-Handle	Link to which traffic mirroring is applied	Salt-encrypted string
26-60	MD-IP-Address	IP address of content destination device to which mirrored traffic is forwarded	Salt-encrypted IP address
26-61	MD-Port-Number	UDP port in the content destination device to which mirrored traffic is forwarded	Salt-encrypted integer
26-63	Interface-Desc	Text string that identifies the subscriber's access interface	string: interface-description
26-65	Activate-Service	Service to activate for the subscriber	string: service-name
26-66	Deactivate-Service	Service to deactivate for the subscriber	string: service-name
26-71	IGMP-Access-Group-Name	Access List to use for the group (G) filter	string: 32-octet

Table 9: Supported Juniper Networks VSAs (continued)

Attribute Number	Attribute Name	Description	Value
26-72	IGMP-Access-Source-Group-Name	Access List to use for the source-group (S,G) filter	string: 32-octet
26-74	MLD-Access-Group-Name	Access List to use for the group (G) filter	string: 32-octet
26-75	MLD-Access-Source-Group-Name	Access List to use for the source-group (S,G) filter	string: 32-octet
26-77	MLD-Version	MLD Protocol Version	integer: 1-octet <ul style="list-style-type: none"> ■ 1 = MLD version ■ 2 = MLD version
26-78	IGMP-Version	IGMP Protocol Version	integer: 1-octet <ul style="list-style-type: none"> ■ 1 = IGMP version ■ 2 = IGMP version ■ 3 = IGMP version
26-83	Acct-Service-Session	Name of the service (including parameter values) that is associated with service manager statistics	string: service-name
26-84	Mobile-IP-Algorithm	Authentication algorithm used for Mobile-IP registration	integer: 4-octet
26-85	Mobile-IP-SPI	Security parameter index number for Mobile IP registration	integer: 4-octet
26-86	Mobile-IP-Key	Security association MD5 key for Mobile IP registration	string: key
26-87	Mobile-IP-Replay	Replay timestamp for Mobile IP registration	integer: 4-octet
26-89	Mobile-IP-Lifetime	Registration lifetime for Mobile IP registration	integer: 4-octet

Table 9: Supported Juniper Networks VSAs *(continued)*

Attribute Number	Attribute Name	Description	Value
26-97	IGMP-Immediate-Leave	IGMP Immediate Leave	integer: 4-octet <ul style="list-style-type: none"> ■ 0 = disable ■ 1 = enable
26-100	MLD-Immediate-Leave	MLD Immediate Leave	integer: 4-octet <ul style="list-style-type: none"> ■ 0 = disable ■ 1 = enable
26-108	CoS-Scheduler-Pmt-Type	Tag (parameter type) value and parameter description: <ul style="list-style-type: none"> ■ 1: CoS scheduler map name ■ 2: CoS shaping rate ■ 3: CoS guaranteed rate ■ 4: CoS delay-buffer rate 	2 parts, delimited by white space: <ul style="list-style-type: none"> ■ Parameter type ■ Parameter value

Table 9: Supported Juniper Networks VSAs (continued)

Attribute Number	Attribute Name	Description	Value
26-146	CoS-Scheduler-Pmt-Type	<p>Tag (parameter type) value and parameter description:</p> <ul style="list-style-type: none"> ■ Null: CoS scheduler name ■ 1: CoS scheduler transmit rate ■ 2: CoS scheduler buffer size ■ 3: CoS scheduler priority ■ 4: CoS scheduler drop-profile low ■ 5: CoS scheduler drop-profile medium-low ■ 6: CoS scheduler drop-profile medium-high ■ 7: CoS scheduler drop-profile high ■ 8: CoS scheduler drop-profile any 	<p>3 parts, delimited by white space:</p> <ul style="list-style-type: none"> ■ Scheduler name ■ Parameter type ■ Parameter value

Error-Cause Codes (RADIUS Attribute 101) for Dynamic Requests

When a RADIUS-initiated CoA or disconnect operation is unsuccessful, the router includes an error-cause attribute (RADIUS attribute 101) in the CoA-NAK or Disconnect-NAK message that it sends back to the RADIUS server. If the detected error does not map to one of the supported error-cause attributes, the router sends the message without an error-cause attribute. Table 10 on page 37 describes the error-cause codes.

Table 10: Error-Cause Codes (RADIUS Attribute 101)

Code	Value	Description
401	Unsupported attribute	The request contains an attribute that is not supported (for example, a third-party attribute).
402	Missing attribute	A critical attribute (for example, the session identification attribute) is missing from a request.
404	Invalid response	Some other aspect of the request is invalid, such as if one or more attributes are not formatted properly.
503	Session context not found	The session context identified in the request does not exist on the router.
504	Session context not removable	The subscriber identified by attributes in the request is owned by a component that is not supported.
506	Resources unavailable	A request could not be honored due to lack of available NAS resources (such as memory).

Attaching Access Profiles

After you have created the access profile that specifies the subscriber access management authentication and accounting parameters, you attach the profile. Subscriber access management supports access profiles attached at the logical system:routing instance level.

```
[edit logical-systems logical-system-name routing-instances routing-instance-name]
access-profile profile-name;
```

For example:

```
[edit logical-systems isp22-bos-metro-12 routing-instances isp22-cmbrg-12-32]
access-profile vz-bos-metro-fios-basic;
```

Verifying and Managing Subscriber Information

To display subscriber access statistics and information, use the following operational commands:

- `show network-access aaa statistics`
- `show network-access aaa subscribers`

To clear subscriber access statistics and to log out specific subscribers, use the following operational command:

- `clear network-access aaa subscribers`

For information about using these operational commands, see the *JUNOS System Basics and Services Command Reference*.

Chapter 4

Configuring Address-Assignment Pools for Subscriber Access

- DHCP and Address Assignment Pools Overview on page 39
- Configuring Address-Assignment Pools on page 39
- DHCP Attributes Table on page 42
- License Requirements for Address-Assignment Pools on page 43
- Tracing Address-Assignment Pool Processes on page 43

DHCP and Address Assignment Pools Overview

The address-assignment pool feature supports subscriber management functionality by enabling you to create address pools that can be shared by different client applications. For example, multiple client applications, such as DHCP, can use an address-assignment pool to provide addresses for their particular clients. Client applications can acquire addresses for either authenticated or unauthenticated clients.

Address-assignment pools support both dynamic and static address assignment. In dynamic address assignment, a client is automatically assigned an address from the address-assignment pool. In static address assignment, you reserve an address that is then always used by a particular client. Addresses that are reserved for static assignment are removed from the dynamic address pool and cannot be assigned to other clients.

Address-assignment pools support named address ranges, which are subsets of the overall address range. A client application can use named ranges to manage address assignment based on client-specific criteria. For example, you might create a named range that is based on a specific DHCP option 82 value. Then, when a DHCP client request matches the specified option 82 value, an address from the specified range is assigned to the client.

Related Topics ■ Configuring Address-Assignment Pools on page 39

Configuring Address-Assignment Pools

The address-assignment pool feature supports subscriber management functionality by enabling you to create address pools that can be shared by different client applications.



NOTE: You cannot use address-assignment pools with the J-series DHCP server. Also, address-assignment pools are completely separate from L2TP address pools, which you create with the **address-pool** statement at the **[edit access]** hierarchy level, and NAT pools, which you create with the **pool** statement at the **[edit services nat]** hierarchy level.

To configure an address-assignment pool, include the **address-assignment** statement at the **[edit access]** hierarchy level. Include the **dhcp-attributes** statement to enable DHCP support and include configuration options in the address lease for the address-assignment pool.

```
[edit access]
address-assignment {
  pool pool-name family inet {
    network address-or-prefix</subnet-mask>;
    range range-name {
      low lower-limit high upper-limit;
    }
    host hostname {
      hardware-address mac-address;
      ip-address ip-address;
    }
    dhcp-attributes {
      [protocol-specific attributes]
    }
  }
}
```

- Configuring an Address-Assignment Pool Name and Network Address on page 40
- Configuring a Named Address Range for Dynamic Address Assignment on page 41
- Configuring Static Address Assignment on page 41
- Configuring DHCP Client-Specific Attributes on page 41

Configuring an Address-Assignment Pool Name and Network Address

To configure an address-assignment pool, include the following mandatory statements at the **[edit access]** hierarchy level:

```
[edit access]
address-assignment {
  pool pool-name family inet {
    network address-or-prefix</subnet-mask>;
  }
}
```

The address-assignment pool definition must include the pool name and the **network** statement. The **network** statement specifies the network address and prefix length for the addresses in the pool.

The following is an example of an address-assignment pool definition:


```
[edit access]
address-assignment {
  pool isp_1 family inet {
    network 192.168.0.0/16;
```

Configuring a Named Address Range for Dynamic Address Assignment

You can optionally configure multiple named subsets of addresses within an address-assignment pool. During dynamic address assignment, a client can be assigned an address from a specific named range. To create a named range, use the `range` statement at the `[edit access address-assignment pool pool-name family inet]` hierarchy level to identify the range and configure the lower and upper address boundaries of the range:

```
range name {
  low lower-limit high upper-limit;
}
```

Configuring Static Address Assignment

You can optionally create a static binding by reserving a specific address for a particular client. When you reserve an address, that address is removed from the address-assignment pool so that it is not assigned to another client. To configure a static address assignment, use the `host` statement at the `[edit access address-assignment pool pool-name family inet]` hierarchy level to identify the client and create a binding between the client MAC address and the assigned IP address:

```
host hostname {
  hardware-address mac-address;
  ip-address ip-address;
}
```

The following is an example of a static binding configuration. This configuration specifies that the client with MAC address 90:00:00:01:00:01 is always assigned IP address 192.168.44.12.

```
host svale6.boston.net {
  hardware-address 90:00:00:01:00:01;
  ip-address 192.168.44.12;
}
```

Configuring DHCP Client-Specific Attributes

Use the address-assignment pool feature to include application-specific attributes when clients obtain an address. The client application, such as DHCP, uses the attributes to determine how addresses are assigned, and to also provide optional application-specific characteristics to the client. For example, the DHCP application might specify that a client that matches certain prerequisite information is dynamically assigned an address from a particular named range. Based on which named range is used, DHCP specifies additional DHCP attributes such as the boot-file that the client uses, the lease grace period, and the maximum lease time.

Use the `dhcp-attributes` statement at the `[edit access address-assignment pool pool-name family inet]` hierarchy level to configure client-specific attributes for DHCP clients. “DHCP Attributes Table” on page 42 describes the DHCP attributes.

```
dhcp-attributes {
  option-match {
    option-82 {
      circuit-id value range named-range;
      remote-id value range named-range;
    }
  }
  boot-file filename;
  boot-server (address | hostname);
  domain-name domain-name;
  grace-period seconds;
  maximum-lease-time seconds;
  name-server [ server-list ];
  netbios-node-type node-type;
  option {
    [ (id-number option-type option-value)
      (id-number array option-type option-value) ];
  }
  router [ router-list ];
  tftp-server address;
  wins-server [ server-list ];
}
```

- Related Topics**
- DHCP Attributes Table on page 42
 - License Requirements for Address-Assignment Pools on page 43
 - Example: Configuring an Address-Assignment Pool on page 117

DHCP Attributes Table

Table 11 on page 42 describes the DHCP client attributes that you can configure for address-assignment pools.

Table 11: DHCP-Attributes Statements

Statement	Description	Corresponding DHCP Option
boot-file	Boot filename advertised to the client, and used by the client to complete configuration.	67
boot-server	Boot server containing the boot file.	66
domain-name	Domain in which clients search for a DHCP server host.	15
grace-period	Grace period offered with the lease.	none
option-match	Maps option 82 value to named address range.	none

Table 11: DHCP-Attributes Statements (*continued*)

Statement	Description	Corresponding DHCP Option
maximum-lease-time	Maximum lease time allowed by the DHCP server.	51
name-server	IP address of domain name server.	6
netbios-node-type	NetBIOS node type.	46
option	User-defined options.	–
router	IP address for routers on the subnetwork.	3
tftp-server	Trivial File Transfer Protocol (TFTP) server that the client uses to obtain the client configuration file.	150
wins-server	IP address of the Windows NetBIOS name server.	44

License Requirements for Address-Assignment Pools

The address-assignment pool feature is part of the JUNOS Subscriber Management Feature Pack license. You must install and properly configure the license to meet the requirements for using the address-assignment pool feature.

For complete information about the JUNOS software licenses, see the “Installing and Managing JUNOS Licenses” chapter of the *JUNOS Software Installation and Upgrade Guide*.

Tracing Address-Assignment Pool Processes

To trace address-assignment pool processes, you can specify flags in the `traceoptions` statement at the `[edit system processes general-authentication-service]` hierarchy level. The default tracing behavior is the following:

- Important events are logged in a file called `authd` located in the `/var/log` directory.
- When the file `authd` reaches 128 kilobytes (KB), it is renamed `authd.0`, then `authd.1`, and so on, until there are 3 trace files. Then the oldest trace file (`authd2`) is overwritten. For more information about how log files are created, see the JUNOS System Log Messages Reference.
- Log files can be accessed only by the user who configures the tracing operation.

You cannot change the directory (`/var/log`) in which trace files are located. However, you can customize the other trace file settings by including the following statements at the `[edit system processes general-authentication-service]` hierarchy level:

```
[edit system processes general-authentication-service]
traceoptions {
  file filename {
    files number;
    size maximum-file-size;
```



```

        world-readable | no-world-readable;
        match regex;
    }
    flag address-assignment;
    flag all;
    flag configuration;
    flag framework;
    flag ldap;
    flag local-authentication;
    flag radius;
}

```

These options are described in the following sections:

- Configuring the Address-Assignment Pool Trace Log Filename on page 44
- Configuring the Number and Size of Address-Assignment Pool Processes Log Files on page 44
- Configuring Access to the Log File on page 45
- Configuring a Regular Expression for Lines to Be Logged on page 45
- Configuring the Trace Operation on page 45

Configuring the Address-Assignment Pool Trace Log Filename

By default, the name of the file that records trace output for address-assignment pools is `authd`. You can specify a different name by including the `file` statement at the `[edit system processes general-authentication-service]` hierarchy level:

```

[edit system processes general-authentication-service traceoptions]
file filename;

```

Configuring the Number and Size of Address-Assignment Pool Processes Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed `filename.0`, then `filename.1`, and so on, until there are 3 trace files. Then the oldest trace file (`filename.2`) is overwritten.

You can configure the limits on the number and size of trace files by including the following statement at the `[edit system processes general-authentication-service traceoptions]` hierarchy level:

```

[edit system processes general-authentication-service traceoptions]
file files number size size;

```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (`filename`) reaches 2 MB, `filename` is renamed `filename.0`, and a new file called `filename` is created. When the new `filename` reaches 2 MB, `filename.0` is renamed `filename.1` and `filename` is renamed `filename.0`. This process repeats until there are 20 trace files. Then the oldest file (`filename.19`) is overwritten by the newest file (`filename.0`).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10 KB through 1 gigabyte (GB).

Configuring Access to the Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the `file world-readable` statement at the `[edit system processes general-authentication-service traceoptions]` hierarchy level:

```
[edit system processes general-authentication-service traceoptions]
file world-readable;
```

To explicitly set the default behavior, include the `file no-world-readable` statement at the `[edit system processes general-authentication-service traceoptions]` hierarchy level:

```
[edit system processes general-authentication-service traceoptions]
file no-world-readable;
```

Configuring a Regular Expression for Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events.

You can refine the output by including the `match` statement at the `[edit system processes general-authentication-service file filename]` hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit system processes general-authentication-service traceoptions]
file filename match regex;
```

Configuring the Trace Operation

By default, only important events are logged. You can configure the trace operations to be logged by including the following statements at the `[edit system processes general-authentication-service traceoptions]` hierarchy level:

```
[edit system processes general-authentication-service traceoptions]
flag {
  address-assignment;
  all;
  configuration;
  framework;
  ldap;
  local-authentication;
  radius;
}
```

You can specify the following access tracing flags:

- `address-assignment`—All address-assignment events
- `all`—All tracing operations
- `configuration`—Configuration events
- `framework`—Authentication framework events

- `ldap`—LDAP authentication events `local-authentication`
- `local-authentication`—Local authentication events
- `radius`—RADIUS authentication events

Chapter 5

Configuring DHCP Local Server for Subscriber Access

- Extended DHCP Local Server Overview on page 48
- Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview on page 52
- Using External AAA Authentication Services with DHCP on page 53
- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool To Use on page 54
- Grouping Interfaces with Common DHCP Configurations on page 55
- Group-Specific DHCP Local Server Options on page 56
- Overriding Default DHCP Local Server Configuration Settings on page 56
- DHCP Auto Logout Overview on page 59
- Automatically Logging Out DHCP Clients on page 61
- Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 62
- Configuring Passwords for Usernames on page 63
- Creating Unique Usernames for DHCP Clients on page 64
- Verifying and Managing DHCP Local Server Configuration on page 66
- Tracing Extended DHCP Operations on page 66

Extended DHCP Local Server Overview

You can enable the router to function as an extended DHCP local server and configure the extended DHCP local server options on the router. The extended DHCP local server provides an IP address and other configuration information in response to a client request.

The extended DHCP local server enhances traditional DHCP server operation in which the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in centralized address-assignment pools, which are managed independently of the DHCP local server and which can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients. See “Configuring Address-Assignment Pools” on page 39 for details about creating and using address-assignment pools.



NOTE: The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

You cannot configure the extended DHCP local server and extended DHCP relay on the same interface.

To configure the extended DHCP local server on the router, you include the `dhcp-local-server` statement at the `[edit system services]` hierarchy level. See the “[edit system services dhcp-local-server] Hierarchy Level” on page 497 for the complete DHCP local server syntax.

You can also include the `dhcp-local-server` statement at the following hierarchy levels:

- `[edit logical-systems logical-system-name system services]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name system services]`
- `[edit routing-instances routing-instance-name system services]`

This overview covers:

- Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools on page 49
- Providing DHCP Client Configuration Information on page 49
- Minimal Configuration for Clients on page 50
- DHCP Local Server and Address-Assignment Pools on page 51

Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools

In a typical carrier edge network configuration, the DHCP client is on the subscriber's computer, and the DHCP local server is configured on the router. The following steps provide a high-level description of the interaction among the DHCP local server, DHCP client, and address-assignment pools:

1. The DHCP client sends a discover packet to one or more DHCP local servers in the network to obtain configuration parameters and an IP address for the subscriber.
2. Each DHCP local server that receives the discover packet then searches its address-assignment pool for the client address and configuration options. Each local server creates an entry in its internal client table to keep track of the client state, then sends a DHCP offer packet to the client.
3. On receipt of the offer packet, the DHCP client selects the DHCP local server from which to obtain configuration information and sends a request packet indicating the DHCP local server that will grant the address and configuration information.
4. The selected DHCP local server sends an acknowledgement packet to the client that contains the client address lease and configuration parameters. The server also installs the host route and ARP entry, and then monitors the lease state.

Providing DHCP Client Configuration Information

When the extended DHCP application receives a response from an external authentication server, the response might include information in addition to the IP address and subnet mask. The extended DHCP application uses the information from the authentication grant for the response the DHCP application sends to the DHCP client. The DHCP application can either send the information in its original form or the application might merge the information with local configuration specifications. For example, if the authentication grant includes an address pool name and a local configuration specifies DHCP attributes for that pool, the extended DHCP application merges the authentication results and the attributes in the reply that the server sends to the client.

A local configuration is optional — a client can be fully configured by the external authentication service. However, if the external authentication service does not provide client configuration, you must configure the local address-assignment pool to provide the configuration for the client. When a local configuration specifies options, the extended DHCP application adds the local configuration options to the offer PDU the server sends to the client. If the two sets of options overlap, the options in the authentication response from the external service take precedence.

When you use RADIUS to provide the authentication, the additional information might be in the form of RADIUS attributes and Juniper Networks VSAs. The following table shows the information that RADIUS might include in the authentication grant. See “RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework” on page 29 for a complete list of RADIUS attributes and Juniper Networks VSAs that the extended DHCP applications supports for subscriber access management.

Attribute Number	Attribute Name	Description
RADIUS attribute 8	Framed-IP-Address	Client IP address
RADIUS attribute 9	Framed-IP-Netmask	Subnet mask for client IP address (DHCP option 1)
Juniper Networks VSA 26-4	Primary-DNS	Primary domain server (DHCP option 6)
Juniper Networks VSA 26-5	Secondary-DNS	Secondary domain server (DHCP option 6)
Juniper Networks VSA 26-6	Primary-WINS	Primary WINS server (DHCP option 44)
Juniper Networks VSA 26-7	Secondary-WINS	Secondary WINS server (DHCP option 44)
RADIUS attribute 88	Framed-Pool	Address assignment pool name
RADIUS attribute 27	Session-Timeout	Lease time
Juniper Networks VSA 26-109	DHCP-Guided-Relay-Server	DHCP relay server

Minimal Configuration for Clients

The extended DHCP local server provides a minimal configuration to the DHCP client if the client does not have DHCP option 55 configured. The server provides the subnet mask of the address-assignment pool that is selected for the client. In addition to the subnet mask, the server provides the following values to the client if the information is configured in the selected address-assignment pool:

- **router**—A router located on the client’s subnet. This statement is the equivalent of DHCP option 3.
- **domain name**—The name of the domain in which the client searches for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. This is equivalent to DHCP option 15.
- **domain name server**—A Domain Name System (DNS) name server that is available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.

DHCP Local Server and Address-Assignment Pools

The extended DHCP local server enhances traditional DHCP server operation in which the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in centralized address-assignment pools, which are managed independently of the DHCP local server and which can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients.



NOTE: The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

- | | |
|-----------------------|---|
| Related Topics | <ul style="list-style-type: none"> ■ Configuring Address-Assignment Pools on page 39 ■ Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool To Use on page 54 ■ Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview on page 52 ■ Using External AAA Authentication Services with DHCP on page 53 ■ Tracing Extended DHCP Operations on page 66 ■ Verifying and Managing DHCP Local Server Configuration on page 66 ■ Example: Minimum Extended DHCP Local Server Configuration on page 118 ■ Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 118 |
|-----------------------|---|

Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview

The router's DHCP support enables you to attach a dynamic profile to a DHCP subscriber interface. When a DHCP subscriber logs in, the router instantiates the specified dynamic profile and then applies the services defined in the profile to the interface.

You can attach dynamic profiles to all interfaces or you can specify a particular group of interfaces to which the profile is attached. Both the DHCP local server and the DHCP relay agent support the attachment of dynamic profiles to interfaces.

You can enable the following optional features when the dynamic profile is attached. The two options cannot be used together.

- Enable multiple DHCP subscribers to share the same VLAN logical interface. The firewall filters, CoS schedulers, and IGMP configuration of the clients are merged.
- Specify the primary dynamic profile that is instantiated when the first subscriber logs in.

Multiple DHCP Subscribers Sharing the Same VLAN Logical Interface

The `aggregate-clients` option specifies that the router merge the firewall filters, CoS schedulers, and IGMP configuration of multiple DHCP clients that are on the same VLAN logical interface (for example, multiple clients belonging to the same household). You can configure the `aggregate-clients` support for all interfaces or for a group of interfaces.

By default, the feature is disabled and a single DHCP client is allowed per VLAN when a dynamic profile is associated with the VLAN logical interface.

The router merges the software components for multiple subscribers as follows:

- Firewall filters—The filters are chained together using the precedence as the order of execution. If the same firewall filter is attached multiple times, the filter is executed only once.
- CoS schedulers—The different CoS schedulers are merged as if the scheduler map has multiple schedulers. The merge operation for the individual traffic-control-profiles parameters (shaping-rate, delay-buffer-rate, guaranteed-rate) preserves the maximum value for each parameter.
- IGMP configuration—The current IGMP configuration is replaced with the configuration of the newest DHCP client.



NOTE: You cannot use a dynamic demux interface to represent multiple subscribers in a dynamic profile attached to an interface. One dynamic demux interface represents one subscriber. Do not configure the `aggregate-clients` option when attaching a dynamic profile to a demux interface for DHCP.

Primary Dynamic Profile

The `use-primary` option enables you to specify the primary dynamic profile that is instantiated when the first subscriber logs in. Subsequent subscribers are not assigned the primary dynamic profile; instead, they are assigned the dynamic profile specified for the interface. When the first subscriber logs out, the next subscriber that logs in is assigned the primary dynamic profile.

This feature can conserve logical interfaces in a network where dynamic demux interfaces are used to represent subscribers. To conserve interfaces, the primary profile that you specify should not be a profile that creates a demux interface but one that provides the initial policies for the primary interface subscriber.

Related Topics ■ Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 62

Using External AAA Authentication Services with DHCP

Both the extended DHCP local server and the extended DHCP relay agent support the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients. When the extended DHCP local server or relay agent receives a discover PDU from a client, the extended DHCP application contacts the AAA server to authenticate the DHCP client. The extended DHCP application can obtain client addresses and DHCP configuration options from the external AAA authentication server.



NOTE: This section uses the term extended DHCP application to refer to both the extended DHCP local server and the extended DHCP relay agent.

The external authentication feature also supports AAA directed logout. If the external AAA service supports a user logout directive, the extended DHCP application honors the logout and views it as if it was requested by a CLI management command. All of the client state information and allocated resources are deleted at logout. The extended DHCP application supports directed logout using the list of configured authentication servers you specify with the `authentication-server` statement at the `[edit access profile profile-name]` hierarchy level.

You can configure either global authentication support or group-specific support.

You must configure the `username-include` statement to enable the use of authentication. The `password` statement is not required and does not cause DHCP to use authentication if the `username-include` statement is not included.

To configure DHCP local server and DHCP relay agent authentication support:

1. Specify that you want to configure authentication options.
 - For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# edit authentication
```


- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# edit authentication
```

2. (Optional) Configure a password that authenticates the username to the external authentication service.

See “Configuring Passwords for Usernames” on page 63.

3. (Optional) Configure optional features to create a unique username.

See “Creating Unique Usernames for DHCP Clients” on page 64.

- Related Topics**
- Extended DHCP Local Server Overview on page 48
 - Extended DHCP Relay Agent Overview on page 72

Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool To Use

You can specify the method that the extended DHCP local server uses to determine which address-assignment pool provides the IP address and configuration for a DHCP client.

By default, the server selects the address-assignment pool to use by matching the IP address in the client DHCP request with the network address of the address-assignment pool. If the client request contains the gateway IP address (giaddr), the local server matches the giaddr to the address-assignment pool’s address. If there is no giaddr in the request, then the DHCP local server matches the IP address of the receiving interface to the address of the address-assignment pool.

You can optionally configure the extended DHCP local server to match the DHCP relay agent information option (option 82) in the client DHCP packets to a named range in the address-assignment pool used for the client. Named ranges are subsets within the overall address-assignment pool address range, and are configured when you create the address-assignment pool.



NOTE: To use the DHCP local server option 82 matching feature, you must ensure that the **option-82** statement is included in the **dhcp-attributes** statement for the address-assignment pool.

To configure the extended DHCP local server to match the DHCP relay agent information option (option 82) in the client DHCP packets to a named range in the address-assignment pool used for the client:

1. Access the **pool-match-order** configuration.

```
[edit system services dhcp-local-server]
user@host# edit pool-match-order
```


2. Specify the default pool matching method. You must configure the default method before configuring the optional Option 82 matching method.

```
[edit system services dhcp-local-server pool-match-order]
user@host# set ip-address-first
```

3. Specify the Option 82 matching method.

```
[edit system services dhcp-local-server pool-match-order]
user@host# set option-82
```

- Related Topics**
- Configuring Address-Assignment Pools on page 39
 - Extended DHCP Local Server Overview on page 48
 - Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 118

Grouping Interfaces with Common DHCP Configurations

You use the group feature to group together a set of interfaces and then apply a common DHCP configuration to the named interface group. The extended DHCP local server and DHCP relay agent both support interface groups.

To configure an interface group:

1. Access the [edit system services dhcp-local-server] hierarchy (for DHCP local server) or the [edit forwarding-options dhcp-relay] hierarchy (for DHCP relay agent), depending on the extended DHCP access method you want to configure. The following steps create a DHCP local server group; the steps are the same for DHCP relay agent.

2. Create the group and assign a name.

```
[edit system services dhcp-local-server]
user@host# edit group boston
```

3. Specify the names of one or more interfaces on which the extended DHCP application is enabled. You can repeat the **interface interface-name** statement to specify multiple interfaces within the group, but you cannot use the same interface in more than one group.

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.1
user@host# set interface fe-1/0/1.2
```

4. (Optional) You can use the *upto* option to specify a range of interfaces for a group.

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.3 upto fe-1/0/1.9
```

5. (Optional) You can use the **exclude** option to exclude a specific interface or a specified range of interfaces from the group. For example:

```
[edit system services dhcp-local-server group boston]
```



```

user@host# interface fe-1/0/1.1 upto fe-1/0/1.102
user@host# interface fe-1/0/1.6 exclude
user@host# interface fe-1/0/1.70 upto fe-1/0/1.80 exclude

```

- Related Topics**
- Extended DHCP Local Server Overview on page 48
 - Extended DHCP Relay Agent Overview on page 72
 - Group-Specific DHCP Local Server Options on page 56
 - Group-Specific DHCP Relay Options on page 78

Group-Specific DHCP Local Server Options

You can include the following statements at both the [edit system services dhcp-local-server group *group-name*] hierarchy level to set group-specific DHCP local server configuration options, and at the [edit system services dhcp-local-server] hierarchy level to set global DHCP local server configuration options:

- **authentication**—Configure the parameters the router sends to the external AAA server.
- **dynamic-profile**—Specify the dynamic profile that is attached to a group of interfaces.
- **interface**—Specify one or more interfaces, or a range of interfaces, that are within the specified group.
- **overrides**—Override the default configuration settings for the extended DHCP local server. For information, see “Overriding Default DHCP Local Server Configuration Settings” on page 56.

The statements configured at the [edit system services dhcp-local-server group *group-name*] hierarchy level apply only to the named group of interfaces, and override any global DHCP local server settings configured with the same statements at the [edit system services dhcp-local-server] hierarchy level.

- Related Topics**
- Grouping Interfaces with Common DHCP Configurations on page 55

Overriding Default DHCP Local Server Configuration Settings

You can override certain default DHCP local server configuration settings. You can override the settings at the global level and for a named group of interfaces.

To override global default DHCP local server configuration options, include the **overrides** statement and its subordinate statements at the [edit system services dhcp-local-server] hierarchy level. To override DHCP local server configuration options for a named group of interfaces, include the statements at the [edit system services dhcp-local-server group *group-name*] hierarchy level.

To remove all DHCP local server configuration overrides at a particular hierarchy level, include the **overrides** statement without any subordinate statements.

To override default DHCP local server configuration settings:

1. Specify that you want to configure override options.

```
[edit system services dhcp-local-server]
user@host# edit overrides
```

2. (Optional) Override the maximum number of DHCP clients allowed per interface.

See “Specifying the Maximum Number of DHCP Clients Per Interface” on page 57.

3. (Optional) Override ARP table population in distrusted environments.

See “Disabling ARP Table Population” on page 58.

4. (Optional) Configure DHCP client auto logout.

See “DHCP Auto Logout Overview” on page 59.

This topic contains the following sections:

- Specifying the Maximum Number of DHCP Clients Per Interface on page 57
- Disabling ARP Table Population on page 58

Specifying the Maximum Number of DHCP Clients Per Interface

By default, there is no limit to the number of DHCP local server or DHCP relay clients allowed on an interface. However, you can override the default setting and specify the maximum number of clients allowed per interface, in the range 1 to 500,000. When the number of clients on the interface reaches the specified limit, no additional DHCP Discover PDUs are accepted. When the number of clients subsequently drops below the limit, new clients are again accepted.



NOTE: The maximum number of DHCP local server clients or DHCP relay clients can also be specified by Juniper Networks VSA 26-143 during client login. The VSA-specified value always takes precedence if the interface-client-limit number statement specifies a different number.

If the VSA-specified value differs with each client login, DHCP uses the largest limit set by the VSA until there are no clients on the interface.

To configure the maximum number of DHCP clients allowed per interface:

1. Specify that you want to configure override options.

- For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# edit overrides
```

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
```



```
user@host# edit overrides
```

2. Configure the maximum number of clients allowed per interface. (DHCP local server and DHCP relay agent both support the `interface-client-limit` statement.)

```
[edit system services dhcp-local-server overrides]
user@host# set interface-client-limit number
```

Disabling ARP Table Population

By default, DHCP populates the ARP table with the MAC address of a client when the client binding is established. However, you may choose to use the DHCP `no-arp` statement to hide the subscriber MAC address information, as it appears in ARP table entries.

When running in a trusted environment (that is, when not using the `no-arp` statement), DHCP populates the ARP table with unique MAC addresses contained within the DHCP PDU for each DHCP client:

Table 12: ARP Table in Trusted Environment

IP Address	MAC Address
Client 1 IP Address	MAC A
Client 2 IP Address	MAC B
Client 3 IP Address	MAC C

In distrusted environments, you can specify the `no-arp` statement to hide the MAC addresses of clients. When you specify the `no-arp` statement, DHCP does not automatically populate the ARP table with MAC address information from the DHCP PDU for each client. Instead, the system performs an ARP to obtain the MAC address of each client and obtains the MAC address of the immediately-attached device (for example, a DSLAM). DHCP populates the ARP table with the same interface MAC address (for example, MAC X from a DSLAM interface) for each client:

Table 13: ARP Table in Distrusted Environment

IP Address	MAC Address
Client 1 IP Address	MAC X
Client 2 IP Address	MAC X
Client 3 IP Address	MAC X

To disable ARP table population:

1. Specify that you want to configure override options.

- For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# edit overrides
```

- For DHCP relay:

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Disable ARP table population with client-specific information. (DHCP local server and DHCP relay agent both support the **no-arp** statement.)

- For DHCP local server:

```
[edit system services dhcp-local-server overrides]
user@host# set no-arp
```

- For DHCP relay:

```
[edit forwarding-options dhcp-relay overrides]
user@host# set no-arp
```

DHCP Auto Logout Overview

This topic provides an introduction to the optional DHCP auto logout feature and includes the following sections:

- Auto Logout Overview on page 59
- How DHCP Identifies and Releases Clients on page 60
- Option 60 and Option 82 Requirements on page 60

Auto Logout Overview

Auto logout is an optional configuration for DHCP local server and DHCP relay agent that improves the efficiency of DHCP IP address assignment. Auto logout enables IP addresses to be immediately released and returned to the address pool when the addresses are no longer used by DHCP clients. DHCP can then assign the addresses to other clients. Without auto logout, an IP address is blocked for the entire lease period, and DHCP must wait until the address lease time expires before reusing the address.

Auto logout is particularly useful when DHCP uses long lease times for IP address assignments and to help avoid allocating duplicate IP addresses for a single client. For example, you might have an environment that includes set-top boxes (STB) that are often upgraded or replaced. Each time a STB is changed, the new STB repeats the DHCP discover process to obtain client configuration information and an IP address. DHCP views the new STB as a completely new client and assigns a new IP address—the previous IP address assigned to the client (the old STB) remains blocked and unavailable until the lease expires. If auto logout is configured in this situation, DHCP recognizes that the new STB is actually the same client and then immediately

releases the original IP address. DHCP relay agent acts as a proxy client for auto logout and sends a DHCP release message to the DHCP server.

How DHCP Identifies and Releases Clients

The auto logout feature requires that DHCP explicitly identify clients. By default, DHCP local server and DHCP relay agent identify clients based on MAC address or Client Identifier. However, in some cases this type of identification might not be sufficient. For example, in the previous STB example, each STB has a different MAC address, so DHCP incorrectly assumes that an upgraded or replacement STB is a new client.

In order to explicitly identify clients, auto logout uses a secondary identification method when the primary identification method is unsuccessful—the primary method is considered unsuccessful if the MAC address or Client Identifier does not match that of an existing client. The secondary identification method is based on the DHCP option 60 and option 82 information in DHCP discover messages.

Both the primary and secondary identification methods use subnet information to differentiate between clients. The primary identification method differentiates between two clients with the same MAC address (or same Client Identifier) if the clients are on different subnets. Similarly, the secondary identification method considers two clients as different if they have the same option 60 and option 82 information, but different subnets.

DHCP local server and DHCP relay agent perform the following operations when auto logout is enabled and the secondary identification method identifies a duplicate client (that is, the discovery packet is from an existing client).

- DHCP local server immediately releases the existing address.
- DHCP relay agent immediately releases the existing client and then sends a DHCP release packet to the DHCP server. Sending the release packet ensures that DHCP relay and the DHCP server are synchronized.



NOTE: If the DHCP relay agent is in snoop mode, DHCP relay releases the client but does not send a release packet to the DHCP server if the discover packet is for a passive client (a client added as a result of snooped packets) or if the discover packet is a snooped packet.

Option 60 and Option 82 Requirements

DHCP local server requires that the received discover packet include both DHCP option 60 and option 82. If either option is missing, DHCP local server cannot perform the secondary identification method and auto logout is not used.

DHCP relay agent requires that the received discover packet contain DHCP option 60. DHCP relay determines the option 82 value based on the guidelines provided in “DHCP Relay Agent Option 82 Value for Auto Logout” on page 85.

Related Topics ■ Automatically Logging Out DHCP Clients on page 61

- DHCP Relay Agent Option 82 Value for Auto Logout on page 85

Automatically Logging Out DHCP Clients

You can configure the extended DHCP local server and extended DHCP relay to automatically log out DHCP clients. Auto logout immediately releases an existing client when DHCP receives a discover packet that has the same DHCP option 60 and DHCP option 82 information as the existing client. DHCP then releases the existing client IP address without waiting for the normal lease expiration.



NOTE: When the existing client is released, the new client undergoes the normal authentication process. The new client might not receive the same IP address as the original client.

To configure DHCP client auto logout:

1. Specify that you want to configure override options.
 - For DHCP local server:


```
[edit system services dhcp-local-server]
user@host# edit overrides
```
 - For DHCP relay agent:


```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```
2. Enable auto logout. (DHCP local server and DHCP relay agent both support the `client-discover-match` statement.)
 - For DHCP local server:


```
[edit system services dhcp-local-server overrides]
user@host# client-discover-match
```
 - For DHCP relay:


```
[edit forwarding-options dhcp-relay overrides]
user@host# client-discover-match
```



NOTE: If you change the auto logout configuration, existing clients continue to use the auto logout setting that was configured when they logged in. New clients use the new setting.

Related Topics

- DHCP Auto Logout Overview on page 59
- Extended DHCP Local Server Overview on page 48
- Extended DHCP Relay Agent Overview on page 72

Attaching Dynamic Profiles to DHCP Subscriber Interfaces

This topic describes how to attach a dynamic profile to a DHCP subscriber interface. When a DHCP subscriber logs in, the specified dynamic profile is instantiated and the services defined in the profile are applied to the interface.

This topic contains the following sections:

- Attaching a Dynamic Profile to All DHCP Subscriber Interfaces on page 62
- Attaching a Dynamic Profile to a Group of DHCP Subscriber Interfaces on page 63

Attaching a Dynamic Profile to All DHCP Subscriber Interfaces

To attach a dynamic profile to all DHCP subscriber interfaces:

1. At the DHCP configuration hierarchy, use the **dynamic-profile** statement to specify the name of the dynamic profile to attach to all interfaces.

- For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# set dynamic-profile vod-profile-22
```

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# set dynamic-profile vod-profile-west
```

2. Optionally, you can configure the attribute to use when attaching the specified profile.

You can include either the **aggregate-clients** option to enable multiple DHCP subscribers to share the same VLAN logical interface, or the **use-primary** option to specify that the primary dynamic profile is used. The two options are mutually exclusive.

- To enable multiple subscribers to share the same VLAN logical interface:

```
[edit system services dhcp-local-server dynamic-profile]
user@host# set aggregate-clients
```

- To use the primary dynamic profile:

```
[edit forwarding-options dhcp-relay dynamic-profile]
user@host# set use-primary subscriber_profile
```


Attaching a Dynamic Profile to a Group of DHCP Subscriber Interfaces

To attach a dynamic profile to a group of interfaces:

Before you begin:

- Configure the interface group.

See “Grouping Interfaces with Common DHCP Configurations” on page 55.

1. At the DHCP configuration hierarchy, specify the name of the interface group and the dynamic profile to attach to the group.

- For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# set group boston dynamic-profile vod-profile-42
```

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# set group quebec dynamic-profile vod-profile-east
```

2. Optionally, you can configure the attribute to use when attaching the specified profile.

You can include either the **aggregate-clients** option to enable multiple DHCP subscribers to share the same VLAN logical interface, or the **use-primary** option to specify that the primary dynamic profile is used. The two options are mutually exclusive.

- To enable multiple subscribers to share the same VLAN logical interface:

```
[edit system services dhcp-local-server dynamic-profile]
user@host# set aggregate-clients
```

- To use the primary dynamic profile:

```
[edit forwarding-options dhcp-relay dynamic-profile]
user@host# set use-primary subscriber_profile
```

Related Topics

- Dynamic Profiles Overview on page 275
- Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview on page 52
- Example: Configuring Dynamic Subscriber Interfaces on IP Demux Interfaces on page 320

Configuring Passwords for Usernames

You can configure an optional password that the extended DHCP application presents to the external AAA authentication service to authenticate the specified username.

To configure a password that authenticates the username:

1. Specify that you want to configure authentication options.

- For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# edit authentication
```

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# edit authentication
```

2. Configure the password. (DHCP local server and DHCP relay agent both support the **password** statement.)

```
[edit system services dhcp-local-server authentication]
user@host# set password myPassword1234
```

- Related Topics**
- Extended DHCP Local Server Overview on page 48
 - Extended DHCP Relay Agent Overview on page 72
 - Using External AAA Authentication Services with DHCP on page 53
 - For information about supported characters in passwords, see “Configuring Special Requirements for Plain-Text Passwords” in the *JUNOS System Basics Configuration Guide*

Creating Unique Usernames for DHCP Clients

You can configure the extended DHCP application to include additional information in the username that is passed to the external AAA authentication service when the DHCP client logs in. This additional information enables you to construct usernames that uniquely identify subscribers.



NOTE: If you do not include a username in the authentication configuration, the router does not perform authentication; however, the IP address is provided by the local pool if it is configured.

The following list describes the optional information that you can include as part of the username:

- **circuit-type**—The circuit type used by the DHCP client, for example **enet**.
- **delimiter**—The delimiter character that separates components that make up the concatenated username. The default delimiter is a period (.). The semicolon (;) is not supported as a delimiter character.
- **domain-name**—The client domain name as string. The router adds the **@** delimiter to the username.

- **logical-system-name**—The name of the logical system, if the receiving interface is in a logical system.
- **mac-address**—The client MAC address, in a string of the format xxxx.xxxx.xxxx.
- **option-60**—The portion of the option 60 payload that follows the length field.
- **option-82 <circuit-id> <remote-id>;** —The specified contents of the option 82 payload.
 - **circuit-id**—The payload of the Agent Circuit ID suboption.
 - **remote-id**—The payload of the Agent Remote ID suboption.
 - Both **circuit-id** and **remote-id**—The payloads of both suboptions, in the format: **circuit-id[delimiter]remote-id**.
 - Neither **circuit-id** or **remote-id**—The raw payload of the option 82 from the PDU is concatenated to the username.
- **routing-instance-name**—The name of the routing instance, if the receiving interface is in a routing instance.
- **user-prefix**—A string indicating the user prefix.

The router creates the unique username by including the specified additional information in the following order, with the fields separated by a delimiter.

```
user-prefix[delimiter]mac-address[delimiter]logical-system-name[delimiter]
routing-instance-name[delimiter]circuit-type[delimiter]option-82[delimiter]
option-60@domain-name
```

To configure a unique username:

1. Specify that you want to configure authentication.
 - For DHCP local server:


```
[edit system services dhcp-local-server]
user@host# edit authentication
```
 - For DHCP relay agent:


```
[edit forwarding-options dhcp-relay]
user@host# edit authentication
```
2. Specify that you want to include optional information in the username. (DHCP local server and DHCP relay agent both support the **username-include** statement.)


```
[edit system services dhcp-local-server authentication]
user@host# set username-include
```
3. (Optional) Specify the optional information you want to include in the username.


```
[edit system services dhcp-local-server authentication username-include]
user@host# set username-include circuit-type
user@host# set username-include domain-name isp55.com
user@host# set username-include mac-address
```



```
user@host# set username-include user-prefix wallybrown
```

The previous `username-include` configuration produces this unique username:

```
wallybrown.0090.1a01.1234.enet@isp55.com
```

- Related Topics**
- Extended DHCP Local Server Overview on page 48
 - Extended DHCP Relay Agent Overview on page 72
 - Using External AAA Authentication Services with DHCP on page 53

Verifying and Managing DHCP Local Server Configuration

Purpose View or clear information about client address bindings and statistics for the extended DHCP local server.

Action

- To display the address bindings in the client table on the extended DHCP local server:

```
user@host> show dhcp server binding
```

- To display extended DHCP local server statistics:

```
user@host> show dhcp server statistics
```

- To clear the binding state of a DHCP client from the client table on the extended DHCP local server:

```
user@host> clear dhcp server binding
```

- To clear all extended DHCP local server statistics:

```
user@host> clear dhcp server statistics
```

- Related Topics**
- For more information, see the *JUNOS System Basics and Services Command Reference*

Tracing Extended DHCP Operations

Both the extended DHCP local server and the extended DHCP relay agent support tracing operations. DHCP tracing operations track extended DHCP operations and record them in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

- Important events are logged in a file called `jdhcpd` located in the `/var/log` directory. You cannot change the directory (`/var/log`) in which trace files are located.

- When the file `jdhcpd` reaches 128 kilobytes (KB), it is renamed `jdhcpd.0`, then `jdhcpd.1`, and so on, until there are three trace files. Then the oldest trace file (`jdhcpd.2`) is overwritten.

You can optionally configure the maximum file size to be from 10 KB through 1 gigabyte (GB). You can also specify the number of trace files to be from 2 through 1000. (For more information about how log files are created, see the *JUNOS System Log Messages Reference*.)

- Log files can be accessed only by the user who configures the tracing operation.

To configure DHCP local server and DHCP relay agent tracing operations:

1. Specify that you want to configure tracing options.

- For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# edit traceoptions
```

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# edit traceoptions
```

2. (Optional) Configure the name for the file used for the trace output.

See “Configuring the Extended DHCP Log Filename” on page 68.

3. (Optional) Configure the number and size of the log files.

See “Configuring the Number and Size of Extended DHCP Log Files” on page 68.

4. (Optional) Configure access to the log file.

See “Configuring Access to the Extended DHCP Log File” on page 68.

5. (Optional) Configure a regular expression to filter logging events.

See “Configuring a Regular Expression for Extended DHCP Lines to Be Logged” on page 69.

6. (Optional) Configure flags to filter the operations to be logged.

See “Configuring the Extended DHCP Tracing Flags” on page 69.

The extended DHCP traceoptions operations are described in the following sections:

- Configuring the Extended DHCP Log Filename on page 68
- Configuring the Number and Size of Extended DHCP Log Files on page 68
- Configuring Access to the Extended DHCP Log File on page 68
- Configuring a Regular Expression for Extended DHCP Lines to Be Logged on page 69
- Configuring the Extended DHCP Tracing Flags on page 69

Configuring the Extended DHCP Log Filename

By default, the name of the file that records trace output is `jdhcpd`. You can specify a different name by including the `file` option:

To configure the filename for DHCP local server and DHCP relay agent tracing operations:

- Specify the name of the file used for the trace output. (DHCP local server and DHCP relay agent both support the `file` option for the `traceoptions` statement.)

```
[edit system services dhcp-local-server traceoptions]
user@host# set file dhcp_logfile_1
```

Configuring the Number and Size of Extended DHCP Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed `filename.0`, then `filename.1`, and so on, until there are three trace files. Then the oldest trace file (`filename.2`) is overwritten.

You can optionally configure the maximum file size to be from 10 KB through 1 gigabyte (GB). You can also specify the number of trace files to be from 2 through 1000.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (`filename`) reaches 2 MB, `filename` is renamed `filename.0`, and a new file called `filename` is created. When the new `filename` reaches 2 MB, `filename.0` is renamed `filename.1` and `filename` is renamed `filename.0`. This process repeats until there are 20 trace files. Then the oldest file (`filename.19`) is overwritten by the newest file (`filename.0`).

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output. (DHCP local server and DHCP relay agent both support the `files` and `size` options for the `traceoptions` statement.)

```
[edit system services dhcp-local-server traceoptions]
user@host# set file dhcp_logfile_1 files 20 size 2097152
```

Configuring Access to the Extended DHCP Log File

By default, log files can be accessed only by the user who configures the tracing operation. You can enable all users to read the log file and you can explicitly set the default behavior of the log file.

To specify that all users can read the log file:

- Configure the log file to be world-readable. (DHCP local server and DHCP relay agent both support the `world-readable` option for the `traceoptions` statement.)

```
[edit system services dhcp-local-server traceoptions]
```



```
user@host# set file dhcp_logfile_1 world-readable
```

To explicitly set the default behavior, in which the log file can only be read by the user who configured tracing:

- Configure the log file to be no-world-readable. (DHCP local server and DHCP relay agent both support the `no-world-readable` option for the `traceoptions` statement.)

```
[edit system services dhcp-local-server traceoptions]
user@host# set file dhcp_logfile_1 no-world-readable
```

Configuring a Regular Expression for Extended DHCP Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events.

You can refine the output by including regular expressions that will be matched.

To configure regular expressions to be matched:

- Configure the regular expression. (DHCP local server and DHCP relay agent both support the `match` option for the `traceoptions` statement.)

```
[edit system services dhcp-local-server traceoptions]
user@host# set file dhcp_logfile_1 match regex
```

Configuring the Extended DHCP Tracing Flags

By default, only important events are logged. You can specify which trace operations are logged by including specific tracing flags. The following table describes the flags that you can include.

Flag	Description
all	Trace all events
auth	Trace authentication events
database	Trace database events
fwd	Trace firewall process events
general	Trace miscellaneous events
ha	Trace high availability-related events
interface	Trace interface operations
io	Trace I/O operations
packet	Trace packet decoding operations
packet-option	Trace DHCP option decoding operations

Flag	Description
rpdp	Trace routing protocol process events
rtstock	Trace routing socket operations
session-db	Trace session database events
state	Trace changes in state
ui	Trace user interface operations

To configure the flags for the events to be logged:

- Configure the flags. (DHCP local server and DHCP relay agent both support the **flag** option for the **traceoptions** statement.)

```
[edit system services dhcp-local-server traceoptions]
```

```
user@host# set flag packet-option
```


Chapter 6

Configuring DHCP Relay for Subscriber Access

- Extended DHCP Relay Agent Overview on page 72
- Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview on page 75
- Using External AAA Authentication Services with DHCP on page 76
- Grouping Interfaces with Common DHCP Configurations on page 77
- Group-Specific DHCP Relay Options on page 78
- Overriding the Default DHCP Relay Configuration on page 79
- DHCP Auto Logout Overview on page 84
- DHCP Relay Agent Option 82 Value for Auto Logout on page 85
- Automatically Logging Out DHCP Clients on page 86
- Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 87
- Enabling and Disabling Insertion of Option 82 Information on page 91
- Configuring Server Groups on page 94
- Configuring Active Server Groups on page 95
- Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 95
- Verifying and Managing DHCP Relay Configuration on page 97
- Tracing Extended DHCP Operations on page 97

Extended DHCP Relay Agent Overview

You can configure extended DHCP relay options on the router and enable the router to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server. You can use DHCP relay in carrier edge applications such as video/IPTV to obtain configuration parameters, including an IP address, for your subscribers.

For more information about how to use the DHCP relay agent in a video/IPTV application, see the *JUNOS Feature Guide*.



NOTE: The extended DHCP relay agent options configured with the `dhcp-relay` statement are incompatible with the DHCP/BOOTP relay agent options configured with the `bootp` statement. As a result, you cannot enable both the extended DHCP relay agent and the DHCP/BOOTP relay agent on the router at the same time.

For information about the DHCP/BOOTP relay agent, see the *JUNOS Policy Framework Configuration Guide*.

To configure the extended DHCP relay agent on the router, include the `dhcp-relay` statement at the `[edit forwarding-options]` hierarchy level. See the “[edit forwarding-options dhcp-relay] Hierarchy Level” on page 494 for the complete DHCP relay agent syntax.

You can also include the `dhcp-relay` statement at the following hierarchy levels:

- `[edit logical-systems logical-system-name forwarding-options]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options]`
- `[edit routing-instances routing-instance-name forwarding-options]`

This overview covers:

- Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers on page 72
- Access and Access-Internal Routes on page 73
- DHCP State Persistence on page 74
- Graceful Routing Engine Switchover on page 74

Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers

In a typical carrier edge network configuration, the DHCP client is on the subscriber’s computer, and the DHCP relay agent is configured on the router between the DHCP client and one or more DHCP servers.

The following steps describe, at a high level, how the DHCP client, DHCP relay agent, and DHCP server interact in a configuration that includes two DHCP servers.

1. The DHCP client sends a discover packet to find a DHCP server in the network from which to obtain configuration parameters for the subscriber, including an IP address.
2. The DHCP relay agent receives the discover packet and forwards copies to each of the two DHCP servers. The DHCP relay agent then creates an entry in its internal client table to keep track of the client's state.
3. In response to receiving the discover packet, each DHCP server sends an offer packet to the client. The DHCP relay agent receives the offer packets and forwards them to the DHCP client.
4. On receipt of the offer packets, the DHCP client selects the DHCP server from which to obtain configuration information. Typically, the client selects the server that offers the longest lease time on the IP address.
5. The DHCP client sends a request packet that specifies the DHCP server from which to obtain configuration information.
6. The DHCP relay agent receives the request packet and forwards copies to each of the two DHCP servers.
7. The DHCP server requested by the client sends an acknowledgement (ACK) packet that contains the client's configuration parameters.
8. The DHCP relay agent receives the ACK packet and forwards it to the client.
9. The DHCP client receives the ACK packet and stores the configuration information.
10. If configured to do so, the DHCP relay agent installs a host route and Address Resolution Protocol (ARP) entry for this client.
11. After establishing the initial lease on the IP address, the DHCP client and the DHCP server use unicast transmission to negotiate lease renewal or release. The DHCP relay agent "snoops" on all of the packets unicast between the client and the server that pass through the router to determine when the lease for this client has expired or been released. This process is referred to as lease shadowing or passive snooping.

Access and Access-Internal Routes

The DHCP application on a video services router uses both access routes and access-internal routes to represent either the end users or the networks behind the attached router. An access route represents a network behind an attached video services router, and is set to a preference of 13. An access-internal route is a /32 route that represents a directly attached end user, and is set to a preference of 12.

To configure import and export of access routes and access-internal routes in a routing policy, include the **access** and **access-internal** keywords as match conditions at the [edit policy-options policy-statement *policy-name* term *term-name* from protocol] hierarchy level. For information, see the *JUNOS Policy Framework Configuration Guide*.

To display configuration information for access routes and access-internal routes, use the **show route extensive**, **show route protocol access**, and **show route protocol**

`access-internal` operational commands. For command syntax and examples, see the *JUNOS Routing Protocols and Policies Command Reference*.

DHCP State Persistence

The extended DHCP relay agent maintains the state of active DHCP client leases in persistent storage on the router. It can recover this state if the DHCP relay agent process fails or is manually restarted, or if you manually reboot (gracefully shut down) the router. DHCP state persistence prevents the loss of active DHCP clients in either of these circumstances. If a power failure occurs or if the kernel stops operating on a single Routing Engine, however, the state of active DHCP client leases is lost.

DHCP state persistence is automatically enabled when you configure the extended DHCP relay agent on the router by including the `dhcp-relay` statement.

The DHCP relay agent records in persistent storage only those DHCP clients that are fully bound, which means that they currently have an active lease on an IP address from a DHCP server. DHCP clients in a renewal or rebind state are considered to be fully bound, and their state is also maintained in persistent storage. When a DHCP client lease expires or the client is released, the DHCP relay agent removes the client state from persistent storage.

Graceful Routing Engine Switchover

The extended DHCP relay agent supports graceful Routing Engine switchover on all routing platforms that contain dual Routing Engines. To support graceful Routing Engine switchover, the DHCP relay agent automatically mirrors (replicates) information about the state of bound DHCP clients from the master Routing Engine to the backup Routing Engine.

To enable graceful Routing Engine switchover support for the extended DHCP relay agent, include the `graceful-switchover` statement at the `[edit chassis redundancy]` hierarchy level. You cannot disable graceful Routing Engine switchover support for the extended DHCP relay agent when the router is configured to support graceful Routing Engine switchover.

For more information about using graceful Routing Engine switchover, see the *JUNOS High Availability Configuration Guide*.

- Related Topics**
- Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview on page 52
 - Using External AAA Authentication Services with DHCP on page 53
 - Verifying and Managing DHCP Relay Configuration on page 97
 - Tracing Extended DHCP Operations on page 66
 - Example: Minimum DHCP Relay Agent Configuration on page 118
 - Example: DHCP Relay Agent Configuration with Multiple Clients and Servers on page 119
 - Example: Using Option 60 Strings to Forward DHCP Client Traffic on page 120
 - Example: Using Option 60 Strings to Drop DHCP Client Traffic on page 121

Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview

The router's DHCP support enables you to attach a dynamic profile to a DHCP subscriber interface. When a DHCP subscriber logs in, the router instantiates the specified dynamic profile and then applies the services defined in the profile to the interface.

You can attach dynamic profiles to all interfaces or you can specify a particular group of interfaces to which the profile is attached. Both the DHCP local server and the DHCP relay agent support the attachment of dynamic profiles to interfaces.

You can enable the following optional features when the dynamic profile is attached. The two options cannot be used together.

- Enable multiple DHCP subscribers to share the same VLAN logical interface. The firewall filters, CoS schedulers, and IGMP configuration of the clients are merged.
- Specify the primary dynamic profile that is instantiated when the first subscriber logs in.

Multiple DHCP Subscribers Sharing the Same VLAN Logical Interface

The `aggregate-clients` option specifies that the router merge the firewall filters, CoS schedulers, and IGMP configuration of multiple DHCP clients that are on the same VLAN logical interface (for example, multiple clients belonging to the same household). You can configure the `aggregate-clients` support for all interfaces or for a group of interfaces.

By default, the feature is disabled and a single DHCP client is allowed per VLAN when a dynamic profile is associated with the VLAN logical interface.

The router merges the software components for multiple subscribers as follows:

- Firewall filters—The filters are chained together using the precedence as the order of execution. If the same firewall filter is attached multiple times, the filter is executed only once.
- CoS schedulers—The different CoS schedulers are merged as if the scheduler map has multiple schedulers. The merge operation for the individual traffic-control-profiles parameters (shaping-rate, delay-buffer-rate, guaranteed-rate) preserves the maximum value for each parameter.
- IGMP configuration—The current IGMP configuration is replaced with the configuration of the newest DHCP client.



NOTE: You cannot use a dynamic demux interface to represent multiple subscribers in a dynamic profile attached to an interface. One dynamic demux interface represents one subscriber. Do not configure the `aggregate-clients` option when attaching a dynamic profile to a demux interface for DHCP.

Primary Dynamic Profile

The `use-primary` option enables you to specify the primary dynamic profile that is instantiated when the first subscriber logs in. Subsequent subscribers are not assigned the primary dynamic profile; instead, they are assigned the dynamic profile specified for the interface. When the first subscriber logs out, the next subscriber that logs in is assigned the primary dynamic profile.

This feature can conserve logical interfaces in a network where dynamic demux interfaces are used to represent subscribers. To conserve interfaces, the primary profile that you specify should not be a profile that creates a demux interface but one that provides the initial policies for the primary interface subscriber.

Related Topics ■ Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 62

Using External AAA Authentication Services with DHCP

Both the extended DHCP local server and the extended DHCP relay agent support the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients. When the extended DHCP local server or relay agent receives a discover PDU from a client, the extended DHCP application contacts the AAA server to authenticate the DHCP client. The extended DHCP application can obtain client addresses and DHCP configuration options from the external AAA authentication server.



NOTE: This section uses the term extended DHCP application to refer to both the extended DHCP local server and the extended DHCP relay agent.

The external authentication feature also supports AAA directed logout. If the external AAA service supports a user logout directive, the extended DHCP application honors the logout and views it as if it was requested by a CLI management command. All of the client state information and allocated resources are deleted at logout. The extended DHCP application supports directed logout using the list of configured authentication servers you specify with the `authentication-server` statement at the `[edit access profile profile-name]` hierarchy level.

You can configure either global authentication support or group-specific support.

You must configure the `username-include` statement to enable the use of authentication. The `password` statement is not required and does not cause DHCP to use authentication if the `username-include` statement is not included.

To configure DHCP local server and DHCP relay agent authentication support:

1. Specify that you want to configure authentication options.
 - For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# edit authentication
```


- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# edit authentication
```

2. (Optional) Configure a password that authenticates the username to the external authentication service.

See “Configuring Passwords for Usernames” on page 63.

3. (Optional) Configure optional features to create a unique username.

See “Creating Unique Usernames for DHCP Clients” on page 64.

- Related Topics**
- Extended DHCP Local Server Overview on page 48
 - Extended DHCP Relay Agent Overview on page 72

Grouping Interfaces with Common DHCP Configurations

You use the group feature to group together a set of interfaces and then apply a common DHCP configuration to the named interface group. The extended DHCP local server and DHCP relay agent both support interface groups.

To configure an interface group:

1. Access the [edit system services dhcp-local-server] hierarchy (for DHCP local server) or the [edit forwarding-options dhcp-relay] hierarchy (for DHCP relay agent), depending on the extended DHCP access method you want to configure. The following steps create a DHCP local server group; the steps are the same for DHCP relay agent.

2. Create the group and assign a name.

```
[edit system services dhcp-local-server]
user@host# edit group boston
```

3. Specify the names of one or more interfaces on which the extended DHCP application is enabled. You can repeat the **interface interface-name** statement to specify multiple interfaces within the group, but you cannot use the same interface in more than one group.

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.1
user@host# set interface fe-1/0/1.2
```

4. (Optional) You can use the **upto** option to specify a range of interfaces for a group.

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.3 upto fe-1/0/1.9
```

5. (Optional) You can use the **exclude** option to exclude a specific interface or a specified range of interfaces from the group. For example:

```
[edit system services dhcp-local-server group boston]
```



```

user@host# interface fe-1/0/1.1 upto fe-1/0/1.102
user@host# interface fe-1/0/1.6 exclude
user@host# interface fe-1/0/1.70 upto fe-1/0/1.80 exclude

```

- Related Topics**
- Extended DHCP Local Server Overview on page 48
 - Extended DHCP Relay Agent Overview on page 72
 - Group-Specific DHCP Local Server Options on page 56
 - Group-Specific DHCP Relay Options on page 78

Group-Specific DHCP Relay Options

You can include the following statements at both the `[edit forwarding-options dhcp-relay group group-name]` hierarchy level to set group-specific DHCP relay agent configuration options, and at the `[edit forwarding-options dhcp-relay]` hierarchy level to set global DHCP relay agent configuration options:

- **active-server-group**—Configure an active server group to apply a common DHCP relay agent configuration to a named group of DHCP server addresses. For information, see “Configuring Active Server Groups” on page 95.
- **authentication**—Configure the parameters the router sends to the external AAA server.
- **dynamic-profile**—Specify the dynamic profile that is attached to a group of interfaces.
- **interface**—Specify one or more interfaces, or a range of interfaces, that are within the specified group.
- **overrides**—Override the default configuration settings for the extended DHCP relay agent. For information, see “Overriding the Default DHCP Relay Configuration” on page 79.
- **relay-option-60**—Use the DHCP vendor class identifier option (option 60) in DHCP client packets to select a DHCP server to which to forward packets. For more information, see “Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers” on page 87.
- **relay-option-82**—Enable or disable the insertion of option 82 information in packets destined for a DHCP server. For information, see “Enabling and Disabling Insertion of Option 82 Information” on page 91.

The statements configured at the `[edit forwarding-options dhcp-relay group group-name]` hierarchy level apply only to the named group of interfaces, and override any global DHCP relay agent settings configured with the same statements at the `[edit forwarding-options dhcp-relay]` hierarchy level.

Related Topics ■ Grouping Interfaces with Common DHCP Configurations on page 55

Overriding the Default DHCP Relay Configuration

You can override certain default DHCP relay agent configuration settings. You can override the settings at the global level and for a named group of interfaces.

To override global default DHCP relay agent configuration options, include the **overrides** statement and its subordinate statements at the `[edit forwarding-options dhcp-relay]` hierarchy level. To override DHCP local server configuration options for a named group of interfaces, include the statements at the `[edit forwarding-options dhcp-relay group group-name]` hierarchy level.

To remove all DHCP relay agent configuration overrides at a particular hierarchy level, include the **overrides** statement without any subordinate statements.

To override default DHCP relay agent configuration settings:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. (Optional) Overwrite the giaddr in DHCP packets the DHCP relay agent forwards.

See “Overwriting giaddr Information” on page 80.

3. (Optional) Override the DHCP relay agent information option (option 82) in DHCP packets.

See “Overriding Option 82 Information” on page 80.

4. (Optional) Override the setting of the broadcast bit in DHCP request packets and use the Layer 2 unicast transmission method.

See “Using Layer 2 Unicast Transmission for DHCP Packets” on page 81.

5. (Optional) Trust DHCP client packets that have a giaddr of 0 and that contain option 82 information.

See “Trusting Option 82 Information” on page 81.

6. (Optional) Override ARP table population in distrusted environments.

See “Disabling ARP Table Population” on page 58.

7. (Optional) Override the maximum number of DHCP clients allowed per interface.

See “Specifying the Maximum Number of DHCP Clients Per Interface” on page 57.

8. (Optional) Configure client auto logout.

See “DHCP Auto Logout Overview” on page 59.

9. (Optional) Disable DHCP relay agent on specific interfaces.

See “Disabling DHCP Relay” on page 83.

This topic contains the following sections:

- Overwriting giaddr Information on page 80
- Overriding Option 82 Information on page 80
- Using Layer 2 Unicast Transmission for DHCP Packets on page 81
- Trusting Option 82 Information on page 81
- Disabling ARP Table Population on page 81
- Specifying the Maximum Number of DHCP Clients Per Interface on page 83
- Disabling DHCP Relay on page 83

Overwriting giaddr Information

You can configure the DHCP relay agent to change the gateway IP address (giaddr) field in packets that it forwards between a DHCP client and a DHCP server.

To overwrite the giaddr of every DHCP packet with the giaddr of the DHCP relay agent before forwarding the packet to the DHCP server:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that the giaddr of DHCP packets is overwritten.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set always-write-giaddr
```

Overriding Option 82 Information

You can configure the DHCP relay agent to add or remove the DHCP relay agent information option (option 82) in DHCP packets.

This feature causes the DHCP relay agent to perform one of the following actions, depending on the configuration:

- If the DHCP relay agent is configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the DHCP packets and inserts the new values before forwarding the packets to the DHCP server.
- If the DHCP relay agent is not configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the packets, but does not add any new values before forwarding the packets to the DHCP server.

To override the default option 82 information in DHCP packets destined for a DHCP server:

1. Specify that you want to configure override options.


```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that the option 82 information in DHCP packets is overwritten.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set always-write-option-82
```

Using Layer 2 Unicast Transmission for DHCP Packets

You can configure the DHCP relay agent to override the setting of the broadcast bit in DHCP request packets. DHCP relay agent then instead uses the Layer 2 unicast transmission method to send DHCP Offer reply packets and DHCP ACK reply packets from the DHCP server to DHCP clients during the discovery process.

To override the default setting of the broadcast bit in DHCP request packets:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that the DHCP relay agent uses the Layer 2 unicast transmission method.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set layer2-unicast-replies
```

Trusting Option 82 Information

By default, the DHCP relay agent treats client packets with a giaddr of 0 (zero) and option 82 information as if the packets originated at an untrusted source, and drops them without further processing. You can override this behavior and specify that the DHCP relay agent process DHCP client packets that have a giaddr of 0 (zero) and contain option 82 information.

To configure DHCP relay agent to trust option 82 information:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that the DHCP relay agent process DHCP client packets with a giaddr of 0 and that contain option 82 information.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set trust-option-82
```

Disabling ARP Table Population

By default, DHCP populates the ARP table with the MAC address of a client when the client binding is established. However, you may choose to use the DHCP **no-arp**

statement to hide the subscriber MAC address information, as it appears in ARP table entries.

When running in a trusted environment (that is, when not using the **no-arp** statement), DHCP populates the ARP table with unique MAC addresses contained within the DHCP PDU for each DHCP client:

Table 14: ARP Table in Trusted Environment

IP Address	MAC Address
Client 1 IP Address	MAC A
Client 2 IP Address	MAC B
Client 3 IP Address	MAC C

In distrusted environments, you can specify the **no-arp** statement to hide the MAC addresses of clients. When you specify the **no-arp** statement, DHCP does not automatically populate the ARP table with MAC address information from the DHCP PDU for each client. Instead, the system performs an ARP to obtain the MAC address of each client and obtains the MAC address of the immediately-attached device (for example, a DSLAM). DHCP populates the ARP table with the same interface MAC address (for example, MAC X from a DSLAM interface) for each client:

Table 15: ARP Table in Distrusted Environment

IP Address	MAC Address
Client 1 IP Address	MAC X
Client 2 IP Address	MAC X
Client 3 IP Address	MAC X

To disable ARP table population:

- Specify that you want to configure override options.
 - For DHCP local server:


```
[edit system services dhcp-local-server]
user@host# edit overrides
```
 - For DHCP relay:


```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```
- Disable ARP table population with client-specific information. (DHCP local server and DHCP relay agent both support the **no-arp** statement.)
 - For DHCP local server:


```
[edit system services dhcp-local-server overrides]
user@host# set no-arp
```

- For DHCP relay:

```
[edit forwarding-options dhcp-relay overrides]
user@host# set no-arp
```

Specifying the Maximum Number of DHCP Clients Per Interface

By default, there is no limit to the number of DHCP local server or DHCP relay clients allowed on an interface. However, you can override the default setting and specify the maximum number of clients allowed per interface, in the range 1 to 500,000. When the number of clients on the interface reaches the specified limit, no additional DHCP Discover PDUs are accepted. When the number of clients subsequently drops below the limit, new clients are again accepted.



NOTE: The maximum number of DHCP local server clients or DHCP relay clients can also be specified by Juniper Networks VSA 26-143 during client login. The VSA-specified value always takes precedence if the interface-client-limit number statement specifies a different number.

If the VSA-specified value differs with each client login, DHCP uses the largest limit set by the VSA until there are no clients on the interface.

To configure the maximum number of DHCP clients allowed per interface:

1. Specify that you want to configure override options.

- For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# edit overrides
```

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Configure the maximum number of clients allowed per interface. (DHCP local server and DHCP relay agent both support the interface-client-limit statement.)

```
[edit system services dhcp-local-server overrides]
user@host# set interface-client-limit number
```

Disabling DHCP Relay

You can disable DHCP relay on all interfaces or a group of interfaces.

To disable DHCP relay agent:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Disable the DHCP relay agent.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set disable-relay
```

DHCP Auto Logout Overview

This topic provides an introduction to the optional DHCP auto logout feature and includes the following sections:

- Auto Logout Overview on page 84
- How DHCP Identifies and Releases Clients on page 84
- Option 60 and Option 82 Requirements on page 85

Auto Logout Overview

Auto logout is an optional configuration for DHCP local server and DHCP relay agent that improves the efficiency of DHCP IP address assignment. Auto logout enables IP addresses to be immediately released and returned to the address pool when the addresses are no longer used by DHCP clients. DHCP can then assign the addresses to other clients. Without auto logout, an IP address is blocked for the entire lease period, and DHCP must wait until the address lease time expires before reusing the address.

Auto logout is particularly useful when DHCP uses long lease times for IP address assignments and to help avoid allocating duplicate IP addresses for a single client. For example, you might have an environment that includes set-top boxes (STB) that are often upgraded or replaced. Each time a STB is changed, the new STB repeats the DHCP discover process to obtain client configuration information and an IP address. DHCP views the new STB as a completely new client and assigns a new IP address—the previous IP address assigned to the client (the old STB) remains blocked and unavailable until the lease expires. If auto logout is configured in this situation, DHCP recognizes that the new STB is actually the same client and then immediately releases the original IP address. DHCP relay agent acts as a proxy client for auto logout and sends a DHCP release message to the DHCP server.

How DHCP Identifies and Releases Clients

The auto logout feature requires that DHCP explicitly identify clients. By default, DHCP local server and DHCP relay agent identify clients based on MAC address or Client Identifier. However, in some cases this type of identification might not be sufficient. For example, in the previous STB example, each STB has a different MAC address, so DHCP incorrectly assumes that an upgraded or replacement STB is a new client.

In order to explicitly identify clients, auto logout uses a secondary identification method when the primary identification method is unsuccessful—the primary method is considered unsuccessful if the MAC address or Client Identifier does not match that of an existing client. The secondary identification method is based on the DHCP option 60 and option 82 information in DHCP discover messages.

Both the primary and secondary identification methods use subnet information to differentiate between clients. The primary identification method differentiates between two clients with the same MAC address (or same Client Identifier) if the clients are on different subnets. Similarly, the secondary identification method considers two clients as different if they have the same option 60 and option 82 information, but different subnets.

DHCP local server and DHCP relay agent perform the following operations when auto logout is enabled and the secondary identification method identifies a duplicate client (that is, the discovery packet is from an existing client).

- DHCP local server immediately releases the existing address.
- DHCP relay agent immediately releases the existing client and then sends a DHCP release packet to the DHCP server. Sending the release packet ensures that DHCP relay and the DHCP server are synchronized.



NOTE: If the DHCP relay agent is in snoop mode, DHCP relay releases the client but does not send a release packet to the DHCP server if the discover packet is for a passive client (a client added as a result of snooped packets) or if the discover packet is a snooped packet.

Option 60 and Option 82 Requirements

DHCP local server requires that the received discover packet include both DHCP option 60 and option 82. If either option is missing, DHCP local server cannot perform the secondary identification method and auto logout is not used.

DHCP relay agent requires that the received discover packet contain DHCP option 60. DHCP relay determines the option 82 value based on the guidelines provided in “DHCP Relay Agent Option 82 Value for Auto Logout” on page 85.

- Related Topics**
- Automatically Logging Out DHCP Clients on page 61
 - DHCP Relay Agent Option 82 Value for Auto Logout on page 85

DHCP Relay Agent Option 82 Value for Auto Logout

Table 16 on page 86 indicates how the DHCP relay agent determines the option 82 value used for the client auto logout feature. Depending on the configuration settings, DHCP relay agent takes the action indicated in the right column.

Table 16: DHCP Relay Agent Option 82 Value for Auto Logout

DHCP Relay Agent Configuration Settings					Action Taken
DHCP Relay Configured with Option 82	Discover Packet Contains Option 82	Override "trust-option-82"	Override "always-write-option-82"	giaddr in non-snooped packet	
No	No	–	–	–	No secondary search performed
No	Yes	Yes	–	–	Use option 82 from packet
No	Yes	No	–	Zero	Drop packet
No	Yes	No	–	Non-zero	Use option 82 from packet
Yes	No	–	–	–	Use configured option 82
Yes	Yes	No	–	Zero	Drop packet
Yes	Yes	No	No	Non-zero	Use option 82 from packet
Yes	Yes	No	Yes	Non-zero	Overwrite the configured option 82
Yes	Yes	Yes	No	–	Use option 82 from packet
Yes	Yes	Yes	Yes	–	Overwrite the configured option 82

- Related Topics**
- DHCP Auto Logout Overview on page 59
 - Automatically Logging Out DHCP Clients on page 61

Automatically Logging Out DHCP Clients

You can configure the extended DHCP local server and extended DHCP relay to automatically log out DHCP clients. Auto logout immediately releases an existing client when DHCP receives a discover packet that has the same DHCP option 60 and DHCP option 82 information as the existing client. DHCP then releases the existing client IP address without waiting for the normal lease expiration.



NOTE: When the existing client is released, the new client undergoes the normal authentication process. The new client might not receive the same IP address as the original client.

To configure DHCP client auto logout:

1. Specify that you want to configure override options.

- For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# edit overrides
```

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Enable auto logout. (DHCP local server and DHCP relay agent both support the `client-discover-match` statement.)

- For DHCP local server:

```
[edit system services dhcp-local-server overrides]
user@host# client-discover-match
```

- For DHCP relay:

```
[edit forwarding-options dhcp-relay overrides]
user@host# client-discover-match
```



NOTE: If you change the auto logout configuration, existing clients continue to use the auto logout setting that was configured when they logged in. New clients use the new setting.

Related Topics

- DHCP Auto Logout Overview on page 59
- Extended DHCP Local Server Overview on page 48
- Extended DHCP Relay Agent Overview on page 72

Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers

You can configure the extended DHCP relay agent to use the DHCP vendor class identifier option (option 60) in DHCP client packets to forward client traffic to specific DHCP servers. This feature is useful in network environments where DHCP clients access services provided by multiple vendors and DHCP servers. For example, a DHCP client might gain Internet access from a particular DHCP server provided by one vendor, and access IPTV service from a different DHCP server provided by

another vendor. The option 60 string enables vendors to include vendor-specific information in DHCP client packets.

You can configure option 60 support globally or for a named group of interfaces. You can also configure option 60 support for the extended DHCP relay agent on a per logical system and per routing instance basis.

To configure the DHCP relay agent to use option 60 vendor-specific information to select a DHCP server to which to forward the client packets:

1. Specify that you want to configure option 60 support.

```
[edit forwarding-options dhcp-relay]
user@host# edit relay-option-60
```

2. (Optional) Configure the DHCP relay to use matching option 60 strings to process client traffic.

See “Using Matching Option 60 Strings to Process DHCP Client Traffic” on page 88.

3. (Optional) Configure the DHCP relay to use nonmatching option 60 strings to process client traffic.

See “Using Nonmatching Option 60 Strings to Process DHCP Client Traffic” on page 91.

This topic includes the following sections:

- Using Matching Option 60 Strings to Process DHCP Client Traffic on page 88
- Using Nonmatching Option 60 Strings to Process DHCP Client Traffic on page 91
- Displaying a Count of Discarded DHCP Packets with Option 60 Information on page 91

Using Matching Option 60 Strings to Process DHCP Client Traffic

Configuring option 60 support helps you manage multivendor networks by enabling the extended DHCP relay agent to compare option 60 vendor-specific strings received in DHCP client packets against a list of ASCII or hexadecimal strings that you configure on the router.

You can configure exact match or partial match criteria for option 60 string-to-DHCP server mapping and specify either the **ascii** statement (to define a nonempty ASCII match string of 1 through 255 alphanumeric characters) or the **hexadecimal** statement (to define a hexadecimal match string of 1 through 255 hexadecimal characters [0 through 9, a through f, A through F]).

When you configure a partial match, the option 60 string can contain a superset of the configured ASCII or hexadecimal string, provided that the leftmost characters of the option 60 string entirely match the characters in the configured match string. For a partial match, the longest match rule applies. For example, the extended DHCP relay agent matches the string “test123” before it matches the string “test”.

If the option 60 string received in the DHCP client packet matches the configured ASCII or hexadecimal string, you can define one of the following actions for the associated DHCP client packets:

- Relay client traffic to a group of specific DHCP relay servers that provide the requested client service.

The DHCP client packet is relayed to all of the servers in the specified group that map to the vendor class identifier information provided in the option 60 string. To configure the named group of DHCP relay servers, which are also referred to as vendor-option servers, include the **server-group** statement at the **[edit forwarding-options dhcp-relay]** hierarchy level, as described in “Configuring Server Groups” on page 94.

The following additional considerations apply when you configure an ASCII or hexadecimal match string:

- You can configure the same ASCII or hexadecimal match string as both an exact (**equals**) match and as a partial (**starts-with**) match. In that case, the exact string match configured with the **equals** statement takes precedence over the partial string match configured with the **starts-with** statement.
- A server group can contain multiple server addresses and can map to more than one match string.
- You can configure an unlimited number of match strings.
- The use of wildcard attributes in match strings is not supported.
- Forward client traffic to a specific extended DHCP local server.
- Drop (discard) the packets. Specifying that certain DHCP client packets be dropped can be useful when DHCP clients request services that are invalid or no longer supported.

1. To configure match criteria:

- To specify an exact, left-to-right match of the configured match string with the option 60 string, use the **vendor-option equals** statement:

- To specify a nonempty ASCII match string.

```
[edit forwarding-options dhcp-relay relay-option-60]
user@host# set vendor-option equals ascii video55
```

- To specify a hexadecimal match string.

```
[edit forwarding-options dhcp-relay relay-option-60]
user@host# set vendor-option equals hexadecimal ff
```

- To specify a partial match of the configured match string with the option 60 string, use the **vendor-option starts-with** statement:

- To specify a partial ASCII match string.

```
[edit forwarding-options dhcp-relay relay-option-60]
user@host# set vendor-option starts-with ascii video
```


- To specify a partial hexadecimal match string.

```
[edit forwarding-options dhcp-relay relay-option-60]
user@host# set vendor-option starts-with hexadecimal ff
```

2. To configure the action to take when the DHCP client packet matches the configured ASCII or hexadecimal string:

- To relay client traffic to a group of specific DHCP relay servers that provide the requested client service.

```
[edit forwarding-options dhcp-relay relay-option-60 vendor-option equals ascii
video55]
user@host# set relay-server-group
```

The DHCP client packet is relayed to all of the servers specified in the **server-group** statement at the [edit forwarding-options dhcp-relay] hierarchy level that map to the vendor class identifier information provided in the option 60 string.

- To forward client traffic to a specific extended DHCP local server.

```
[edit forwarding-options dhcp-relay relay-option-60 vendor-option equals ascii
video55]
user@host# set local-server-group
```

To configure an extended DHCP local server, include the **dhcp-local-server** statement at the [edit system services] hierarchy level. For information about configuring and using the extended DHCP local server, see [Configuring the Extended DHCP Local Server](#).

- To drop (discard) the packets:

```
[edit forwarding-options dhcp-relay relay-option-60 vendor-option equals ascii
video55]
user@host# set drop
```

For configuration examples that illustrate how to use matching option 60 strings to forward or drop DHCP client traffic, see “Example: Using Option 60 Strings to Forward DHCP Client Traffic” on page 120 and “Example: Using Option 60 Strings to Drop DHCP Client Traffic” on page 121.

Using Nonmatching Option 60 Strings to Process DHCP Client Traffic

If the option 60 string received in the DHCP client packet does not match the configured ASCII or hexadecimal string, you can specify the default action that the DHCP relay agent uses for the associated DHCP client packets.

In rare instances, the extended DHCP relay agent might receive a DHCP client packet with an option 60 string of zero (0) length. In this case, there is nothing in the option 60 string against which to match. As a result, such packets are treated as if they contained nonmatching option 60 strings; that is, they can be relayed to a default DHCP relay server, forwarded to a default DHCP extended local server, or dropped.

- To relay client traffic to a default extended DHCP relay server that you specify:

```
[edit forwarding-options dhcp-relay relay-option-60 vendor-option]
user@host# set default-relay-server-group relayServer16
```

- To forward client traffic to a default extended DHCP local server that you specify:

```
[edit forwarding-options dhcp-relay relay-option-60 vendor-option]
user@host# set default-local-server-group localServer25
```

- To drop (discard) the non-matching packets:

```
[edit forwarding-options dhcp-relay relay-option-60 vendor-option]
user@host# set drop
```

For configuration examples that illustrate how to use nonmatching option 60 strings to forward or drop DHCP client traffic, see “Example: Using Option 60 Strings to Forward DHCP Client Traffic” on page 120 and “Example: Using Option 60 Strings to Drop DHCP Client Traffic” on page 121.

Displaying a Count of Discarded DHCP Packets with Option 60 Information

To display the number of discarded DHCP client packets containing option 60 vendor-specific information, use the following operational command:

- `show dhcp relay statistics`

For information about using this command, see the *JUNOS Routing Protocols and Policies Command Reference*.

Enabling and Disabling Insertion of Option 82 Information

You can enable or disable support for the DHCP relay agent information option (option 82) in packets destined for a DHCP server. To enable support for the DHCP relay agent information option you use the `relay-option-82` statement.

You can configure option 82 support globally or for a named group of interfaces.

To enable support for DHCP relay agent information option 82:

1. Specify that you want to configure option 82 support.


```
[edit forwarding-options dhcp-relay]
user@host# edit relay-option-82
```

2. Insert the option 82 information in DHCP packets.

See “Configuring Agent-Circuit-Id Information” on page 92.

3. (Optional) Include an option 82 prefix with the base option 82 information.

See “Configuring an Option 82 Prefix” on page 93.

4. (Optional) To restore the default behavior (option 82 information is not inserted into DHCP packets), do not include any subordinate statements.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option-82
```

This topic includes the following sections:

- Configuring Agent-Circuit-Id Information on page 92
- Configuring an Option 82 Prefix on page 93

Configuring Agent-Circuit-Id Information

You use the `relay-option-82` statement to enable insertion of option 82 information in DHCP packets. You must also specify at least the `circuit-id` statement to include the agent-circuit-id suboption (suboption 1) of the DHCP relay agent information option.

If you specify the `circuit-id` statement, the format of the agent-circuit id information for Fast Ethernet (**fe**) or Gigabit Ethernet (**ge**) interfaces is one of the following, depending on your network configuration:

- For Fast Ethernet or Gigabit Ethernet interfaces that do not use virtual local area networks (VLANs) or stacked VLANs (S-VLANs):

```
(fe | ge)-fpc/pic/port
```

- For Fast Ethernet or Gigabit Ethernet interfaces that use VLANs:

```
(fe | ge)-fpc/pic/port:vlan-id
```

- For Fast Ethernet or Gigabit Ethernet interfaces that use S-VLANs:

```
(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

To enable insertion of option 82 information:

1. Specify that you want to configure option 82 support.

```
[edit forwarding-options dhcp-relay]
user@host# edit relay-option-82
```

2. Specify insertion of the agent-circuit id.


```
[edit forwarding-options dhcp-relay relay-option-82]
user@host# set circuit-id
```

Configuring an Option 82 Prefix

You can include an optional prefix to the base option 82 information in DHCP packets destined for a DHCP server.

The prefix is separated from the option 82 agent-circuit-id information by a colon (:), and can include any combination of the **host-name**, **logical-system-name**, and **routing-instance-name** options. The DHCP relay agent obtains the values for the **host-name**, **logical-system-name**, and **routing-instance-name** as follows:

- If you include the **host-name** option, the DHCP relay agent uses the hostname of the router configured with the **host-name** statement at the [edit system] hierarchy level.
- If you include the **logical-system-name** option, the DHCP relay agent uses the logical system name configured with the **logical-system** statement at the [edit logical-system] hierarchy level.
- If you include the **routing-instance-name** option, the DHCP relay agent uses the routing instance name configured with the **routing-instance** statement at the [edit routing-instances] hierarchy level or at the [edit logical-system *logical-system-name* routing-instances] hierarchy level.

If you include the hostname and either or both of the logical system name and the routing instance name in the prefix, the hostname is followed by a forward slash (/). If you include both the logical system name and the routing instance name in the prefix, these values are separated by a semicolon (;).

The following examples show several possible formats for the agent-circuit-id information when you specify the **prefix** statement for Fast Ethernet (**fe**) or Gigabit Ethernet (**ge**) interfaces with S-VLANs.

- If you include only the hostname in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
hostname:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

- If you include only the logical system name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
logical-system-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

- If you include only the routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

- If you include both the hostname and the logical system name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
host-name/logical-system-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```


- If you include both the logical system name and the routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
logical-system-name;routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

- If you include the hostname, logical system name, and routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
host-name/logical-system-name;routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

For Fast Ethernet or Gigabit Ethernet interfaces that use VLANs but not S-VLANs, only the *vlan-id* value appears in the agent-circuit-id format. For Fast Ethernet or Gigabit Ethernet interfaces that do not use VLANs or S-VLANs, neither the *vlan-id* value nor the *svlan-id* value appears.

To configure an optional prefix with the option 82 information:

1. Specify that you want to configure option 82 support.

```
[edit forwarding-options dhcp-relay]
user@host# edit relay-option-82
```

2. Specify insertion of the agent-circuit id.

```
[edit forwarding-options dhcp-relay relay-option-82]
user@host# set circuit-id
```

3. Specify that the prefix is included in the option 82 information. In this example, the prefix includes the hostname and logical system name

```
[edit forwarding-options dhcp-relay relay-option-82]
user@host# set circuit-id prefix host-name logical-system-name
```

Configuring Server Groups

You can configure a named group of DHCP servers for use by the extended DHCP relay agent on the router.

You specify the name of the DHCP server group and the IP addresses of one or more DHCP servers that belong to this group. You can configure a maximum of five IP addresses per named server group.

To configure a named server group:

1. Specify the name of the server group.

```
[edit forwarding-options dhcp-relay]
user@host# set server-group myServerGroup
```

2. Add the IP addresses of the DHCP servers belonging to the group.

```
[edit forwarding-options dhcp-relay server-group myServerGroup]
user@host# set 192.168.100.50
```



```
user@host# set 192.168.100.75
```

Configuring Active Server Groups

You can configure an active server group. Using an active server group enables you to apply a common DHCP relay agent configuration to a named group of DHCP server addresses.

To configure an active server group:

- Specify the name of the active server group.

```
[edit forwarding-options dhcp-relay]
user@host# set active-server-group myServerGroup
```

To create an active server group as a global DHCP relay agent configuration option, include the **active-server-group** statement at the [edit forwarding-options dhcp-relay] hierarchy level. To have the group apply only to a named group of interfaces, include the **active-server-group** statement at the [edit forwarding-options dhcp-relay group *group-name*] hierarchy level.

Including the **active-server-group** statement at the [edit forwarding-options dhcp-relay group *group-name*] hierarchy level (as a group-specific option) overrides the effect of including the **active-server-group** statement at the [edit forwarding-options dhcp-relay] hierarchy level as a global option.

Attaching Dynamic Profiles to DHCP Subscriber Interfaces

This topic describes how to attach a dynamic profile to a DHCP subscriber interface. When a DHCP subscriber logs in, the specified dynamic profile is instantiated and the services defined in the profile are applied to the interface.

This topic contains the following sections:

- Attaching a Dynamic Profile to All DHCP Subscriber Interfaces on page 95
- Attaching a Dynamic Profile to a Group of DHCP Subscriber Interfaces on page 96

Attaching a Dynamic Profile to All DHCP Subscriber Interfaces

To attach a dynamic profile to all DHCP subscriber interfaces:

1. At the DHCP configuration hierarchy, use the **dynamic-profile** statement to specify the name of the dynamic profile to attach to all interfaces.

- For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# set dynamic-profile vod-profile-22
```

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
```



```
user@host# set dynamic-profile vod-profile-west
```

2. Optionally, you can configure the attribute to use when attaching the specified profile.

You can include either the **aggregate-clients** option to enable multiple DHCP subscribers to share the same VLAN logical interface, or the **use-primary** option to specify that the primary dynamic profile is used. The two options are mutually exclusive.

- To enable multiple subscribers to share the same VLAN logical interface:

```
[edit system services dhcp-local-server dynamic-profile]
user@host# set aggregate-clients
```

- To use the primary dynamic profile:

```
[edit forwarding-options dhcp-relay dynamic-profile]
user@host# set use-primary subscriber_profile
```

Attaching a Dynamic Profile to a Group of DHCP Subscriber Interfaces

To attach a dynamic profile to a group of interfaces:

Before you begin:

- Configure the interface group.

See “Grouping Interfaces with Common DHCP Configurations” on page 55.

1. At the DHCP configuration hierarchy, specify the name of the interface group and the dynamic profile to attach to the group.

- For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# set group boston dynamic-profile vod-profile-42
```

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# set group quebec dynamic-profile vod-profile-east
```

2. Optionally, you can configure the attribute to use when attaching the specified profile.

You can include either the **aggregate-clients** option to enable multiple DHCP subscribers to share the same VLAN logical interface, or the **use-primary** option to specify that the primary dynamic profile is used. The two options are mutually exclusive.

- To enable multiple subscribers to share the same VLAN logical interface:

```
[edit system services dhcp-local-server dynamic-profile]
user@host# set aggregate-clients
```


- To use the primary dynamic profile:

```
[edit forwarding-options dhcp-relay dynamic-profile]
user@host# set use-primary subscriber_profile
```

- Related Topics**
- Dynamic Profiles Overview on page 275
 - Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview on page 52
 - Example: Configuring Dynamic Subscriber Interfaces on IP Demux Interfaces on page 320

Verifying and Managing DHCP Relay Configuration

Purpose View or clear address bindings or statistics for extended DHCP relay agent clients:

- Action**
- To display the address bindings for extended DHCP relay agent clients:

```
user@host> show dhcp relay binding
```

- To display extended DHCP relay agent statistics:

```
user@host> show dhcp relay statistics
```

- To clear the binding state of DHCP relay agent clients:

```
user@host> clear dhcp relay binding
```

- To clear all extended DHCP relay agent statistics:

```
user@host> clear dhcp relay statistics
```

- Related Topics**
- For more information, see the *JUNOS System Basics and Services Command Reference*

Tracing Extended DHCP Operations

Both the extended DHCP local server and the extended DHCP relay agent support tracing operations. DHCP tracing operations track extended DHCP operations and record them in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

- Important events are logged in a file called `jdhcpd` located in the `/var/log` directory. You cannot change the directory (`/var/log`) in which trace files are located.
- When the file `jdhcpd` reaches 128 kilobytes (KB), it is renamed `jdhcpd.0`, then `jdhcpd.1`, and so on, until there are three trace files. Then the oldest trace file (`jdhcpd.2`) is overwritten.

You can optionally configure the maximum file size to be from 10 KB through 1 gigabyte (GB). You can also specify the number of trace files to be from 2 through 1000. (For more information about how log files are created, see the *JUNOS System Log Messages Reference*.)

- Log files can be accessed only by the user who configures the tracing operation.

To configure DHCP local server and DHCP relay agent tracing operations:

1. Specify that you want to configure tracing options.

- For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# edit traceoptions
```

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# edit traceoptions
```

2. (Optional) Configure the name for the file used for the trace output.

See “Configuring the Extended DHCP Log Filename” on page 68.

3. (Optional) Configure the number and size of the log files.

See “Configuring the Number and Size of Extended DHCP Log Files” on page 68.

4. (Optional) Configure access to the log file.

See “Configuring Access to the Extended DHCP Log File” on page 68.

5. (Optional) Configure a regular expression to filter logging events.

See “Configuring a Regular Expression for Extended DHCP Lines to Be Logged” on page 69.

6. (Optional) Configure flags to filter the operations to be logged.

See “Configuring the Extended DHCP Tracing Flags” on page 69.

The extended DHCP traceoptions operations are described in the following sections:

- Configuring the Extended DHCP Log Filename on page 98
- Configuring the Number and Size of Extended DHCP Log Files on page 99
- Configuring Access to the Extended DHCP Log File on page 99
- Configuring a Regular Expression for Extended DHCP Lines to Be Logged on page 100
- Configuring the Extended DHCP Tracing Flags on page 100

Configuring the Extended DHCP Log Filename

By default, the name of the file that records trace output is `jdhcpd`. You can specify a different name by including the `file` option:

To configure the filename for DHCP local server and DHCP relay agent tracing operations:

- Specify the name of the file used for the trace output. (DHCP local server and DHCP relay agent both support the file option for the `traceoptions` statement.)

```
[edit system services dhcp-local-server traceoptions]
user@host# set file dhcp_logfile_1
```

Configuring the Number and Size of Extended DHCP Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed *filename.0*, then *filename.1*, and so on, until there are three trace files. Then the oldest trace file (*filename.2*) is overwritten.

You can optionally configure the maximum file size to be from 10 KB through 1 gigabyte (GB). You can also specify the number of trace files to be from 2 through 1000.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (*filename*) reaches 2 MB, *filename* is renamed *filename.0*, and a new file called *filename* is created. When the new *filename* reaches 2 MB, *filename.0* is renamed *filename.1* and *filename* is renamed *filename.0*. This process repeats until there are 20 trace files. Then the oldest file (*filename.19*) is overwritten by the newest file (*filename.0*).

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output. (DHCP local server and DHCP relay agent both support the `files` and `size` options for the `traceoptions` statement.)

```
[edit system services dhcp-local-server traceoptions]
user@host# set file dhcp_logfile_1 files 20 size 2097152
```

Configuring Access to the Extended DHCP Log File

By default, log files can be accessed only by the user who configures the tracing operation. You can enable all users to read the log file and you can explicitly set the default behavior of the log file.

To specify that all users can read the log file:

- Configure the log file to be world-readable. (DHCP local server and DHCP relay agent both support the `world-readable` option for the `traceoptions` statement.)

```
[edit system services dhcp-local-server traceoptions]
user@host# set file dhcp_logfile_1 world-readable
```


To explicitly set the default behavior, in which the log file can only be read by the user who configured tracing:

- Configure the log file to be no-world-readable. (DHCP local server and DHCP relay agent both support the `no-world-readable` option for the `traceoptions` statement.)

```
[edit system services dhcp-local-server traceoptions]
user@host# set file dhcp_logfile_1 no-world-readable
```

Configuring a Regular Expression for Extended DHCP Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events.

You can refine the output by including regular expressions that will be matched.

To configure regular expressions to be matched:

- Configure the regular expression. (DHCP local server and DHCP relay agent both support the `match` option for the `traceoptions` statement.)

```
[edit system services dhcp-local-server traceoptions]
user@host# set file dhcp_logfile_1 match regex
```

Configuring the Extended DHCP Tracing Flags

By default, only important events are logged. You can specify which trace operations are logged by including specific tracing flags. The following table describes the flags that you can include.

Flag	Description
all	Trace all events
auth	Trace authentication events
database	Trace database events
fwd	Trace firewall process events
general	Trace miscellaneous events
ha	Trace high availability-related events
interface	Trace interface operations
io	Trace I/O operations
packet	Trace packet decoding operations
packet-option	Trace DHCP option decoding operations
rpd	Trace routing protocol process events

Flag	Description
rtstock	Trace routing socket operations
session-db	Trace session database events
state	Trace changes in state
ui	Trace user interface operations

To configure the flags for the events to be logged:

- Configure the flags. (DHCP local server and DHCP relay agent both support the `flag` option for the `traceoptions` statement.)

```
[edit system services dhcp-local-server traceoptions]
user@host# set flag packet-option
```


Chapter 7

Configuring Subscriber Secure Policy Traffic Mirroring

- Subscriber Secure Policy Overview on page 104
- Subscriber Secure Policy Traffic Mirroring Architecture on page 105
- RADIUS Attributes Used for Subscriber Secure Policy on page 107
- Configuring Subscriber Secure Policy Mirroring Overview on page 110
- Guidelines for Configuring Subscriber Secure Policy Mirroring on the Flow-Tap Service on page 111
- Configuring Flow-Tap Service Support for Subscriber Secure Policy Mirroring on page 112
- Configuring RADIUS Server Support for Subscriber Secure Policy Mirroring on page 113
- Terminating Subscriber Secure Policy Mirroring Sessions on page 114

Subscriber Secure Policy Overview

Subscriber secure policy provides RADIUS-initiated traffic mirroring on a per-subscriber basis. RADIUS-initiated mirroring creates secure policies based on certain RADIUS VSAs and uses RADIUS attributes to identify the subscriber whose traffic is to be mirrored. The traffic mirroring operation is triggered by the attributes received in RADIUS messages. Both the subscriber's ingress and egress traffic are mirrored. The original traffic is sent to its intended destination and the mirrored traffic is sent to a mediation device for analysis.

There are two variations of RADIUS-initiated mirroring. For both types, the mirroring operation is initiated without regard to the subscriber location, router, interface, or type of traffic.

- **Subscriber log in**—The mirroring operation starts when the subscriber logs in and the trigger is received in a RADIUS Access-Accept message. Using triggers in RADIUS Access-Accept messages enables you to mirror per-subscriber traffic without regard to how often the subscriber logs in or out, or which router or interface the subscriber uses.
- **In-session**—The mirroring operation starts when the trigger is received in a RADIUS Change-of-Authorization-Request (CoA-Request) message. Using triggers in CoA messages enables you to immediately mirror traffic of a subscriber who is already logged in.

Configuration of RADIUS-based mirroring is independent of the actual mirroring session—you can configure the mirroring parameters at any time. Also, you can use a single RADIUS server to provision mirroring operations on multiple routers in a service provider's network. To provide security, the ability to configure, access, and view the subscriber secure policy components and configuration is restricted to authorized users. The actual mirroring operation is transparent to subscribers whose traffic is being mirrored.

Traffic mirroring has many uses, such as debugging network problems, troubleshooting specific user issues, and lawful intercept. For example, you might use RADIUS-based mirroring when debugging network problems related to mobile users, who do not always log in to the same router. RADIUS-based mirroring is particularly useful for large networks, in which you can use a single RADIUS server to provision the mirroring operation.

Subscriber Secure Policy Terms

Table 17 on page 104 defines terms that are used in the discussion of subscriber secure policy.

Table 17: Subscriber Secure Policy Terms

Term	Definition
Flow-tap service	The application that extends the Dynamic Tasking Control Protocol (DTCP) for active traffic monitoring. The subscriber secure policy service runs on top of the flow-tap service.

Table 17: Subscriber Secure Policy Terms *(continued)*

Term	Definition
Intercept access point	Device that requests and configures the subscriber secure policy service. The Juniper Networks router performs this function.
Mediation device	Location to which the mirrored traffic is sent. Also called an analyzer device.
Mirrored subscriber	Subscriber whose traffic is mirrored.
Mirror trigger	RADIUS attribute that identifies a subscriber whose traffic is to be mirrored. Mirroring starts when the trigger is detected.
Requesting authority	Authorized group that requests or conducts traffic mirroring.
Salt encryption	Random string of data used to modify a password hash. The mirroring VSAs sent to the router by the RADIUS server are Salt-encrypted.
Target system	The system on which the subscriber secure policy service (and flow-tap service) is configured.

- Related Topics**
- Subscriber Secure Policy Traffic Mirroring Architecture on page 105
 - RADIUS Attributes Used for Subscriber Secure Policy on page 107
 - Configuring Subscriber Secure Policy Mirroring Overview on page 110

Subscriber Secure Policy Traffic Mirroring Architecture

This topic describes the subscriber secure policy architecture and includes a description of how mirrored traffic flows within the subscriber secure policy environment.

Figure 4 on page 106 illustrates the subscriber secure policy mirroring environment. The Juniper Networks router, functioning as an intercept access point, is the center piece of the subscriber secure policy architecture. The figure indicates the sequence of events that are performed to configure mirroring operations and the traffic flow that occurs during mirroring. The tables after the figure describe the events indicated by the figure. Table 18 on page 106 describes the configuration sequence. Table 19 on page 106 and Table 20 on page 107 describe the sequence of events that occur during mirroring operations.



NOTE: A special UDP/IP header is prepended to each mirrored packet sent to the mediation device. The prepended header is used as a demultiplexer, enabling the mediation device to differentiate the multiple mirrored streams that arrive from different sources.

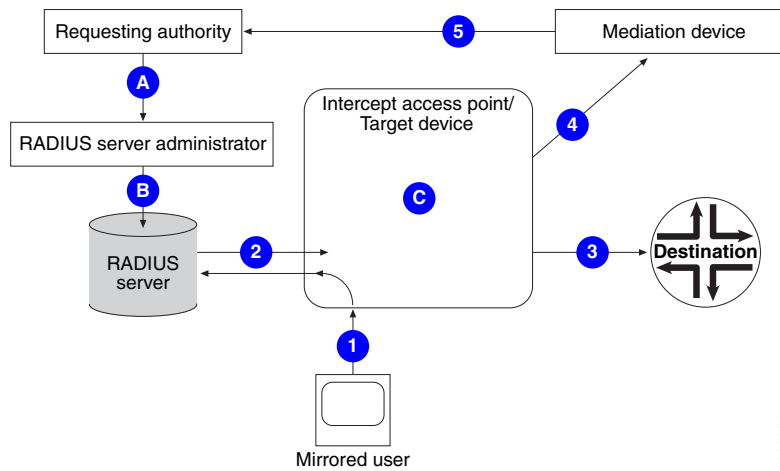
Figure 4: Subscriber Secure Policy Architecture

Table 18 on page 106 lists the high-level steps that are required to configure the subscriber secure policy traffic mirroring environment.

Table 18: Subscriber Secure Policy Configuration Steps

Step	Description
A	An authorized individual or group requests traffic mirroring. This group also ensures that the mediation device is configured to receive and analyze mirrored traffic.
B	The RADIUS server administrator configures the subscriber RADIUS record to include the mirroring-related RADIUS attributes and VSAs.
C	The Juniper Networks router administrator configures the subscriber secure policy service on the router, including the flow-tap service configuration, RADIUS server information, and mediation device information.

Table 19 on page 106 shows the process for a subscriber login mirroring operation, which is initiated when the mirrored subscriber logs in.

Table 19: RADIUS-Initiated Mirroring at Subscriber Login

Step	Description
1	The subscriber logs in, requesting authentication by the RADIUS server.
2	<ul style="list-style-type: none"> ■ The RADIUS server authenticates the subscriber and sends an Access-Accept message containing the mirroring-related RADIUS attributes and VSAs to the router (intercept access point). ■ The mirroring trigger in the RADIUS Access-Accept message initiates the mirroring operation. ■ The intercept access point creates the subscriber secure policy based on the mirroring VSAs and begins mirroring the subscriber's traffic.
3	The intercept access point sends the original subscriber traffic to its intended destination.

Table 19: RADIUS-Initiated Mirroring at Subscriber Login (continued)

Step	Description
4	The intercept access point sends the mirrored subscriber traffic to the mediation device.
5	The mediation device provides information about the mirrored traffic to the requesting authority.

Table 20 on page 107 shows the mirroring procedure for an in-session mirroring operation, in which the subscriber is already logged in.

Table 20: RADIUS-Initiated Mirroring for Current Subscriber

Step	Description
1	The subscriber logs in, requesting authentication by the RADIUS server. The RADIUS server authenticates the subscriber (no mirroring activity occurs).
2	<ul style="list-style-type: none"> ■ Subscriber-based mirroring is later requested by the requesting authority and then enabled on the RADIUS server. ■ The RADIUS server sends a CoA message containing the mirroring-related RADIUS attributes and VSAs to the router (intercept access point). ■ The mirroring trigger in the RADIUS CoA message initiates the mirroring operation. ■ The intercept access point creates the subscriber secure policy based on the mirroring VSAs and immediately begins mirroring subscriber traffic.
3	The intercept access point sends the original subscriber traffic to its intended destination.
4	The intercept access point sends the mirrored subscriber traffic to the mediation device.
5	The mediation device provides information about the mirrored traffic to the requesting authority.

- Related Topics**
- Subscriber Secure Policy Overview on page 104
 - RADIUS Attributes Used for Subscriber Secure Policy on page 107
 - Configuring Subscriber Secure Policy Mirroring Overview on page 110

RADIUS Attributes Used for Subscriber Secure Policy

Subscriber secure policy mirroring triggers are RADIUS attributes that identify a subscriber whose traffic is to be mirrored. The actual traffic mirroring session starts when the router (intercept access point) receives a RADIUS packet that contains a trigger and then applies the subscriber secure policy configuration to the appropriate interface.

The router receives subscriber secure policy triggers in the following types of RADIUS messages:

- RADIUS Access-Accept—Used to start a mirroring session when the specified subscriber logs in.

- RADIUS Change-of-Authorization-Request (CoA-Request)—Used to immediately begin mirroring traffic of the specified subscriber, who is already logged in.

Table 21 on page 108 lists the mirroring triggers that the RADIUS server administrator adds to the RADIUS record of the subscriber whose traffic is to be mirrored. In addition, the RADIUS VSAs listed in Table 22 on page 108 must be included in the mirrored subscriber's RADIUS record.

RADIUS Attributes Used as Traffic Mirroring Triggers

Table 21 on page 108 lists the subscriber secure policy mirroring triggers (RADIUS attributes) that can be present in RADIUS Access-Accept and CoA messages. The attributes identify the subscriber whose traffic is to be mirrored.

Table 21: RADIUS Attributes Used as Traffic Mirroring Triggers

Attribute Number	Attribute Name
[1]	User-Name
[8]	Framed-IP-Address
[31]	Calling-Station-ID
[44]	Acct-Session-ID
[87]	Nas-Port-ID

RADIUS-Based Mirroring Attributes

Table 22 on page 108 lists the RADIUS VSAs that you must include in the RADIUS record of the subscriber whose traffic is to be mirrored. The VSAs carry mirroring-related information.

The AAA Service Framework uses vendor ID 4874, which is assigned to Juniper Networks by the Internet Assigned Numbers Authority (IANA).



NOTE: VSA 26-10 uses vendor ID 2636.

Table 22: RADIUS-Based Mirroring Attributes

Attribute Number	Attribute Name	Description	Value
[26-10]	Juniper-User-Permissions	Information that specifies user permissions. This attribute is used only in Access-Accept packets.	String
This attribute uses vendor ID 2636.			

Table 22: RADIUS-Based Mirroring Attributes (continued)

Attribute Number	Attribute Name	Description	Value
[26-58]	LI-Action	Traffic mirroring action	<ul style="list-style-type: none"> ■ 0 = stop mirroring ■ 1 = start mirroring ■ 2 = no action
[26-59]	Med-Dev-Handle	Link to which traffic mirroring is applied	Salt-encrypted string
[26-60]	MD-Ip-Address	IP address of mediation device to which mirrored traffic is forwarded	Salt-encrypted IP address
[26-61]	MD-Port-Number	UDP port in the mediation device to which mirrored traffic is forwarded	Salt-encrypted integer

Considerations When Using RADIUS Attributes for Subscriber Secure Policy

When using RADIUS attributes and VSAs for the subscriber secure policy service, keep the following considerations in mind:

- A dynamic profile must exist for a subscriber whose traffic is to be mirrored. Otherwise, the subscriber is unable to log in when the mirroring-related VSAs are received in RADIUS Accept-Accept or CoA messages. See “Dynamic Profiles Overview” on page 275 for information about dynamic profiles.
- VSA 26-60 must always be present in the RADIUS Access-Accept or CoA message, or the instantiation of the mirroring session will fail. The presence of VSA 26-60 triggers the prepending operation—all mirrored packets must be prepended with both the UDP/IP header and the MD header.
- VSA 26-58 (LI-Action) specifies the action taken by the router. The action differs if the VSA is received in an Access-Accept message or a CoA message, as indicated in Table 23 on page 109.

Table 23: LI-Action VSA Action

LI-Action Value	Access-Accept Message Action	CoA Message Action
0	Prevents subscriber from logging in	Immediately stops mirroring subscriber traffic; subscriber remains logged in
1	Starts mirroring subscriber traffic when subscriber logs in	Immediately starts mirroring subscriber traffic

Table 23: LI-Action VSA Action (continued)

LI-Action Value	Access-Accept Message Action	CoA Message Action
2	No action	No action

- A VSA 26–58 value of 2 specifies that the router does not perform any traffic mirroring-related action. This setting can provide additional security by confusing unauthorized users who attempt to access traffic mirroring communication between the router and the RADIUS server.

Related Topics

- Subscriber Secure Policy Overview on page 104
- Subscriber Secure Policy Traffic Mirroring Architecture on page 105
- Configuring Subscriber Secure Policy Mirroring Overview on page 110
- Dynamic Profiles Overview on page 275
- Example: Subscriber Secure Policy Dynamic Profile

Configuring Subscriber Secure Policy Mirroring Overview

You can configure subscriber secure policy mirroring to mirror the traffic of a particular subscriber.



NOTE: Subscriber secure policy RADIUS-initiated mirroring runs on the flow-tap service infrastructure. To configure the subscriber secure policy service, you must have the same privileges that are required to configure the flow-tap service.

To configure the subscriber secure policy service:

1. Configure the flow-tap service.

See the *JUNOS Services Interfaces Configuration Guide* for information about configuring the flow-tap service.

2. Configure additional secure subscriber policy support for the flow-tap service. This support includes configuring the tunnels and optional forwarding-class information that the subscriber secure policy service uses to send mirrored traffic to the content destination device.

See “Configuring Flow-Tap Service Support for Subscriber Secure Policy Mirroring” on page 112.

3. Configure an access profile that specifies the RADIUS-related support for subscriber secure policy on the router, including a list of one or more RADIUS authentication servers. The router uses the list of specified servers for both authentication and dynamic request operations. You must also configure the RADIUS dynamic request feature, which provides the CoA message support used in-session traffic mirroring.

See “Configuring RADIUS Server Support for Subscriber Secure Policy Mirroring” on page 113.

See “Using RADIUS Dynamic Requests for Subscriber Access Management” on page 25.

4. Ensure that the following support is also configured:
 - The RADIUS record of the mirrored subscriber must include the RADIUS attributes and VSAs required for subscriber secure policy mirroring. See “RADIUS Attributes Used for Subscriber Secure Policy” on page 107 for descriptions of the supported attributes used in RADIUS Accept-Accept and CoA messages.
 - The content destination device must be configured to accept the mirrored data from the mediation device.

The descriptions of these configurations are beyond the scope of this document.

5. You can terminate an active subscriber mirroring session at any time. See “Terminating Subscriber Secure Policy Mirroring Sessions” on page 114.



NOTE: The subscriber secure policy feature requires some system resources while mirroring, encrypting, and sending traffic to the mediation device. We recommend that you consider this requirement when you configure subscriber secure policy. For example, you might elect to use a 10-Gigabit Ethernet interface for the tunnel and mediation device if you expect the amount of traffic you plan to mirror to approach 1 Gps of actual user data.

-
- Related Topics**
- Subscriber Secure Policy Overview on page 104
 - Subscriber Secure Policy Traffic Mirroring Architecture on page 105
 - RADIUS Attributes Used for Subscriber Secure Policy on page 107
 - Terminating Subscriber Secure Policy Mirroring Sessions on page 114

Guidelines for Configuring Subscriber Secure Policy Mirroring on the Flow-Tap Service

The subscriber secure policy service runs on the flow-tap service infrastructure. When configuring subscriber secure policy mirroring, consider the following guidelines regarding the relationship between subscriber secure policy service and the flow-tap service:

- Subscriber secure policy inherits the limitations of the flow-tap service. For example, port mirroring and the flow-tap service cannot run simultaneously on the router. Therefore, port mirroring and subscriber secure policy mirroring cannot run simultaneously on the same router.
- You can configure one instance of the flow-tap service on the router. Both subscriber secure policy RADIUS-initiated mirroring and DTCP-initiated mirroring use the flow-tap service.

- If you configure both RADIUS-initiated mirroring and DTCP-initiated mirroring, and the two mirroring requests are the same, duplicate mirrored traffic is sent to the mediation device.
- You cannot delete the flow-tap service configuration while a subscriber secure policy mirroring session is active on the service.

Related Topics

- Subscriber Secure Policy Overview on page 104
- Configuring Subscriber Secure Policy Mirroring Overview on page 110
- Configuring Flow-Tap Service Support for Subscriber Secure Policy Mirroring on page 112

Configuring Flow-Tap Service Support for Subscriber Secure Policy Mirroring

The RADIUS-initiated mirroring provided by the subscriber secure policy service runs on the flow-tap service infrastructure. This topic describes the steps to enable flow-tap support for subscriber secure policy mirroring.



NOTE: To configure the subscriber secure policy service, you must have the same privileges that are required to configure the flow-tap service.

To configure the flow-tap service to support subscriber secure policy mirroring:

1. Configure the standard flow-tap service.

```
[edit services]
user@host# set flow-tap interface sp-1/2/0.100
```

See “Flow-Tap Configuration Guidelines” in the *JUNOS Services Interfaces Configuration Guide* for details on configuring the flow-tap service.

2. Allocate a pool of tunnel interfaces that the flow-tap service can use for subscriber secure policy mirroring. The intercept access point uses these interfaces to send mirrored traffic to the mediation device. The intercept access point equally distributes the mirrored traffic across the available tunnel interfaces.

You can configure a maximum of 2048 mirrored subscriber sessions per chassis.

```
[edit chassis]
user@host# set fpc 4 pic 1 tunnel-services bandwidth 1g
```

3. Configure the tunnel interfaces.

```
[edit interfaces]
user@host# set vt-4/1/10.0
user@host# set vt-4/2/10.0
```

4. Assign the tunnel interfaces that the flow-tap service uses for RADIUS-initiated subscriber secure policy mirroring.



NOTE: If a currently used tunnel interface is deleted from the pool of interfaces, the subscriber secure policy service redistributes the active mirroring sessions from the deleted interface to other tunnel interfaces in the pool. Also, when a new tunnel interface is added into the pool, the service adds the new interface to the list of available interfaces—the new interface is used for new mirroring sessions or for existing sessions transferred from a failed interface.

```
[edit services]
user@host# set radius-flow-tap interfaces vt-4/1/10.0
user@host# set radius-flow-tap interfaces vt-4/2/10.0
```

5. Specify the source IP address that the flow-tap service uses for RADIUS-initiated mirroring. This address is used in the IP header prepended to mirrored packets that are sent to the content destination device.

```
[edit services]
user@host# set radius-flow-tap source-ipv4-address 192.168.100.33
```

6. (Optional) Specify the forwarding class that is applied to the mirrored packets sent to the mediation device.

If you do not specify a forwarding class, the mirrored packets inherit the forwarding class from the original packet (which is the forwarding class set by default classification that CoS applies to the packet on the ingress interface).

```
[edit services]
user@host# set radius-flow-tap forwarding-class best-effort
```

- Related Topics**
- Subscriber Secure Policy Overview on page 104
 - Configuring Subscriber Secure Policy Mirroring Overview on page 110
 - Guidelines for Configuring Subscriber Secure Policy Mirroring on the Flow-Tap Service on page 111

Configuring RADIUS Server Support for Subscriber Secure Policy Mirroring

This topic describes how to configure RADIUS server support for the subscriber secure policy service. The RADIUS server can then initiate subscriber-based traffic mirroring. You create an access profile to specify the RADIUS server support.

To configure the router's interaction with the RADIUS server in support of subscriber secure policy mirroring:

1. Create the access profile and assign a name.

```
[edit access]
user@host# edit profile ssp-server
```

2. Specify RADIUS as the authentication method.

```
[edit access profile ssp-server]
```



```
user@host# set authentication-order radius
```

3. Specify the IP address of the RADIUS server that performs authentication. This server also performs dynamic request (CoA) functions.

```
[edit access profile ssp-server]
user@host# set radius authentication-server 192.168.53.105
```

4. Specify the secret to use when communicating with the RADIUS server.

```
[edit access profile ssp-server]
user@host# set radius-server 192.168.53.105 secret mysecret42
```

5. Specify other optional RADIUS configuration settings as needed, such as accounting support.

- Related Topics**
- Subscriber Secure Policy Overview on page 104
 - Configuring Subscriber Secure Policy Mirroring Overview on page 110
 - RADIUS Attributes Used for Subscriber Secure Policy on page 107

Terminating Subscriber Secure Policy Mirroring Sessions

This topic describes how active subscriber secure policy mirroring operations might be terminated. The RADIUS-initiated mirroring sessions can be explicitly terminated upon receipt of a RADIUS dynamic request or passively terminated as a result of a timeout or disconnection.

A RADIUS-initiated traffic mirroring session is terminated by the following actions:

- RADIUS CoA message receipt—Mirroring is terminated upon receipt of a CoA message with a VSA 26-58 (LI-Action) value of 0. The RADIUS administrator configures the LI-Action of 0 in the mirrored subscriber's RADIUS record.
- Subscriber logout—Mirroring is terminated when the mirrored subscriber logs out.
- Session timeout—Mirroring is terminated when the current subscriber session times out.
- Session disconnect—Mirroring is terminated when the current subscriber session is disconnected.

- Related Topics**
- Subscriber Secure Policy Overview on page 104
 - Configuring Subscriber Secure Policy Mirroring Overview on page 110
 - RADIUS Attributes Used for Subscriber Secure Policy on page 107

Chapter 8

AAA and Remote Subscriber Access Configuration Examples

- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 115
- Example: Configuring an Address-Assignment Pool on page 117
- Example: Minimum Extended DHCP Local Server Configuration on page 118
- Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 118
- Example: Minimum DHCP Relay Agent Configuration on page 118
- Example: DHCP Relay Agent Configuration with Multiple Clients and Servers on page 119
- Example: Using Option 60 Strings to Forward DHCP Client Traffic on page 120
- Example: Using Option 60 Strings to Drop DHCP Client Traffic on page 121

Example: Configuring RADIUS-Based Subscriber Authentication and Accounting

This section shows an example RADIUS-based authentication and accounting configuration.

```
[edit access]
radius-server {
  192.168.1.250 {
    port 1812;
    accounting-port 1813;
    retry 3;
    secret &tlUEI*7688+;
    source-address 192.168.1.100;
    timeout 45;
  }
  192.168.1.251 {
    port 1812;
    accounting-port 1813;
    retry 3;
    secret $Dyu*UY(877-;
    source-address 192.168.1.100;
    timeout 30;
  }
  192.168.1.252 {
```



```

    port 1812;
    secret $Dyu*UY(877-;
  }
}
profile isp-bos-metro-fiber-basic {
  authentication {
    order radius none;
  }
  accounting {
    order radius;
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    immediate-update;
    statistics time;
    update-interval 12;
  }
  radius {
    authentication-server 192.168.1.251 192.168.1.252;
    accounting-server 192.168.1.250 192.168.1.251;
    options {
      accounting-session-id-format decimal;
      nas-identifier 56;
      override-nas-information;
    }
    attributes {
      ignore {
        framed-ip-netmask;
      }
      exclude {
        accounting-delay-time [accounting-start accounting-stop];
        accounting-session-id [access-request accounting-on accounting-off
        accounting-start accounting-stop];
        dhcp-gi-address [access-request accounting-start accounting-stop];
        dhcp-mac-address [access-request accounting-start accounting-stop];
        nas-identifier [access-request accounting-start accounting-stop];
        nas-port [accounting-start accounting-stop];
        nas-port-id [accounting-start accounting-stop];
        nas-port-type [access-request accounting-start accounting-stop];
      }
    }
  }
}
[edit logical-systems isp-bos-metro-12 routing-instances isp-cmbrg-12-32]
interfaces {
  lo0 {
    unit 0 {
      family inet {
        address 192.168.1.100/24;
      }
    }
  }
  ge-0/0/0 {
    vlan-tagging;
    unit 0 {
      vlan-id 200;
      family inet {

```



```

        unnumbered-address lo0.0;
    }
}
}

```

Example: Configuring an Address-Assignment Pool

This section shows an example address-assignment pool configuration. The configuration includes the `dhcp-attributes` statement, indicating that the pool is used for DHCP clients.

```

[edit access]
address-assignment {
  pool isp_1 family inet {
    network 192.168.0.0/16;
    range southeast {
      low 192.168.102.2 high 192.168.102.254;
    }
    range northeast {
      low 192.168.119.2 high 192.168.119.250;
    }
    host sval6.boston.net {
      hardware-address 90:00:00:01:00:01;
      ip-address 192.168.44.12;
    }
  }
  dhcp-attributes {
    option-match {
      option-82 {
        circuit-id fiber range northeast;
      }
      option-82 {
        circuit-id cable_net range southeast;
      }
    }
    boot-file boot.client;
    boot-server 192.168.200.100;
    grace-period 3600;
    maximum-lease-time 18000;
    netbios-node-type p-node;
  }
  router 192.168.44.44 192.168.44.45;
}

```

This example creates address-assignment pool **isp-1**, which contains two named address ranges, **southeast** and **northeast**. The address-assignment pool also contains a static binding for client **host sval6.boston.net**. If the option 82 circuit-id entry matches the string **fiber**, then DHCP assigns the client an address from the **northeast** range. If the option 82 circuit-id matches the string **cable_net**, DHCP assigns an address from the **southeast** range.

Example: Minimum Extended DHCP Local Server Configuration

The following example shows the minimum configuration you need to use the extended DHCP local server on the router:

```
[edit system services]
dhcp-local-server {
  group group_one {
    interface fe-0/0/2.0;
  }
}
```

This example creates the server group named **group_one**, and specifies that the DHCP local server is enabled on interface **fe-0/0/2.0** within the group. The DHCP local server uses the default pool match configuration of **ip-address-first**.

Example: Extended DHCP Local Server Configuration with Optional Pool Matching

The following example shows an extended DHCP local server configuration that includes optional pool matching and interface groups. This configuration specifies that the DHCP local server uses option 82 information to match the named address range for client IP address assignment. The option 82 matching must also be included in the address-assignment pool configuration.

```
[edit system services]
dhcp-local-server {
  group group_one {
    interface fe-0/0/2.0;
    interface fe-0/0/2.1;
  }
  group group_two {
    interface fe-0/0/3.0;
    interface fe-0/0/3.1;
  }
  pool-match-order {
    ip-address-first;
    option-82;
  }
}
```

Example: Minimum DHCP Relay Agent Configuration

The following example shows the minimum configuration you need to use the extended DHCP relay agent on the router:

```
[edit forwarding-options]
dhcp-relay {
  server-group {
    test 10.0.2.1;
  }
  active-server-group test;
  group all {
    interface fe-0/0/2.0;
  }
}
```



```

    }
}

```

This example creates a server group and an active server group named **test** with IP address 10.0.2.1. The DHCP relay agent configuration is applied to a group named **all**. Within this group, the DHCP relay agent is enabled on interface fe-0/0/2.0.

Example: DHCP Relay Agent Configuration with Multiple Clients and Servers

The following example shows a more complex extended DHCP relay agent configuration for a network that includes multiple DHCP clients and DHCP servers. A more detailed explanation follows the example.

```

[edit forwarding-options]
dhcp-relay {
  server-group {
    sp-1 {
      10.0.2.1;
      10.0.2.2;
    }
    sp-2 {
      10.33.2.1;
      10.33.2.2;
      10.33.2.3;
    }
  }
  active-server-group sp-1;
  overrides layer2-unicast-replies;
  group clients_a {
    relay-option-82 circuit-id;
    interface fe-1/0/1.1;
    interface fe-1/0/1.2;
    interface fe-1/0/1.3;
  }
  group clients_b {
    relay-option-82 {
      circuit-id {
        prefix routing-instance-name;
      }
    }
    interface fe-1/0/1.4;
    interface fe-1/0/1.5;
    interface fe-1/0/1.6;
  }
  group eth_dslam_relay {
    active-server-group sp-2;
    overrides {
      trust-option-82;
      layer2-unicast-replies;
    }
    interface fe-1/0/1.7;
    interface fe-1/0/1.8;
    interface fe-1/0/1.9;
  }
}

```


This example creates two server-groups: **sp-1**, which includes DHCP server addresses 10.0.2.1 and 10.0.2.2, and **sp-2**, which includes DHCP server addresses 10.33.2.1, 10.33.2.2, and 10.33.2.3. The active server group to which the DHCP relay agent configuration applies is **sp-1**. A global override is set that causes the DHCP relay agent to use Layer 2 unicast transmission to send DHCP reply packets from the DHCP server to DHCP clients during the discovery process.

The example also creates three groups of subscribers and their associated Fast Ethernet interfaces: **clients_a**, **clients_b**, and **eth_dslam_relay**. These groups are configured to meet different needs, as follows:

- The **clients_a** and **clients_b** groups consist of basic subscribers. The service provider for these groups inserts option 82 information in the DHCP packets that are destined for the DHCP server.
- The subscribers in **eth_dslam_relay** are connected to an Ethernet digital subscriber line access multiplexer (DSLAM) that functions as a Layer 2 DHCP relay agent. The active server group for **eth_dslam_relay** is **sp-2**. Overrides are set for the **eth_dslam_relay** group that enable the DHCP relay agent to trust option 82 information and to use Layer 2 unicast transmission to send DHCP reply packets to DHCP clients during discovery.

Example: Using Option 60 Strings to Forward DHCP Client Traffic

The following extended DHCP relay agent configuration shows how to use the option 60 vendor-specific information in DHCP client packets to forward client traffic to specific DHCP servers. A more detailed explanation follows the example.

```
[edit forwarding-options]
dhcp-relay {
  server-group {
    sp-1 {
      10.0.2.1;
    }
    sp-2 {
      10.33.2.1;
    }
    sp-3 {
      10.22.2.1;
    }
    sp-4 {
      10.10.2.1;
    }
  }
  active-server-group sp-1;
  relay-option-60 {
    vendor-option {
      equals {
        ascii motorola {
          relay-server-group sp-2;
        }
      }
    }
    starts-with {
      hexadecimal ff {
```



```

        relay-server-group sp-3;
    }
}
default-relay-server-group sp-4;
}
}
group all {
    interface fe-0/0/2.0;
}
}

```

This example defines the following actions for DHCP client packets containing option 60 information:

- All packets that contain an exact match with the ASCII string “motorola” are relayed to server group **sp-2**.
- All packets that start with the hexadecimal string “ff” are relayed to server group **sp-3**.
- All packets that do not either exactly match the ASCII string “motorola” or start with the hexadecimal string “ff” are relayed to the default relay server group, **sp-4**.

DHCP client packets that do not contain option 60 information are relayed to the currently configured active server group, **sp-1**.

Server groups **sp-1**, **sp-2**, **sp-3**, and **sp-4** in this example are configured with the `server-group` statement at the `[edit forwarding-options dhcp-relay]` hierarchy level.

Example: Using Option 60 Strings to Drop DHCP Client Traffic

The following extended DHCP relay agent configuration shows how to use the option 60 vendor-specific information in DHCP client packets to drop client traffic. Specifying that certain DHCP client packets be dropped can be useful when DHCP clients request services that are invalid or no longer supported.

```

[edit forwarding-options]
dhcp-relay {
    server-group {
        sp-1 {
            10.0.2.1;
        }
    }
    active-server-group sp-1;
    relay-option-60 {
        vendor-option {
            drop;
        }
    }
    group all {
        interface fe-0/0/2.0;
    }
}

```


In this example, all DHCP client packets containing option 60 information are discarded (dropped), and all packets that do not contain option 60 information are relayed to the currently configured active server group, **sp-1**.

Chapter 9

Summary of AAA and Remote Subscriber Access Statements

accounting

Syntax accounting {
 accounting-stop-on-access-deny;
 accounting-stop-on-failure;
 order [*accounting-method*];
 statistics (time | volume-time);
 update-interval *minutes*;
 }

Hierarchy Level [edit access profile *profile-name*]

Release Information Statement introduced in JUNOS Release 9.1.

Description Configure RADIUS accounting parameters and enable RADIUS accounting for an access profile.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

Related Topics ■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19

accounting-port

Syntax	<code>accounting-port <i>port-number</i>;</code>
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
Release Information	Statement introduced before JUNOS Release 7.4.
Description	Configure the port number on which to contact the accounting server.
Options	<i>port-number</i> —The port number on which to contact the accounting server. Most RADIUS servers use port number 1813 (as specified in RFC 2866).
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none">■ Router Interaction with RADIUS Servers Overview on page 18■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19

accounting-server

Syntax	accounting-server [<i>ip-address</i>];
Hierarchy Level	[edit access profile <i>profile-name</i> radius]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Specify a list of the RADIUS accounting servers used to for accounting for DHCP, L2TP, and PPP clients.
Options	<i>ip-address</i> —The IP version 4 (IPv4) address.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19

accounting-session-id-format

Syntax	accounting-session-id-format (decimal description);
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Configure the format the router uses to identify the accounting session.
Options	decimal—Use the decimal format. description—Use the generic format, in the form: <i>jnpr interface-specifier;subscriber-session-id</i> . Default: decimal
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19

accounting-stop-on-access-deny

Syntax	accounting-stop-on-access-deny;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Configure RADIUS accounting to send an Acct-Stop message when the AAA server denies a client access.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19

accounting-stop-on-failure

Syntax	accounting-stop-on-failure;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Configure RADIUS accounting to send an Acct-Stop message when client access fails AAA but the AAA server grants access.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19

active-server-group

Syntax	<code>active-server-group server-group-name;</code>
Hierarchy Level	<code>[edit forwarding-options dhcp-relay],</code> <code>[edit forwarding-options dhcp-relay group group-name],</code> <code>[edit logical-systems logical-system-name forwarding-options dhcp-relay],</code> <code>[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name],</code> <code>[edit logical-systems logical-system-name routing-instances routing-instance-name</code> <code>forwarding-options dhcp-relay],</code> <code>[edit logical-systems logical-system-name routing-instances routing-instance-name</code> <code>forwarding-options dhcp-relay group group-name],</code> <code>[edit routing-instances routing-instance-name forwarding-options dhcp-relay],</code> <code>[edit routing-instances routing-instance-name forwarding-options dhcp-relay group</code> <code>group-name]</code>
Release Information	Statement introduced in JUNOS Release 8.3.
Description	<p>Apply a DHCP relay agent configuration to the named group of DHCP server addresses.</p> <p>You can include the active-server-group statement at the <code>[edit forwarding-options dhcp-relay]</code> hierarchy level as a global DHCP relay agent configuration option, or at the <code>[edit forwarding-options dhcp-relay group group-name]</code> hierarchy level as a DHCP relay agent configuration option that applies only to a named group of interfaces.</p> <p>Including the active-server-group statement at the <code>[edit forwarding-options dhcp-relay group group-name]</code> hierarchy level as a group-specific option overrides use of the active-server-group statement at the <code>[edit forwarding-options dhcp-relay]</code> hierarchy level as a global option.</p>
Options	<i>server-group-name</i> —Name of the group of DHCP server addresses to which the DHCP relay agent configuration applies.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	■ Extended DHCP Relay Agent Overview on page 72

address-assignment

Syntax

```
address-assignment {
  pool pool-name family inet {
    network address-or-prefix</subnet-mask>;
    range range-name {
      low lower-limit high upper-limit;
    }
    host hostname {
      hardware-address mac-address;
      ip-address ip-address;
    }
    dhcp-attributes {
      [protocol-specific attributes]
    }
  }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced in JUNOS Release 9.0.

Description Configure address-assignment pools that can be used by different client applications.

Options *pool-name*—Name assigned to an address-assignment pool.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Topics ■ [Configuring Address-Assignment Pools on page 39](#)

always-write-giaddr

Syntax	always-write-giaddr;
Hierarchy Level	[edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides]
Release Information	Statement introduced in JUNOS Release 8.3.
Description	Overwrite the gateway IP address (giaddr) of every DHCP packet with the giaddr of the DHCP relay agent before forwarding the packet to the DHCP server.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Extended DHCP Local Server Overview on page 48

always-write-option-82

Syntax	always-write-option-82;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides]</p>
Release Information	Statement introduced in JUNOS Release 8.3.
Description	<p>Override the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server. The use of this option causes the DHCP relay agent to perform one of the following actions, depending on how it is configured:</p> <ul style="list-style-type: none"> ■ If the DHCP relay agent is configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the DHCP packets and inserts the new values before forwarding the packets to the DHCP server. ■ If the DHCP relay agent is not configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the packets, but does not add any new values before forwarding the packets to the DHCP server.
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Extended DHCP Local Server Overview on page 48

attributes

Syntax

```

attributes {
  ignore {
    framed-ip-netmask;
    input-filter;
    logical-system::routing-instance;
    output-filter;
  }
  exclude {
    accounting-authentic [ accounting-on | accounting-off ];
    accounting-delay-time [ accounting-on | accounting-off ];
    accounting-session-id [ access-request | accounting-on | accounting-off |
      accounting-stop ];
    accounting-terminate-cause [ accounting-off ];
    called-station-id [ access-request | accounting-start | accounting-stop ];
    calling-station-id [ access-request | accounting-start | accounting-stop ];
    class [ accounting-start | accounting-stop ];
    dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
    dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
    output-filter [ accounting-start | accounting-stop ];
    event-timestamp [ accounting-on | accounting-off | accounting-start | accounting-stop
      ];
    framed-ip-address [ accounting-start | accounting-stop ];
    framed-ip-netmask [ accounting-start | accounting-stop ];
    input-filter [ accounting-start | accounting-stop ];
    input-gigapackets [ accounting-stop ];
    input-gigawords [ accounting-stop ];
    interface-description [ access-request | accounting-start | accounting-stop ];
    nas-identifier [ access-request | accounting-on | accounting-off | accounting-start |
      accounting-stop ];
    nas-port [ access-request | accounting-start | accounting-stop ];
    nas-port-id [ access-request | accounting-start | accounting-stop ];
    nas-port-type [ access-request | accounting-start | accounting-stop ];
    output-gigapackets [ accounting-stop ];
    output-gigawords [ accounting-stop ];
  }
}

```

Hierarchy Level [edit access profile *profile-name* radius]

Release Information Statement introduced in JUNOS Release 9.1.

Description Specify how the router processes RADIUS attributes.

The statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Topics ■ Configuring How RADIUS Attributes Are Used for Subscriber Access on page 23

authentication

Syntax

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

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name],
[edit logical-systems logical-system-name system services dhcp-local-server],
[edit logical-systems logical-system-name system services dhcp-local-server group
group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name],
[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit routing-instances routing-instance-name system services dhcp-local-server group
group-name],
[edit system services dhcp-local-server],
[edit system services dhcp-local-server group group-name]
```

Release Information Statement introduced in JUNOS Release 9.1.

Description Configure the parameters the router sends to the external AAA server. A group configuration takes precedence over a global DHCP relay or DHCP local server configuration.

The statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Topics ■ Using External AAA Authentication Services with DHCP on page 53

authentication

Syntax

```
authentication {
  password password-string;
  username-include {
    circuit-type;
    delimiter delimiter-character;
    domain-name domain-name-string;
    logical-system-name;
    mac-address;
    option-60;
    option-82 [circuit-id] [remote-id];
    routing-instance-name;
    user-prefix user-prefix-string;
  }
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay group group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay],
[edit logical-systems logical-system-name forwarding-options group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name
 forwarding-options dhcp-relay],
[edit logical-systems logical-system-name routing-instances routing-instance-name
 forwarding-options dhcp-relay group group-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group
 group-name]
```

Release Information Statement introduced in JUNOS Release 9.1.


Description Configure the parameters the router sends to the external AAA server. A group configuration takes precedence over a global DHCP relay or DHCP local server configuration.

The statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Topics ■ Using External AAA Authentication Services with DHCP on page 53

authentication-order

Syntax	authentication-order [<i>authentication-methods</i>];
Hierarchy Level	[edit access profile <i>profile-name</i>]
Release Information	Statement introduced before JUNOS Release 7.4.
Description	Set the order in which the JUNOS software tries different authentication methods when verifying that a client can access the router. For each login attempt, the software tries the authentication methods in order, from first to last.
Options	<p>radius—Verify the client using RADIUS authentication services.</p> <p>password—Verify the client using the information configured at the [edit access profile <i>profile-name</i> client <i>client-name</i>] hierarchy level.</p>
<hr/> <div>  NOTE: The password keyword is not supported by the subscriber access management feature. </div> <hr/>	
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Specifying the Authentication and Accounting Methods for Subscriber Access on page 19

authentication-server

Syntax	authentication-server [<i>ip-address</i>];
Hierarchy Level	[edit access profile <i>profile-name</i> radius]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Specify a list of the RADIUS authentication servers used to authenticate DHCP, L2TP, and PPP clients. The servers in the list are also used as RADIUS dynamic-request servers, from which the router accepts and processes RADIUS disconnect requests, CoA requests, and dynamic service activations and deactivations.
Options	<i>ip-address</i> —The IPv4 address.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Configuring RADIUS Server Parameters for Subscriber Access on page 21

boot-file

Syntax	<code>boot-file filename;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Set the boot file advertised to DHCP clients. After the client receives an IP address and the boot file location from the DHCP server, the client uses the boot image stored in the boot file to complete DHCP setup. This is equivalent to DHCP option 67.
Options	<i>filename</i> —The location of the boot file on the boot server. The filename can include a pathname.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring Address-Assignment Pools on page 39 ■ boot-server

boot-server

Syntax	<code>boot-server (address hostname);</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Configure the name of the boot server advertised to DHCP clients. The client uses a boot file located on the boot server to complete DHCP setup. This is equivalent to DHCP option 66.
Options	<ul style="list-style-type: none"> ■ <i>address</i>—The IPv4 address of a boot server. ■ <i>hostname</i>—The fully qualified hostname of a boot server.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring Address-Assignment Pools on page 39 ■ boot-file

circuit-id

Syntax	circuit-id <i>value</i> range <i>named-range</i> ;
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> dhcp-attributes option-match option-82]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Configure the address-assignment pool <i>named-range</i> to use for a particular option 82 Agent Circuit ID value.
Options	<ul style="list-style-type: none">■ circuit-id <i>value</i>—The string for the Agent Circuit ID suboption (suboption 1) of the DHCP relay agent information option (option 82) in DHCP packets.■ range <i>named-range</i>—The name of the address-assignment pool range to use.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none">■ Configuring Address-Assignment Pools on page 39

circuit-id

Syntax	<pre>circuit-id { prefix host-name logical-system-name routing-instance-name; }</pre>
Hierarchy Level	<pre>[edit forwarding-options dhcp-relay relay-option-82], [edit forwarding-options dhcp-relay group group-name relay-option-82], [edit logical-systems logical-system-name forwarding-options dhcp-relay relay-option-82], [edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name relay-option-82], [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82], [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name relay-option-82], [edit routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82], [edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name relay-option-82]</pre>
Release Information	Statement introduced in JUNOS Release 8.3.
Description	<p>Include the agent-circuit-id suboption (suboption 1) of the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server.</p> <p>The format of the agent-circuit-id information for Fast Ethernet or Gigabit Ethernet interfaces that do not use virtual local area networks (VLANs) or stacked VLANs (S-VLANs) is as follows:</p> <pre>(fe ge)-fpc/pic/port</pre> <p>The format of the agent-circuit-id information for Fast Ethernet or Gigabit Ethernet interfaces that use VLANs is as follows:</p> <pre>(fe ge)-fpc/pic/port:vlan-id</pre> <p>The format of the agent-circuit-id information for Fast Ethernet or Gigabit Ethernet interfaces that use S-VLANs is as follows:</p> <pre>(fe ge)-fpc/pic/port:svlan-id-vlan-id</pre> <p>The remaining statement is explained separately.</p>
Required Privilege Level	<pre>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</pre>
Related Topics	<ul style="list-style-type: none"> ■ Extended DHCP Local Server Overview on page 48

circuit-type

Syntax circuit-type;

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit system services dhcp-local-server authentication username-include],
 [edit system services dhcp-local-server group *group-name* authentication username-include]

Release Information Statement introduced in JUNOS Release 9.1.

Description Specify that the circuit type is concatenated with the username during the subscriber authentication process.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Topics ■ Using External AAA Authentication Services with DHCP on page 53

circuit-type

Syntax	circuit-type;
Hierarchy Level	[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Specify that the circuit type is concatenated with the username during the subscriber authentication process.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Using External AAA Authentication Services with DHCP on page 53

client-discover-match

Syntax	client-discover-match;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit system services dhcp-local-server overrides],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> overrides]</p>
Release Information	Statement introduced in JUNOS Release 9.4.
Description	Configure DHCP local server to use option 60 and option 82 information to uniquely identify DHCP subscribers when primary subscriber identification fails.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Extended DHCP Local Server Overview on page 48 ■ Overriding Default DHCP Local Server Configuration Settings on page 56

client-discover-match

Syntax	client-discover-match;
Hierarchy Level	[edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides]
Release Information	Statement introduced in JUNOS Release 9.4.
Description	Configure DHCP relay to use option 60 and option 82 information to uniquely identify DHCP subscribers when primary subscriber identification fails.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Extended DHCP Relay Agent Overview on page 72 ■ Overriding the Default DHCP Relay Configuration on page 79

default-local-server-group

Syntax	default-local-server-group <i>local-server-group-name</i> ;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay relay-option-60 vendor-option],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay relay-option-60 vendor-option],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-60 vendor-option],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-60 vendor-option],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option]</p>
Release Information	Statement introduced in JUNOS Release 9.0.
Description	<p>Forward DHCP client packets to a default extended DHCP local server when you use the DHCP vendor class identifier option (option 60) in DHCP packets to forward client traffic to specific DHCP servers.</p> <p>If the option 60 string received in the DHCP client packet does not match the ASCII or hexadecimal match string and match criteria (exact match or partial match) that you specify, the extended DHCP relay agent forwards the client packets to the specified default DHCP local server group configured with the <code>dhcp-local-server</code> statement at the [edit system services] hierarchy level.</p>
Options	<i>local-server-group-name</i> —Name of the default extended DHCP local server group.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 87

default-relay-server-group

Syntax	default-relay-server-group <i>server-group-name</i> ;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay relay-option-60 vendor-option], [edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay relay-option-60 vendor-option], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-60 vendor-option], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-60 vendor-option], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option]</p>
Release Information	Statement introduced in JUNOS Release 9.0.
Description	<p>Relay DHCP client packets to a default group of extended DHCP relay servers when you use the DHCP vendor class identifier option (option 60) in DHCP packets to forward client traffic to specific DHCP servers.</p> <p>If the option 60 string received in the DHCP client packet does not match the ASCII or hexadecimal match string and match criteria (exact match or partial match) that you specify, the extended DHCP relay agent relays the client packets to the specified default group of servers configured with the server-group statement at the [edit forwarding-options dhcp-relay] hierarchy level.</p>
Options	<i>server-group-name</i> —Name of the default DHCP relay server group.
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 87

delimiter

Syntax `delimiter delimiter-character;`

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit system services dhcp-local-server authentication username-include],
 [edit system services dhcp-local-server group *group-name* authentication username-include]

Release Information Statement introduced in JUNOS Release 9.1.

Description Specify the character used as the delimiter between the concatenated components of the username. The semicolon (;) cannot be used as a delimiter.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Topics ■ Using External AAA Authentication Services with DHCP on page 53

delimiter

Syntax	<code>delimiter <i>delimiter-character</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]</p>
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Specify the character used as the delimiter between the concatenated components of the username. You cannot use the semicolon (;) as a delimiter.
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Using External AAA Authentication Services with DHCP on page 53

dhcp-attributes

Syntax

```
dhcp-attributes {
  option-match {
    option-82 {
      circuit-id value range named-range;
      remote-id value range named-range;
    }
  }
  boot-file filename;
  boot-server (address | hostname);
  domain-name domain-name;
  grace-period seconds;
  maximum-lease-time seconds;
  name-server [ server-list ];
  netbios-node-type node-type;
  option {
    [ (id-number option-type option-value)
      (id-number array option-type option-value) ];
  }
  router [ router-list ];
  tftp-server address;
  wins-server [ server-list ];
}
```

Hierarchy Level [edit access address-assignment pool *pool-name* family inet]

Release Information Statement introduced in JUNOS Release 9.0.

Description Configure address pools that can be used by different client applications.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Topics ■ [Configuring Address-Assignment Pools on page 39](#)

dhcp-local-server

```

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

```



```

        <match regex>;
        flag flag;
    }
}

```

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services],
 [edit logical-systems *logical-system-name* system services],
 [edit routing-instances *routing-instance-name* system services],
 [edit system services]

Release Information Statement introduced in JUNOS Release 9.0.

Description Configure Dynamic Host Configuration Protocol (DHCP) local server options on the router and enable the router to function as an extended DHCP local server. The DHCP local server receives DHCP request and reply packets from DHCP clients and then responds with an IP address and other optional configuration information to the client.

The DHCP local server supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication. You can configure dynamic profile and authentication support on a global basis or for a specific group of interfaces.

The DHCP local server also supports the use of JUNOS software address-assignment pools or external authorities, such as RADIUS, to provide the client address and configuration information.

The extended DHCP local server is incompatible with the J-series DHCP server and is not supported on the J-series Services Router. Also, the DHCP local server and the DHCP/BOOTP relay, which are configured under the [edit forwarding-options helpers] hierarchy level, cannot both be enabled on the router at the same time. The extended DHCP local server is fully compatible with the extended DHCP relay feature.



NOTE: When you configure the `dhcp-local-server` statement at the routing instance hierarchy level, you must use a routing instance type of virtual-router.

The statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Topics

- Extended DHCP Local Server Overview on page 48
- address-assignment
- dhcp-attributes

dhcp-relay

Syntax

```

dhcp-relay {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      logical-system-name;
      mac-address;
      option-60;
      option-82 [circuit-id] [remote-id];
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  dynamic-profile profile-name (aggregate-clients | use-primary primary-profile-name);
}
overrides {
  always-write-giaddr;
  always-write-option-82;
  client-discover-match;
  interface-client-limit number;
  layer2-unicast-replies;
  no-arp;
  trust-option-82;
  disable-relay;
}
relay-option-60 {
  vendor-option {
    (equals | starts-with) (ascii match-string | hexadecimal match-hex) {
      default-local-server-group local-server-group-name |
      (default-relay-server-group server-group-name |
      drop);
    }
    default-local-server-group local-server-group-name |
    (default-relay-server-group server-group-name |
    drop);
  }
}
relay-option-82 {
  circuit-id {
    prefix host-name logical-system-name routing-instance-name;
  }
}
server-group {
  server-group-name {
    server-ip-address;
  }
}
active-server-group server-group-name;
group group-name {

```



```

active-server-group server-group-name;
authentication {
    password password-string;
    username-include {
        circuit-type;
        delimiter delimiter-character;
        domain-name domain-name-string;
        logical-system-name;
        mac-address;
        option-60;
        option-82 [circuit-id] [remote-id];
        routing-instance-name;
        user-prefix user-prefix-string;
    }
}
dynamic-profile profile-name (aggregate-clients | use-primary primary-profile-name);
overrides {
    always-write-giaddr;
    always-write-option-82;
    client-discover-match;
    interface-client-limit number;
    layer2-unicast-replies;
    no-arp;
    trust-option-82;
    disable-relay;
}
relay-option-60 {
    vendor-option {
        (equals | starts-with) (ascii match-string | hexadecimal match-hex) {
            default-local-server-group local-server-group-name |
            (default-relay-server-group server-group-name |
            drop);
        }
        default-local-server-group local-server-group-name |
        (default-relay-server-group server-group-name |
        drop);
    }
}
relay-option-82 {
    circuit-id {
        prefix host-name logical-system-name routing-instance-name;
    }
}
interface interface-name [upto upto-interface-name] [exclude];
}
traceoptions {
    flag all;
    flag database;
    flag state;
    flag interface;
    flag rtsock;
    flag packet;
    flag packet-option;
    flag io;
    flag ha;
    flag ui;
}

```



```

flag general;
flag fwd;
flag rpd;
file file-name {
    <files number>;
    <size maximum-file-size>;
    <match regex>;
    <world-readable | no-world-readable>;
}
}
}

```

Hierarchy Level	[edit forwarding-options], [edit logical-systems <i>logical-system-name</i> forwarding-options], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options], [edit routing-instances <i>routing-instance-name</i> forwarding-options]
Release Information	Statement introduced in JUNOS Release 8.3. traceoptions option introduced in JUNOS Release 8.5. relay-option-60 option introduced in JUNOS Release 9.0. authentication option introduced in JUNOS Release 9.1.
Description	<p>Configure extended Dynamic Host Configuration Protocol (DHCP) relay options on the router and enable the router to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server.</p> <p>The DHCP relay supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication. You can attach dynamic profiles and configure authentication support on a global basis or for a specific group of interfaces.</p> <p>The extended DHCP relay agent options configured with the dhcp-relay statement are incompatible with the DHCP/BOOTP relay agent options configured with the bootp statement. As a result, the extended DHCP relay agent and the DHCP/BOOTP relay agent cannot both be enabled on the router at the same time.</p> <p>The statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Extended DHCP Local Server Overview on page 48 ■ Using External AAA Authentication Services with DHCP on page 53

disable-relay

Syntax	disable-relay;
Hierarchy Level	[edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides]
Release Information	Statement introduced in JUNOS Release 8.3.
Description	Disable DHCP relay on specific interfaces in a group.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Extended DHCP Relay Agent Overview on page 72

domain-name

Syntax	domain-name <i>domain-name</i> ;
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Configure the name of the domain in which clients search for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. This is equivalent to DHCP option 15.
Options	<i>domain-name</i> —Name of the domain.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	■ Configuring Address-Assignment Pools on page 39

domain-name

Syntax	<code>domain-name <i>domain-name-string</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication username-include]</p>
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Specify the domain name that is concatenated with the username during the subscriber authentication process.
Options	<i>domain-name-string</i> —The domain name formatted string.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Topics	■ Using External AAA Authentication Services with DHCP on page 53

domain-name

Syntax	<code>domain-name <i>domain-name-string</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]</p>
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Specify the domain name that is concatenated with the username during the subscriber authentication process.
Options	<i>domain-name-string</i> —The domain name formatted string.
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Using External AAA Authentication Services with DHCP on page 53

drop

Syntax drop;

Hierarchy Level [edit forwarding-options dhcp-relay relay-option-60 vendor-option],
 [edit forwarding-options dhcp-relay relay-option-60 vendor-option (equals | starts-with)
 (ascii *match-string* | hexadecimal *match-hex*)],
 [edit forwarding-options dhcp-relay relay-option-60 vendor-option],
 [edit forwarding-options dhcp-relay relay-option-60 vendor-option (equals | starts-with)
 (ascii *match-string* | hexadecimal *match-hex*)],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay relay-option-60
 vendor-option],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay relay-option-60
 vendor-option (equals | starts-with) (ascii *match-string* | hexadecimal *match-hex*)],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name*
 relay-option-60 vendor-option],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name*
 relay-option-60 vendor-option (equals | starts-with) (ascii *match-string* | hexadecimal
 match-hex)],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay relay-option-60 vendor-option],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay relay-option-60 vendor-option (equals | starts-with) (ascii
 match-string | hexadecimal *match-hex*)],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay group *group-name* relay-option-60 vendor-option],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay group *group-name* relay-option-60 vendor-option (equals
 | starts-with) (ascii *match-string* | hexadecimal *match-hex*)],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay relay-option-60
 vendor-option],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay relay-option-60
 vendor-option (equals | starts-with) (ascii *match-string* | hexadecimal *match-hex*)],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group
 group-name relay-option-60 vendor-option],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group
 group-name relay-option-60 vendor-option (equals | starts-with) (ascii *match-string* |
 hexadecimal *match-hex*)]

Release Information Statement introduced in JUNOS Release 9.0.

Description Drop (discard) DHCP client packets when you use the DHCP vendor class identifier option (option 60) in DHCP packets to forward client traffic to specific DHCP servers.

To drop DHCP client packets that contain an option 60 string that matches the ASCII or hexadecimal match string and match criteria (exact match or partial match) that you specify, include the drop statement at the [edit forwarding-options dhcp-relay relay-option-60 vendor-option (equals | starts-with) (ascii *match-string* | hexadecimal *match-hex*)] hierarchy level.

To drop DHCP client packets that contain an option 60 string that does *not* match the ASCII or hexadecimal match string and match criteria (exact match or partial

match) that you specify, include the **drop** statement at the [edit forwarding-options dhcp-relay relay-option-60 vendor-option] hierarchy level.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

- Related Topics** ■ Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 87

dynamic-profile

Syntax `dynamic-profile profile-name (aggregate-clients | use-primary primary-profile-name);`

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*],
 [edit logical-systems *logical-system-name* system services dhcp-local-server],
 [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name*],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*],
 [edit system services dhcp-local-server],
 [edit system services dhcp-local-server group *group-name*]

Release Information Statement introduced in JUNOS Release 9.2.
 aggregate-clients and use-primary options introduced in JUNOS Release 9.3.

Description Specify the dynamic profile that is attached to a group of interfaces or to all interfaces.
 The remaining statements are explained separately.

Options aggregate-clients—Enable multiple DHCP subscribers to share the same VLAN logical interface.

profile-name—Name of the dynamic profile.

use-primary *primary-profile-name*—Name of the dynamic profile to configure as the primary dynamic profile. The primary dynamic profile is instantiated when the first subscriber logs in. Subsequent subscribers are not assigned the primary dynamic profile; instead, they are assigned the dynamic profile specified for the interface. When the first subscriber logs out, the next subscriber that logs in is assigned the primary dynamic profile.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

- Related Topics** ■ Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 62

dynamic-profile

Syntax	<code>dynamic-profile <i>profile-name</i> (aggregate-clients use-primary <i>primary-profile-name</i>);</code>
Hierarchy Level	<pre>[edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay], [edit logical-systems <i>logical-system-name</i> forwarding-options group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i>]</pre>
Release Information	<p>Statement introduced in JUNOS Release 9.2.</p> <p><code>aggregate-clients</code> and <code>use-primary</code> options introduced in JUNOS Release 9.3.</p>
Description	Specify the dynamic profile that is attached to a group of interfaces or to all interfaces.
Options	<p><code>aggregate-clients</code>—Enable multiple DHCP subscribers to share the same VLAN logical interface.</p> <p><i>profile-name</i>—Name of the dynamic profile.</p> <p><code>use-primary <i>primary-profile-name</i></code>—Name of the dynamic profile to configure as the primary dynamic profile. The primary dynamic profile is instantiated when the first subscriber logs in. Subsequent subscribers are not assigned the primary dynamic profile; instead, they are assigned the dynamic profile specified for the interface. When the first subscriber logs out, the next subscriber that logs in is assigned the primary dynamic profile.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 62

ethernet-port-type-virtual

Syntax	ethernet-port-type-virtual;
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Specify the physical port type the router uses to authenticate clients. The port type is passed in RADIUS attribute 61 (NAS-Port-Type). This statement specifies a port type of virtual ; by default the router passes a port type of ethernet in RADIUS attribute 61.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	■ Configuring RADIUS Server Parameters for Subscriber Access on page 21

exclude

Syntax `exclude {
 accounting-authentic [accounting-on | accounting-off];
 accounting-delay-time [accounting-on | accounting-off];
 accounting-session-id [access-request | accounting-on | accounting-off | accounting-stop
];
 accounting-terminate-cause [accounting-off];
 called-station-id [access-request | accounting-start | accounting-stop];
 calling-station-id [access-request | accounting-start | accounting-stop];
 class [accounting-start | accounting-stop];
 dhcp-gi-address [access-request | accounting-start | accounting-stop];
 dhcp-mac-address [access-request | accounting-start | accounting-stop];
 output-filter [accounting-start | accounting-stop];
 event-timestamp [accounting-on | accounting-off | accounting-start | accounting-stop
];
 framed-ip-address [accounting-start | accounting-stop];
 framed-ip-netmask [accounting-start | accounting-stop];
 input-filter [accounting-start | accounting-stop];
 input-gigapackets [accounting-stop];
 input-gigawords [accounting-stop];
 interface-description [access-request | accounting-start | accounting-stop];
 nas-identifier [access-request | accounting-on | accounting-off | accounting-start |
 accounting-stop];
 nas-port [access-request | accounting-start | accounting-stop];
 nas-port-id [access-request | accounting-start | accounting-stop];
 nas-port-type [access-request | accounting-start | accounting-stop];
 output-gigapackets [accounting-stop];
 output-gigawords [accounting-stop];
 }`

Hierarchy Level [edit access profile *profile-name* radius attributes]

Release Information Statement introduced in JUNOS Release 9.1.

Description Configure the router to exclude the specified attributes from the specified type of RADIUS message.

Not all attributes are available in all types of RADIUS messages. By default, the router includes the specified attributes in RADIUS Access-Request, Acct-On, Acct-Off, Acct-Start, and Acct-Stop messages.

Options RADIUS attribute type—RADIUS attribute or Juniper Networks VSA number and name.

- accounting-authentic—RADIUS attribute 45, Acct-Authentic.
- accounting-delay-time—RADIUS attribute 41, Acct-Delay-Time.
- accounting-session-id—RADIUS attribute 44, Acct-Session-Id.
- accounting-terminate-cause—RADIUS attribute 49, Acct-Terminate-Cause.
- called-station-id—RADIUS attribute 30, Called-Station-Id.

- calling-station-id—RADIUS attribute 31, Calling-Station-Id.
- class—RADIUS attribute 25, Class.
- dhcp-gi-address—Juniper VSA 26-57, DHCP-GI-Address.
- dhcp-mac-address—Juniper VSA 26-56, DHCP-MAC-Address.
- event-timestamp—RADIUS attribute 55, Event-Timestamp.
- framed-ip-address—RADIUS attribute 8, Framed-IP-Address.
- framed-ip-netmask—RADIUS attribute 9, Framed-IP-Netmask.
- input-filter—Juniper VSA 26-10, Ingress-Policy-Name.
- input-gigapackets—Juniper VSA 26-42, Acct-Input-Gigapackets.
- input-gigawords—RADIUS attribute 52, Acct-Input-Gigawords.
- interface-description—Juniper VSA 26-53, Interface-Desc.
- nas-identifier—RADIUS attribute 32, NAS-Identifier.
- nas-port—RADIUS attribute 5, NAS-Port.
- nas-port-id—RADIUS attribute 87, NAS-Port-Id.
- nas-port-type—RADIUS attribute 61, NAS-Port-Type.
- output-filter—Juniper VSA 26-11, Egress-Policy-Name.
- output-gigapackets—Juniper VSA 25-43, Acct-Output-Gigapackets.
- output-gigawords—RADIUS attribute 53, Acct-Output-Gigawords.

RADIUS message type

- access-request—RADIUS Access-Accept messages.
- accounting-off—RADIUS Accounting-Off messages.
- accounting-on—RADIUS Accounting-On messages.
- accounting-start—RADIUS Accounting-Start messages.
- accounting-stop—RADIUS Accounting-Stop messages.

Required Privilege Level

admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

Related Topics ■ [Configuring RADIUS Server Parameters for Subscriber Access on page 21](#)

forwarding-class

Syntax forwarding-class *class-name*;

Hierarchy Level [edit services radius-flow-tap]

Release Information Statement introduced in JUNOS Release 9.4.

Description Specify forwarding class that is applied to mirrored packets sent to a mediation device.

Options *class-name*—Name of the forwarding class.

Required Privilege Level flow-tap—To view this statement in the configuration.
flow-tap-control—To add this statement to the configuration.

Related Topics ■ [Subscriber Secure Policy Overview on page 104](#)
■ [Configuring Subscriber Secure Policy Mirroring Overview on page 110](#)

grace-period

Syntax	<code>grace-period seconds;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Configure the amount of time that the client retains the address lease after the lease expires. The address cannot be reassigned to another client during the grace period.
Options	<p><i>seconds</i>—Number of seconds the lease is retained.</p> <p>Range: 0 through 4,294,967,295 seconds</p> <p>Default: 0 (no grace period)</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Configuring Address-Assignment Pools on page 39

group

Syntax `group group-name {
 authentication {
 option-60 password-string;
 username-include {
 circuit-type;
 delimiter delimiter-character;
 domain-name domain-name-string;
 logical-system-name;
 mac-address;
 option-60;
 option-82 <circuit-id> <remote-id>;
 routing-instance-name;
 user-prefix user-prefix-string;
 }
 }
 dynamic-profile profile-name (aggregate-clients | use-primary primary-profile-name);
 interface interface-name [upto upto-interface-name] [exclude];
 overrides {
 client-discover-match;
 interface-client-limit number;
 no-arp;
 }
}`

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server],
 [edit logical-systems *logical-system-name* system services dhcp-local-server],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server],
 [edit system services dhcp-local-server]

Release Information Statement introduced in JUNOS Release 9.0.

Description Configure a group of interfaces that have a common configuration, such as authentication parameters. A group must contain at least one interface.

Options *group-name*—Name of the group.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Topics

- Extended DHCP Local Server Overview on page 48
- Using External AAA Authentication Services with DHCP on page 53
- Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 62

group

Syntax

```
group group-name {
    active-server-group server-group-name;
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            mac-address;
            option-60;
            option-82 [circuit-id] [remote-id];
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    dynamic-profile profile-name (aggregate-clients | use-primary primary-profile-name);
    overrides {
        always-write-giaddr;
        always-write-option-82;
        client-discover-match;
        interface-client-limit number;
        layer2-unicast-replies;
        no-arp;
        trust-option-82;
        disable-relay;
    }
    relay-option-60 {
        vendor-option {
            (equals | starts-with) (ascii match-string | hexadecimal match-hex) {
                (default-relay-server-group server-group-name |
                 default-local-server-group local-server-group-name |
                 drop);
            }
            (default-relay-server-group server-group-name |
             default-local-server-group local-server-group-name |
             drop);
        }
    }
    relay-option-82 {
        circuit-id {
            prefix host-name logical-system-name routing-instance-name;
        }
    }
    interface interface-name [upto upto-interface-name] [exclude];
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit logical-systems logical-system-name forwarding-options dhcp-relay],
[edit logical-systems logical-system-name routing-instances routing-instance-name
 forwarding-options dhcp-relay],
```


[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay]

Release Information Statement introduced in JUNOS Release 8.3.

Description Specify the name of a group of interfaces that have a common DHCP relay agent configuration. A group must contain at least one interface.

The statements configured at the [edit forwarding-options dhcp-relay group *group-name*] hierarchy level apply only to the named group of interfaces, and override any global DHCP relay agent settings configured with the same statements at the [edit forwarding-options dhcp-relay] hierarchy level.

Options *group-name*—Name of a group of interfaces that have a common DHCP relay agent configuration.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Topics

- Extended DHCP Relay Agent Overview on page 72
- Using External AAA Authentication Services with DHCP on page 53
- Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 62

hardware-address

Syntax	hardware-address <i>mac-address</i> ;
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet host <i>hostname</i>]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Specify the MAC address of the client. This is the hardware address that identifies the client on the network.
Options	<i>mac-address</i> —The MAC address of the client.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	■ Configuring Address-Assignment Pools on page 39

host

Syntax	host <i>hostname</i> { hardware-address <i>mac-address</i> ; ip-address <i>ip-address</i> ; }
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Configure a static binding for the specified client.
Options	<i>hostname</i> —Name of the client. The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	■ Configuring Address-Assignment Pools on page 39

ignore

Syntax	ignore { framed-ip-netmask; input-filter; logical-system:routing-instance; output-filter; }
Hierarchy Level	[edit access profile <i>profile-name</i> radius attributes]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Configure the router to ignore the specified attributes in RADIUS Access-Accept messages. By default, the router processes the attributes it receives from the external server.
Options	framed-ip-netmask—Framed-IP-Netmask (RADIUS attribute 9). input-filter—Ingress-Policy-Name (VSA 26-10). logical-system:routing-instance—Virtual-Router (VSA 26-1). output-filter—Egress-Policy-Name (VSA 26-11).
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	■ Configuring RADIUS Server Parameters for Subscriber Access on page 21

immediate-update

Syntax	immediate-update;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Configure the router to send an Acct-Update message to the RADIUS accounting server on receipt of a response (for example, an ACK or timeout) to the Acct-Start message.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	■ Configuring RADIUS Server Parameters for Subscriber Access on page 21

interface

Syntax	interface <i>interface-name</i> [upto <i>upto-interface-name</i>] [exclude];
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i>], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i>], [edit system services dhcp-local-server group <i>group-name</i>]
Release Information	Statement introduced in JUNOS Release 9.0. upto and exclude options introduced in JUNOS Release 9.1.
Description	Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP local server is enabled. You can repeat the interface <i>interface-name</i> statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. Also, you cannot use an interface that is being used by the DHCP relay agent.
Options	<p>exclude—Exclude an interface or a range of interfaces from the group.</p> <p><i>interface-name</i>—The name of the interface. You can repeat this keyword multiple times.</p> <p><i>upto-interface-name</i>—The upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the <i>upto-interface-name</i> must be the same as the device name of the <i>interface-name</i>.</p>
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Extended DHCP Local Server Overview on page 48 ■ Using External AAA Authentication Services with DHCP on page 53

interface

Syntax	<code>interface <i>interface-name</i> [upto <i>upto-interface-name</i>] [exclude];</code>
Hierarchy Level	[edit forwarding-options dhcp-relay group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i>]
Release Information	Statement introduced in JUNOS Release 8.3. upto and exclude options introduced in JUNOS Release 9.1.
Description	Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP local server is enabled. You can repeat the interface <i>interface-name</i> statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. Also, you cannot use an interface that is being used by the DHCP relay agent.
Options	<p>exclude—Exclude an interface or a range of interfaces from the group.</p> <p><i>interface-name</i>—The name of the interface. You can repeat this keyword multiple times.</p> <p><i>upto-interface-name</i>—The upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the <i>upto-interface-name</i> must be the same as the device name of the <i>interface-name</i>.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Extended DHCP Relay Agent Overview on page 72 ■ Using External AAA Authentication Services with DHCP on page 53

interface-client-limit

Syntax	interface-client-limit <i>number</i> ;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit system services dhcp-local-server overrides],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> overrides]</p>
Release Information	Statement introduced in JUNOS Release 9.2.
Description	Sets the maximum number of DHCP subscribers per interface allowed for a specific group or for all groups. A group specification takes precedence over a global specification for the members of that group.
Options	<p><i>number</i>—Maximum number of clients allowed.</p> <p>Range: 1 through 500,000</p> <p>Default: No limit</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Extended DHCP Local Server Overview on page 48 ■ Overriding Default DHCP Local Server Configuration Settings on page 56

interface-client-limit

Syntax	interface-client-limit <i>number</i> ;
Hierarchy Level	[edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides]
Release Information	Statement introduced in JUNOS Release 9.2.
Description	Sets the maximum number of DHCP subscribers per interface allowed for a specific group or for all groups. A group specification takes precedence over a global specification for the members of that group.
Options	<i>number</i> —Maximum number of clients allowed. Range: 1 through 500,000 Default: No limit
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Extended DHCP Relay Agent Overview on page 72 ■ Overriding the Default DHCP Relay Configuration on page 79

interface-description-format

Syntax	interface-description-format [sub-interface adapter];
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Specifies the information that is included in or omitted from the interface description that the router passes to RADIUS for inclusion in the RADIUS attribute 87 (NAS-Port-Id). By default, the router includes both the subinterface and the adapter in the interface description.
Options	sub-interface—Specifies the subinterface. adapter—Specifies the adapter.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring RADIUS Server Parameters for Subscriber Access on page 21

interfaces

Syntax	interfaces <i>interface-name</i> ;
Hierarchy Level	[edit services radius-flow-tap]
Release Information	Statement introduced in JUNOS Release 9.4.
Description	Specify tunnel interfaces that are used to send mirrored packets to a mediation device.
Options	<i>interface-name</i> —Name of the interface.
Required Privilege Level	flow-tap—To view this statement in the configuration. flow-tap-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Subscriber Secure Policy Overview on page 104 ■ Configuring Subscriber Secure Policy Mirroring Overview on page 110

ip-address

Syntax	<code>ip-address <i>ip-address</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet host <i>hostname</i>]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Specify the reserved IP address assigned to the client.
Options	<i>ip-address</i> —The IP version 4 (IPv4) address.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none">■ Configuring Address-Assignment Pools on page 39■ Configuring Static Address Assignment on page 41

ip-address-first

Syntax	ip-address-first;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server pool-match-order], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order], [edit system services dhcp-local-server pool-match-order]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Configure the extended DHCP local server to use the IP address method to determine which address-assignment pool to use. The local server uses the IP address in the giaddr if one is present in the DHCP client PDU. If no giaddr is present, the local server uses the IP address of the receiving interface to find the address-assignment pool. The DHCP local server uses this method by default when no method is explicitly specified.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Topics	■ Extended DHCP Local Server Overview on page 48

layer2-unicast-replies

Syntax	layer2-unicast-replies;
Hierarchy Level	[edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides]
Release Information	Statement introduced in JUNOS Release 8.3.
Description	Override the setting of the broadcast bit in DHCP request packets and instead use the Layer 2 unicast transmission method to transmit DHCP Offer reply packets and DHCP ACK reply packets from the DHCP server to DHCP clients during the discovery process.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> Extended DHCP Relay Agent Overview on page 72

local-server-group

Syntax	<code>local-server-group <i>local-server-group-name</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay relay-option-60 vendor-option (equals starts-with) (ascii <i>match-string</i> hexadecimal <i>match-hex</i>)],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option (equals starts-with) (ascii <i>match-string</i> hexadecimal <i>match-hex</i>)],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay relay-option-60 vendor-option (equals starts-with) (ascii <i>match-string</i> hexadecimal <i>match-hex</i>)],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option (equals starts-with) (ascii <i>match-string</i> hexadecimal <i>match-hex</i>)],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-60 vendor-option (equals starts-with) (ascii <i>match-string</i> hexadecimal <i>match-hex</i>)],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option (equals starts-with) (ascii <i>match-string</i> hexadecimal <i>match-hex</i>)],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-60 vendor-option (equals starts-with) (ascii <i>match-string</i> hexadecimal <i>match-hex</i>)],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option (equals starts-with) (ascii <i>match-string</i> hexadecimal <i>match-hex</i>)]</p>
Release Information	Statement introduced in JUNOS Release 9.0.
Description	<p>Forward DHCP client packets to a specific extended DHCP local server when you use the DHCP vendor class identifier option (option 60) in DHCP packets to forward client traffic to specific DHCP servers.</p> <p>If the option 60 string received in the DHCP client packet matches the ASCII or hexadecimal match string and match criteria (exact match or partial match) that you specify, the extended DHCP relay agent forwards the client packets to the specified extended DHCP local server group configured with the <code>dhcp-local-server</code> statement at the [edit system services] hierarchy level.</p>
Options	<i>local-server-group-name</i> —Name of the extended DHCP local server group.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 87

logical-system-name

Syntax	logical-system-name;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]</p>
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Specify that the logical system name is concatenated with the username during the subscriber authentication process. No logical system name is concatenated if the configuration is in the default logical system.
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Using External AAA Authentication Services with DHCP on page 53

logical-system-name

Syntax logical-system-name;

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit system services dhcp-local-server authentication username-include],
 [edit system services dhcp-local-server group *group-name* authentication username-include]

Release Information Statement introduced in JUNOS Release 9.1.

Description Specify that the logical system name is concatenated with the username during the subscriber authentication process. No logical system name is concatenated if the configuration is in the default logical system.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Topics ■ Using External AAA Authentication Services with DHCP on page 53

mac-address

Syntax mac-address;

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit system services dhcp-local-server authentication username-include],
 [edit system services dhcp-local-server group *group-name* authentication username-include]

Release Information Statement introduced in JUNOS Release 9.1.

Description Specify that the MAC address from the client PDU is concatenated with the username during the subscriber authentication process.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Topics ■ Using External AAA Authentication Services with DHCP on page 53

mac-address

Syntax	mac-address;
Hierarchy Level	[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Specify that the MAC address from the client PDU be concatenated with the username during the subscriber authentication process.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Using External AAA Authentication Services with DHCP on page 53

maximum-lease-time

Syntax	maximum-lease-time <i>seconds</i> ;
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Specify the maximum length of time, in seconds, that the lease is held for a client if the client does not renew the lease. This is equivalent to DHCP option 51.
Options	<i>seconds</i> —The maximum number of seconds the lease can be held. Range: 30 through 4,294,967,295 seconds Default: 86,400 (24 hours)
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	■ Configuring Address-Assignment Pools on page 39

name-server

Syntax	name-server [<i>server-list</i>];
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Configure one or more Domain Name System (DNS) name servers available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.
Options	<i>server-list</i> —IP addresses of the domain name servers, listed in order of preference.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	■ Configuring Address-Assignment Pools on page 39

nas-identifier

Syntax	nas-identifier <i>identifier-value</i> ;
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Configure the value for the client RADIUS attribute 32 (NAS-Identifier). This attribute is used for authentication and accounting requests.
Options	<i>identifier-value</i> —A string in the range from 1 through 64 characters.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	■ Configuring RADIUS Server Parameters for Subscriber Access on page 21

nas-port-extended-format

Syntax nas-port-extended-format {
 adapter-width *width*;
 port-width *width*;
 slot-width *width*;
 stacked-vlan-width *width*;
 vlan-width *width*;
 }

Hierarchy Level [edit access profile *profile-name* radius options]

Release Information Statement introduced in JUNOS Release 9.1.

Description Configure the RADIUS client to use the extended format for RADIUS attribute 5 (NAS-Port) and specify the width of the fields in the NAS-Port attribute.

Options adapter-width *width*—Number of bits in the adapter field.

port-width *width*—Number of bits in the port field.

slot-width *width*—Number of bits in the slot field.

stacked-vlan-width *width*—Number of bits in the SVLAN ID field.

vlan-width *width*—Number of bits in the VLAN ID field.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

Related Topics ■ Configuring RADIUS Server Parameters for Subscriber Access on page 21

netbios-node-type

Syntax	<code>netbios-node-type <i>node-type</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Specify the NetBIOS node type. This is equivalent to DHCP option 46.
Options	<i>node-type</i> —You can specify one of the following node types: <ul style="list-style-type: none"> ■ <i>b-node</i>—Broadcast node ■ <i>h-node</i>—Hybrid node ■ <i>m-node</i>—Mixed node ■ <i>p-node</i>—Peer-to-peer node
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring Address-Assignment Pools on page 39

network

Syntax	<code>network <i>address-or-prefix</i></subnet-mask>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Configure subnet information for an address-assignment pool.
Options	<ul style="list-style-type: none"> ■ <i>address-or-prefix</i>—IP version 4 address or prefix value. ■ <i>subnet-mask</i>—Subnet mask.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring Address-Assignment Pools on page 39

no-arp

Syntax no-arp;

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server overrides],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* overrides],
 [edit logical-systems *logical-system-name* system services dhcp-local-server overrides],
 [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* overrides],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server overrides],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* overrides],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server overrides],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* overrides],
 [edit system services dhcp-local-server overrides],
 [edit system services dhcp-local-server group *group-name* overrides]

Release Information Statement introduced in JUNOS Release 9.3.**Description** Turn off ARP table population in a distrusted environment.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

no-arp

Syntax no-arp;

Hierarchy Level [edit forwarding-options dhcp-relay overrides],
 [edit forwarding-options dhcp-relay group *group-name* overrides],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay overrides],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* overrides],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides]

Release Information Statement introduced in JUNOS Release 9.3.**Description** Turn off ARP table population in a distrusted environment.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Topics

- Extended DHCP Relay Agent Overview on page 72
- Overriding the Default DHCP Relay Configuration on page 79

option

Syntax option {
 [(*id-number option-type option-value*)
 (*id-number array option-type option-value*)];
 }

Hierarchy Level [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

Release Information Statement introduced in JUNOS Release 9.0.

Description Specify user-defined options that are added to client packets.

Options *id-number*—Any whole number. The ID number is used to index the option and must be unique across a DHCP server.

option-type—Any of the following types: flag, byte, string, short, unsigned-short, integer, unsigned-integer, or ip-address.

array—An option can include an array of values.

option-value—Value associated with an option. The option value must be compatible with the option type (for example, an On or Off value for a flag type).

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

Related Topics ■ Configuring Address-Assignment Pools on page 39

option-60

Syntax	option-60;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication username-include]</p>
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Specify that the payload of Option 60 (Vendor Class Identifier) from the client PDU is concatenated with the username during the subscriber authentication process.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Using External AAA Authentication Services with DHCP on page 53

option-60

Syntax	option-60;
Hierarchy Level	[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Specify that the payload of the Option 60 (Vendor Class Identifier) from the client PDU is concatenated with the username during the subscriber authentication process.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Using External AAA Authentication Services with DHCP on page 53

option-82

Syntax option-82 {
 circuit-id *value range named-range*;
 remote-id *value range named-range*;
 }

Hierarchy Level [edit access address-assignment pool *pool-name* family inet dhcp-attributes option-match]

Release Information Statement introduced in JUNOS Release 9.0.

Description Specify the list of option 82 suboption match criteria used to select the named address range used for the client. The server matches the option 82 value in the user PDU to the specified option 82 match criteria and uses the named address range associated with the string.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

Related Topics ■ Configuring Address-Assignment Pools on page 39

option-82

Syntax option-82 <circuit-id> <remote-id>;

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit system services dhcp-local-server authentication username-include],
 [edit system services dhcp-local-server group *group-name* authentication username-include]

Release Information Statement introduced in JUNOS Release 9.1.

Description Specify the type of Option 82 information from the client PDU that is concatenated with the username during the subscriber authentication process. You can specify either, both, or neither of the Agent Circuit ID and Agent Remote ID suboptions. If you specify both, the Agent Circuit ID is supplied first, followed by a delimiter, and then the Agent Remote ID. If you specify that neither suboption is supplied, the raw payload of Option 82 from the PDU is concatenated to the username.

Options circuit-id—The string for the Agent Circuit ID suboption (suboption 1).

remote-id—The string for the Agent Remote ID suboption (suboption 2).

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Topics ■ Using External AAA Authentication Services with DHCP on page 53

option-82

Syntax	option-82;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server pool-match-order], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order], [edit system services dhcp-local-server pool-match-order]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Configure the extended DHCP local server to use the option 82 value in the DHCP client DHCP PDU together with the ip-address-first method to determine which address-assignment pool to use. You must configure the ip-address-first statement before configuring the option-82 statement. The DHCP local server first determines which address-assignment pool to use based on the ip-address-first method. Then, the local server matches the option 82 value in the client PDU with the option 82 configuration in the address-assignment pool.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Topics	■ Extended DHCP Local Server Overview on page 48

option-82

Syntax	option-82 <circuit-id> <remote-id>;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]</p>
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Specify the type of option 82 information from the client PDU that is concatenated with the username during the subscriber authentication process. You can specify either, both, or neither the agent circuit ID nor the agent remote ID suboptions. If you specify both, the agent circuit ID is supplied first, followed by a delimiter, and then the agent remote ID. If you specify that neither suboption is supplied, the raw payload of option 82 from the PDU is concatenated to the username.
Options	<p>circuit-id—The string for the agent circuit ID suboption (suboption 1).</p> <p>remote-id—The string for the agent remote ID suboption (suboption 2).</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	■ Using External AAA Authentication Services with DHCP on page 53

option-match

Syntax option-match {
 option-82 {
 circuit-id *value* range *named-range*;
 remote-id *value* range *named-range*;
 }
 }

Hierarchy Level [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

Release Information Statement introduced in JUNOS Release 9.0.

Description Specify a list of match criteria used to determine which named address range in the address-assignment pool to use. The extended DHCP local server matches this information to the match criteria specified in the client PDUs. For example, for option 82 match criteria, the server matches the option 82 value in the user PDU to the specified option 82 string and uses the named range associated with the string.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

Related Topics ■ Configuring Address-Assignment Pools on page 39

options

Syntax options {
 accounting-session-id-format (decimal | description);
 ethernet-port-type-virtual;
 interface-description-format [sub-interface | adapter];
 nas-identifier *identifier-value*;
 nas-port-extended-format {
 adapter-width *width*;
 port-width *width*;
 slot-width *width*;
 stacked-vlan-width *width*;
 vlan-width *width*;
 }
 override-nas-information;
 revert-interval *interval*;
 vlan-nas-port-stacked-format;
 }

Hierarchy Level [edit access profile *profile-name* radius]

Release Information Statement introduced in JUNOS Release 9.1.

Description Configure the options used by RADIUS authentication and accounting servers.
 The statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

Related Topics ■ Configuring RADIUS Server Parameters for Subscriber Access on page 21

order

Syntax	<code>order [accounting-method]</code>
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Set the order in which the JUNOS software tries different accounting methods for client activity. When a client logs in, the software tries the accounting methods in the specified order. RADIUS is the only method available at this release.
Options	<p><i>accounting-method</i>—One or more accounting methods. When a client logs in, the software tries the accounting methods in the following order, from first to last.</p> <ul style="list-style-type: none"> ■ <i>radius</i>—Use RADIUS accounting.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19

override-nas-information

Syntax	<code>override-nas-information;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Specify the information that the RADIUS client includes in broadcast accounting packets. By default, AAA broadcast accounting packets include the NAS-IP-Address and NAS-Identifier attributes of the <code>logical-system:routing-instance</code> that generates the accounting information. This statement configures the RADIUS client to override the default behavior and include RADIUS attribute 4 (NAS-IP-Address) and RADIUS attribute 32 (NAS-Identifier) of the <code>logical-system:routing-instance</code> that authenticates the client.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Configuring RADIUS Server Parameters for Subscriber Access on page 21

overrides

Syntax overrides {
 client-discover-match;
 interface-client-limit *number*;
 no-arp;
 }

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*],
 [edit logical-systems *logical-system-name* system services dhcp-local-server],
 [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name*],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*],
 [edit system services dhcp-local-server],
 [edit system services dhcp-local-server group *group-name*]

Release Information Statement introduced in JUNOS Release 9.2.

Description Override the default configuration settings for the extended DHCP local server. Specifying the **overrides** statement with no subordinate statements removes all DHCP local server overrides at that hierarchy level.

To override global DHCP local server configuration options, include the **overrides** statement and its subordinate statements at the [edit system services dhcp-local-server] hierarchy level. To override DHCP relay agent configuration options for a named group of interfaces, include the statements at the [edit system services dhcp-local-server group *group-name*] hierarchy level.

The statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Topics ■ Extended DHCP Local Server Overview on page 48
 ■ Overriding Default DHCP Local Server Configuration Settings on page 56

overrides

Syntax overrides {
 always-write-giaddr;
 always-write-option-82;
 client-discover-match;
 interface-client-limit *number*;
 layer2-unicast-replies;
 no-arp;
 trust-option-82;
 disable-relay;
 }

Hierarchy Level [edit forwarding-options dhcp-relay],
 [edit forwarding-options dhcp-relay group *group-name*],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name*],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay group *group-name*],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group
 group-name]

Release Information Statement introduced in JUNOS Release 8.3.

Description Override the default configuration settings for the extended DHCP relay agent. Specifying the **overrides** statement with no subordinate statements removes all DHCP relay agent overrides at that hierarchy level.

To override global DHCP relay agent configuration options, include the **overrides** statement and its subordinate statements at the [edit forwarding-options dhcp-relay] hierarchy level. To override DHCP relay agent configuration options for a named group of interfaces, include the statements at the [edit forwarding-options dhcp-relay group *group-name*] hierarchy level.

The statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Topics ■ Extended DHCP Relay Agent Overview on page 72

password

Syntax	<code>password <i>password-string</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication],</p> <p>[edit system services dhcp-local-server authentication],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication]</p>
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Configure the password that is sent to the external AAA authentication server for subscriber authentication.
Options	<i>password-string</i> —Authentication password.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Topics	■ Using External AAA Authentication Services with DHCP on page 53

password

Syntax	<code>password <i>password-string</i>;</code>
Hierarchy Level	[edit forwarding-options dhcp-relay authentication], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Configure the password that is sent to the external AAA authentication server for subscriber authentication.
Options	<i>password-string</i> —Authentication password.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Using External AAA Authentication Services with DHCP on page 53

pool

Syntax	<code>pool <i>pool-name</i>;</code>
Hierarchy Level	[edit access address-assignment]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Configure the name of an address-assignment pool.
Options	<i>pool-name</i> —The name assigned to the address-assignment pool.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring Address-Assignment Pools on page 39

pool-match-order

Syntax	pool-match-order { ip-address-first; option-82; }
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server], [edit system services dhcp-local-server]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Configure the order in which the DHCP local server uses information in the DHCP client PDU to determine how to obtain an address for the client. By default, the DHCP local server uses the ip-address-first method to determine which address pool to use. The statements are explained separately.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Topics	■ Extended DHCP Local Server Overview on page 48

port

Syntax	port <i>port-number</i> ;
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
Release Information	Statement introduced before JUNOS Release 7.4.
Description	Configure the port number on which to contact the RADIUS server.
Options	<i>port-number</i> —Port number on which to contact the RADIUS server. Default: 1812 (as specified in RFC 2865)
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Topics	■ Router Interaction with RADIUS Servers Overview on page 18 ■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19

prefix

Syntax	prefix host-name logical-system-name routing-instance-name;
Hierarchy Level	[edit forwarding-options dhcp-relay relay-option-82 circuit-id], [edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-82 circuit-id], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay relay-option-82 circuit-id], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-82 circuit-id], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-82 circuit-id], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-82 circuit-id], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-82 circuit-id], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-82 circuit-id]
Release Information	Statement introduced in JUNOS Release 8.3.
Description	Add a prefix to the base option 82 agent-circuit-id information in DHCP packets destined for a DHCP server. The prefix can consist of any combination of the hostname, logical system name, and routing instance name.

If you include only the hostname, only the logical system name, or only the routing instance name in the prefix, the format of the agent-circuit-id information for Fast Ethernet or Gigabit Ethernet interfaces with stacked virtual LANs (S-VLANs) is one of the following:

```
host-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
logical-system-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

If you include both the logical system name and the routing instance name in the prefix, the format of the agent-circuit-id information for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs is as follows:

```
logical-system-name;routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

If you include the hostname, logical system name, and routing instance name in the prefix, the format of the agent-circuit-id information for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs is as follows:

```
host-name/logical-system-name;routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

For Fast Ethernet or Gigabit Ethernet interfaces that use virtual LANs (VLANs) but not S-VLANs, only the *vlan-id* value appears in the agent-circuit-id format. For Fast Ethernet or Gigabit Ethernet interfaces that do not use VLANs or S-VLANs, neither the *vlan-id* value nor the *svlan-id* value appears.

Options **host-name**—Prepend the hostname of the router configured with the **host-name** statement at the **[edit system]** hierarchy level to the agent-circuit-id information.

logical-system-name—Prepend the name of the logical system to the agent-circuit-id information.

routing-instance-name—Prepend the name of the routing instance to the agent-circuit-id information.

Required Privilege Level **interface**—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Topics ■ [Extended DHCP Relay Agent Overview on page 72](#)

profile

Syntax `profile profile-name {`

```

authentication-order [ authentication-methods ];
accounting {
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    order [ accounting-method ];
    statistics (time | volume-time);
    update-interval minutes;
}
radius {
    authentication-server [ ip-address ];
    accounting-server [ ip-address ];
    options {
        accounting-session-id-format (decimal | description);
        ethernet-port-type-virtual;
        interface-description-format [sub-interface | adapter];
        nas-identifier identifier-value;
        nas-port-extended-format {
            adapter-width width;
            port-width width;
            slot-width width;
            stacked-vlan-width width;
            vlan-width width;
        }
        override-nas-information;
        revert-interval interval;
        vlan-nas-port-stacked-format;
    }
}
attributes {
    ignore {
        framed-ip-netmask;
        input-filter;
        logical-system:routing-instance;
        output-filter;
    }
}
exclude
    accounting-authentic [ accounting-on | accounting-off ];
    accounting-delay-time [ accounting-on | accounting-off ];
    accounting-session-id [ access-request | accounting-on | accounting-off |
        accounting-stop ];
    accounting-terminate-cause [ accounting-off ];
    called-station-id [ access-request | accounting-start | accounting-stop ];
    calling-station-id [ access-request | accounting-start | accounting-stop ];
    class [ accounting-start | accounting-stop ];
    dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
    dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
    output-filter [ accounting-start | accounting-stop ];
    event-timestamp [ accounting-on | accounting-off | accounting-start |
        accounting-stop ];
    framed-ip-address [ accounting-start | accounting-stop ];
    framed-ip-netmask [ accounting-start | accounting-stop ];

```



```

        input-filter [ accounting-start | accounting-stop ];
        input-gigapackets [ accounting-stop ];
        input-gigawords [ accounting-stop ];
        interface-description [ access-request | accounting-start | accounting-stop ];
        nas-identifier [ access-request | accounting-on | accounting-off | accounting-start
            | accounting-stop ];
        nas-port [ access-request | accounting-start | accounting-stop ];
        nas-port-id [ access-request | accounting-start | accounting-stop ];
        nas-port-type [ access-request | accounting-start | accounting-stop ];
        output-gigapackets [ accounting-stop ];
        output-gigawords [ accounting-stop ];
    }
}
radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
    secret password;
    timeout source-address;
    timeout seconds;
}
}

```

Hierarchy Level [edit access]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure an access profile and its subscriber access properties.

The remaining statements are explained separately.



NOTE: This topic describes the **profile** statement options for subscriber access management. See the *JUNOS System Basics Configuration Guide* for a complete description of the **profile** statement.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Topics ■ AAA Service Framework Overview on page 17

radius

```

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

```



```

        output-gigapackets [ accounting-stop ];
        output-gigawords [ accounting-stop ];
    }
}

```

Hierarchy Level [edit access profile *profile-name*]

Release Information Statement introduced in JUNOS Release 9.1.

Description Configure the RADIUS parameters that the router uses for AAA authentication and accounting for subscribers.

The statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Topics ■ Configuring RADIUS Server Parameters for Subscriber Access on page 21

radius-flow-tap

Syntax radius-flow-tap {
 forwarding-class *class-name*;
 interfaces *interface-name*;
 source-ipv4-address *ipv4-address*;
}

Hierarchy Level [edit services]

Release Information Statement introduced in JUNOS Release 9.4.

Description Assign parameters that are used with subscriber secure policy mirroring.

The remaining statements are explained separately.

Required Privilege Level flow-tap—To view this statement in the configuration.
flow-tap-control—To add this statement to the configuration.

Related Topics ■ Subscriber Secure Policy Overview on page 104
■ Configuring Subscriber Secure Policy Mirroring Overview on page 110

radius-server

Syntax `radius-server server-address {
 accounting-port port-number;
 port port-number;
 retry attempts;
 routing-instance routing-instance-name;
 secret password;
 source-address source-address;
 timeout seconds;
 }`

Hierarchy Level [edit access],
 [edit access profile *profile-name*]

Release Information Statement introduced before JUNOS Release 7.4.

Description Configure RADIUS for subscriber access management, L2TP, or PPP.

To configure multiple RADIUS servers, include multiple **radius-server** statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.



NOTE: This topic describes the **radius-server** statement options for subscriber access management. See the *JUNOS System Basics Configuration Guide* for a complete description of the **radius-server** statement.

Options `server-address`—Address of the RADIUS authentication server.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Topics ■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19

range

Syntax `range range-name {
 low lower-limit high upper-limit;
 }`

Hierarchy Level [edit access address-assignment pool *pool-name* family inet]

Release Information Statement introduced in JUNOS Release 9.0.

Description Configure a named address range used within an address-assignment pool.

Options *range-name*—The name assigned to the range of addresses.

 low *lower-limit*—The lower limit of an address range.

 high *upper-limit*—The upper limit of an address range.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

Related Topics ■ Configuring Address-Assignment Pools on page 39

relay-option-60

Syntax

```

relay-option-60 {
  vendor-option {
    (equals | starts-with) (ascii match-string | hexadecimal match-hex) {
      (relay-server-group server-group-name |
        local-server-group local-server-group-name |
        drop);
    }
    (default-relay-server-group server-group-name |
      default-local-server-group local-server-group-name |
      drop);
  }
}
```

Hierarchy Level

```

[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay group group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay],
[edit logical-systems logical-system-name routing-instances routing-instance-name
  forwarding-options dhcp-relay group group-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group
  group-name]
```

Release Information Statement introduced in JUNOS Release 9.0.

Description Configure the extended DHCP relay agent to use the DHCP vendor class identifier option (option 60) in DHCP client packets to forward client traffic to specific DHCP servers, or to drop selected DHCP client packets. This feature is useful in network environments where DHCP clients access services provided by multiple vendors and DHCP servers.

You can use the **relay-option-60** statement and its subordinate statements at the **[edit forwarding-options dhcp-relay]** hierarchy level to configure option 60 support globally, or at the **[edit forwarding-options dhcp-relay group *group-name*]** hierarchy level to configure option 60 support for a named group of interfaces. You can also configure option 60 support for the extended DHCP relay agent on a per logical system and per routing instance basis.

The statements are explained separately.

Required Privilege Level

```

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
```

Related Topics

- Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 87

relay-option-82

Syntax relay-option-82 {
 circuit-id {
 prefix host-name logical-system-name routing-instance-name;
 }
 }

Hierarchy Level [edit forwarding-options dhcp-relay],
 [edit forwarding-options dhcp-relay group *group-name*],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name*],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay group *group-name*],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group
 group-name]

Release Information Statement introduced in JUNOS Release 8.3.

Description Enable or disable the insertion of the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server.

If you enable insertion of option 82 information in DHCP packets, you must specify at least the **circuit-id** statement to include the agent-circuit-id suboption (suboption 1) of the DHCP relay agent information option. Optionally, you can also specify the **prefix** statement to add a prefix to the base option 82 information that consists of any combination of the hostname, logical system name, and routing instance name. Specifying the **relay-option-82** statement with no subordinate statements disables insertion of option 82 information in DHCP packets, which is the default behavior.

You can use the **relay-option-82** statement and its subordinate statements at the [edit forwarding-options dhcp-relay] hierarchy level to control insertion of option 82 information globally, or at the [edit forwarding-options dhcp-relay group *group-name*] hierarchy level to control insertion of option 82 information for a named group of interfaces.

The statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Topics ■ Enabling and Disabling Insertion of Option 82 Information on page 91

relay-server-group

Syntax	<code>relay-server-group server-group-name;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay relay-option-60 vendor-option (equals starts-with) (ascii <i>match-string</i> hexadecimal <i>match-hex</i>)],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option (equals starts-with) (ascii <i>match-string</i> hexadecimal <i>match-hex</i>)],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay relay-option-60 vendor-option (equals starts-with) (ascii <i>match-string</i> hexadecimal <i>match-hex</i>)],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option (equals starts-with) (ascii <i>match-string</i> hexadecimal <i>match-hex</i>)],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-60 vendor-option (equals starts-with) (ascii <i>match-string</i> hexadecimal <i>match-hex</i>)],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option (equals starts-with) (ascii <i>match-string</i> hexadecimal <i>match-hex</i>)],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-60 vendor-option (equals starts-with) (ascii <i>match-string</i> hexadecimal <i>match-hex</i>)],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option (equals starts-with) (ascii <i>match-string</i> hexadecimal <i>match-hex</i>)]</p>
Release Information	Statement introduced in JUNOS Release 9.0.
Description	<p>Relay DHCP client packets to the specified group of extended DHCP relay servers when you use the DHCP vendor class identifier option (option 60) in DHCP packets to forward client traffic to specific DHCP servers.</p> <p>If the option 60 string received in the DHCP client packet matches the ASCII or hexadecimal match string and match criteria (exact match or partial match) that you specify, the extended DHCP relay agent relays the client packets to the specified group of servers configured with the server-group statement at the [edit forwarding-options dhcp-relay] hierarchy level. A server group can contain multiple server addresses and can map to more than one ASCII or hexadecimal match string.</p>
Options	<i>server-group-name</i> —Name of the extended DHCP relay server group.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 87

remote-id

Syntax	<code>remote-id value range named-range;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes option-match option-82]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Specify the address-assignment pool named range to use based on the particular option 82 Agent Remote ID value.
Options	<p><i>remote-id value</i>—The string for Agent Remote ID suboption (suboption 2) of the DHCP relay agent information option (option 82) in DHCP packets.</p> <p><i>range named-range</i>—Name of the address-assignment pool range to use.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Configuring Address-Assignment Pools on page 39

retry

Syntax	<code>retry attempts;</code>
Hierarchy Level	<p>[edit access radius-server <i>server-address</i>],</p> <p>[edit access profile <i>profile-name</i> radius-server <i>server-address</i>]</p>
Release Information	Statement introduced before JUNOS Release 7.4.
Description	Number of times that the router is allowed to attempt to contact a RADIUS authentication or accounting server.
Options	<p><i>attempts</i>—Number of times that the router is allowed to attempt to contact a RADIUS server.</p> <p>Range: 1 through 10</p> <p>Default: 3</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19 ■ Router Interaction with RADIUS Servers Overview on page 18 ■ timeout

revert-interval

Syntax	<code>revert-interval <i>interval</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Configure the amount of time the router waits after a server has become unreachable. The router rechecks the connection to the server when the revert-interval expires. If the server is then reachable, it is used in accordance with the order of the server list.
Options	<i>interval</i> —Amount of time to wait. Range: 60 through 4294967295 seconds Default: 3 seconds
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19

router

Syntax	<code>router [<i>hostnames</i>];</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Specify a list of the routers located on the client's subnet. This statement is the equivalent of DHCP option 3.
Options	<i>router-list</i> —IP addresses of the routers.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring Address-Assignment Pools on page 39

routing-instance

Syntax	<code>routing-instance <i>routing-instance-name</i>;</code>
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
Release Information	Statement introduced before JUNOS Release 7.4.
Description	Configure the routing instance used to send RADIUS packets to the RADIUS server.
Options	<i>routing-instance-name</i> —Routing instance name.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Topics	■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19

routing-instance-name

Syntax routing-instance-name;

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit logical-systems *logical-system-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server authentication username-include],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication username-include],
 [edit system services dhcp-local-server authentication username-include],
 [edit system services dhcp-local-server group *group-name* authentication username-include]

Release Information Statement introduced in JUNOS Release 9.1.

Description Specify that the routing instance name is concatenated with the username during the subscriber authentication process. No routing instance name is concatenated if the configuration is in the default routing instance.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Topics ■ Using External AAA Authentication Services with DHCP on page 53

routing-instance-name

Syntax	routing-instance-name;
Hierarchy Level	[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Specify that the routing instance name is concatenated with the username during the subscriber authentication process. No routing instance name is concatenated if the configuration is in the default routing instance.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Using External AAA Authentication Services with DHCP on page 53

secret

Syntax	secret <i>password</i> ;
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
Release Information	Statement introduced before JUNOS Release 7.4.
Description	Configure the password to use with the RADIUS server. The secret password used by the local router must match that used by the server.
Options	<i>password</i> —Password to use; can include spaces.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Topics	■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19 ■ Router Interaction with RADIUS Servers Overview on page 18

server-group

Syntax	<pre>server-group { server-group-name { server-ip-address; } }</pre>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay]</p>
Release Information	Statement introduced in JUNOS Release 8.3.
Description	Specify the name of a group of DHCP server addresses for use by the extended DHCP relay agent.
Options	<p><i>server-group-name</i>—Name of the group of DHCP server addresses.</p> <p><i>server-ip-address</i>—IP address of the DHCP server belonging to this named server group. You can configure a maximum of five IP addresses per named server group.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> Extended DHCP Relay Agent Overview on page 72

source-address

Syntax	source-address <i>source-address</i> ;
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
Release Information	Statement introduced before JUNOS Release 7.4.
Description	Configure a source address for each configured RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address.
Options	<i>source-address</i> —A valid IPv4 address configured on one of the router interfaces. On M-series routers only, the source address can be an IPv6 address and the UDP source port is 514.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Router Interaction with RADIUS Servers Overview on page 18 ■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19

source-ipv4-address

Syntax	source-ipv4-address <i>ipv4-address</i> ;
Hierarchy Level	[edit services radius-flow-tap]
Release Information	Statement introduced in JUNOS Release 9.4.
Description	Specify the source IP address used in the IP header that is prepended to mirrored packets sent to a mediation device.
Options	<i>ipv4-address</i> —IPv4 address.
Required Privilege Level	flow-tap—To view this statement in the configuration. flow-tap-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Subscriber Secure Policy Overview on page 104 ■ Configuring Subscriber Secure Policy Mirroring Overview on page 110

statistics

Syntax	statistics (time volume-time);
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in JUNOS Release 9.1. volume-time option introduced in JUNOS Release 9.4.
Description	Configure the router to collect time statistics or both volume and time statistics for the sessions being managed by AAA.
Options	time—Collect uptime statistics only. volume-time—Collect both volume and uptime statistics. This option is not available for Mobile IP.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Mobile IP Home Agent Elements and Behavior on page 243 ■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19

tftp-server

Syntax	<code>tftp-server ip-address;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Specify the Trivial File Transfer Protocol (TFTP) server that the client uses to obtain the client configuration file. This is equivalent to DHCP option 150.
Options	<i>ip-address</i> —IP address of the TFTP server.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	■ Configuring Address-Assignment Pools on page 39

timeout

Syntax	<code>timeout seconds;</code>
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
Release Information	Statement introduced before JUNOS Release 7.4.
Description	Configure the amount of time that the local router waits to receive a response from a RADIUS server.
Options	<i>seconds</i> —Amount of time to wait. Range: 1 through 90 seconds Default: 3 seconds
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Topics	■ Router Interaction with RADIUS Servers Overview on page 18 ■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19

traceoptions

Syntax traceoptions {
 file *file-name* <files *number*> <size *size*> <world-readable | no-world-readable> <match
 regex>;
 flag *flag*;
 }

Hierarchy Level [edit system processes general-authentication-service]

Release Information Flag for tracing address-assignment pool operations introduced in JUNOS Release 9.0.
 option-name option introduced in JUNOS Release 8.3.

Description Configure tracing options.

Options file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory */var/log*.

files *number*—(Optional) Maximum number of trace files. When a trace file named *trace-file* reaches its maximum size, it is renamed *trace-file.0*, then *trace-file.1*, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the *size* option and a filename.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple *flag* statements. You can include the following flags:

- address-assignment—All address-assignment events
- all—All tracing operations
- configuration—Configuration events
- framework—Authentication framework events
- ldap—LDAP authentication events
- local-authentication—Local authentication events
- radius—RADIUS authentication events

match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the *files* option and filename.

Syntax: *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

Related Topics ■ [Tracing Address-Assignment Pool Processes on page 43](#)

traceoptions

Syntax	<pre>traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>> <world-readable no-world-readable> <match <i>regex</i>>; flag <i>flag</i>; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server],</p> <p>[edit system services dhcp-local-server]</p>
Release Information	Statement introduced in JUNOS Release 9.0.
Description	Define tracing operations for DHCP processes.
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory <code>/var/log</code>.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named <code>trace-file</code> reaches its maximum size, it is renamed <code>trace-file.0</code>, then <code>trace-file.1</code>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the <code>size</code> option and a filename.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple <code>flag</code> statements. You can include the following flags:</p> <ul style="list-style-type: none"> ■ all—Trace all operations. ■ auth—Trace authentication operations. ■ database—Trace database events. ■ fwd—Trace firewall process events. ■ general—Trace miscellaneous events. ■ ha—Trace high availability-related events. ■ interface—Trace interface operations. ■ io—Trace I/O operations. ■ packet—Trace packet decoding operations. ■ packet-option—Trace DHCP option decoding operations. ■ rpd—Trace routing protocol process events.

- **rtsock**—Trace routing socket operations.
- **session-db**—Trace session database operations.
- **state**—Trace changes in state.
- **ui**—Trace user interface operations.

match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the trace-file again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten. If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and filename.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Related Topics ■ Tracing Extended DHCP Operations on page 66

traceoptions

Syntax traceoptions {
 file *file-name* <files *number*> <size *size*> <world-readable | no-world-readable> <match
 regex>;
 flag *flag*;
 }

Hierarchy Level [edit forwarding-options dhcp-relay],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay]

Release Information Statement introduced in JUNOS Release 8.5.

Description Configure tracing operations for extended DHCP relay agent processes.

Default If you do not include this statement, no tracing operations are performed.

Options *file-name*—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (“ ”). All files are placed in a file named **jdhcpd** in the directory **/var/log**. If you include the **file** statement, you must specify a filename.

files number—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000

Default: 3 files

flag flag—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all events
- **auth**—Trace authentication events
- **database**—Trace database events
- **fwd**—Trace firewall process events
- **general**—Trace miscellaneous events
- **ha**—Trace high availability-related events
- **interface**—Trace interface operations
- **io**—Trace I/O operations
- **packet**—Trace packet decoding operations

- **packet-option**—Trace DHCP option decoding operations
- **rpd**—Trace routing protocol process events
- **rtsock**—Trace routing socket operations
- **session-db**—Trace session database operations
- **state**—Trace changes in state
- **ui**—Trace user interface operations

match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** file again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and filename.

Syntax: *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB

Range: 0 bytes through 4,294,967,295 KB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Related Topics ■ [Tracing Extended DHCP Operations on page 66](#)

trust-option-82

Syntax `trust-option-82;`

Hierarchy Level [edit forwarding-options dhcp-relay overrides],
 [edit forwarding-options dhcp-relay group *group-name* overrides],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay overrides],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* overrides],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay overrides],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* overrides]

Release Information Statement introduced in JUNOS Release 8.3.

Description Enable processing of DHCP client packets that have a gateway IP address (giaddr) of 0 (zero) and contain option 82 information. By default, the DHCP relay agent treats such packets as if they originated at an untrusted source, and drops them without further processing.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Topics ■ [Extended DHCP Relay Agent Overview on page 72](#)

update-interval

Syntax	update-interval <i>minutes</i> ;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Configure the amount of time, in minutes, that the router waits before sending a new accounting update.
Options	<i>minutes</i> —Amount of time between updates, in minutes. Range: 15 through 1440 minutes Default: no updates
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19

username-include

Syntax username-include {
 circuit-type;
 delimiter *delimiter-character*;
 domain-name *domain-name-string*;
 logical-system-name;
 mac-address;
 option-60;
 option-82 <circuit-id> <remote-id>;
 routing-instance-name;
 user-prefix *user-prefix-string*;
 }

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication],
 [edit logical-systems *logical-system-name* system services dhcp-local-server authentication],
 [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* authentication],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server authentication],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server authentication],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* authentication],
 [edit system services dhcp-local-server authentication],
 [edit system services dhcp-local-server group *group-name* authentication]

Release Information Statement introduced in JUNOS Release 9.1.

Description Configure the username that the router passes to the external AAA server. You must include at least one of the optional statements for the username to be valid. If you do not configure a username, the router accesses the local authentication service only and does not use external authentication services, such as RADIUS.

The statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Topics ■ Using External AAA Authentication Services with DHCP on page 53

username-include

Syntax username-include {
 circuit-type;
 delimiter *delimiter-character*;
 domain-name *domain-name-string*;
 logical-system-name;
 mac-address;
 option-60;
 option-82 <circuit-id> <remote-id>;
 routing-instance-name;
 user-prefix *user-prefix-string*;
 }

Hierarchy Level [edit forwarding-options dhcp-relay authentication],
 [edit forwarding-options dhcp-relay group *group-name* authentication],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay authentication],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name*
 authentication],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay authentication],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay group *group-name* authentication],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay authentication],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group
 group-name authentication]

Release Information Statement introduced in JUNOS Release 9.1.

Description Configure the username that the router passes to the external AAA server. You must include at least one of the optional statements for the username to be valid. If you do not configure a username, the router accesses the local authentication service only and does not use external authentication services, such as RADIUS.

The statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Topics ■ Using External AAA Authentication Services with DHCP on page 53

user-prefix

Syntax	<code>user-prefix <i>user-prefix-string</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication username-include]</p>
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Specify the user prefix that is concatenated with the username during the subscriber authentication process.
Options	<i>user-prefix-string</i> —The user prefix string.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Topics	■ Using External AAA Authentication Services with DHCP on page 53

user-prefix

Syntax	<code>user-prefix <i>user-prefix-string</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]</p>
Release Information	Statement introduced in JUNOS Release 9.1.
Description	Specify the user prefix that is concatenated with the username during the subscriber authentication process.
Options	<i>user-prefix-string</i> —The user prefix string.
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Using External AAA Authentication Services with DHCP on page 53

vendor-option

Syntax vendor-option {
 (equals | starts-with) (ascii *match-string* | hexadecimal *match-hex*) {
 (relay-server-group *server-group-name* |
 local-server-group *local-server-group-name* |
 drop);
 }
 (default-relay-server-group *server-group-name* |
 default-local-server-group *local-server-group-name* |
 drop);
}

Hierarchy Level [edit forwarding-options dhcp-relay relay-option-60],
 [edit forwarding-options dhcp-relay group *group-name* relay-option-60],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay relay-option-60],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay group *group-name* relay-option-60],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay relay-option-60],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* relay-option-60],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay relay-option-60],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay group *group-name* relay-option-60]

Release Information Statement introduced in JUNOS Release 9.0.

Description Configure the match criteria when you use the DHCP vendor class identifier option (option 60) in DHCP client packets to forward client traffic to specific DHCP servers. The extended DHCP relay agent compares the option 60 vendor-specific strings received in DHCP client packets against the match criteria that you specify. If there is a match, you can define certain actions for the associated DHCP client packets.

The **vendor-option** statement enables you to specify either an exact, left-to-right match (with the **equals** statement) or a partial match (with the **starts-with** statement), and configure either an ASCII match string (with the **ascii** statement) or a hexadecimal match string (with the **hexadecimal** statement).

You can configure an unlimited number of match strings. Match strings do not support the use of wildcard attributes.

Options **equals**—Exact, left-to-right match of the ASCII or hexadecimal match string with the option 60 string.

starts-with—Partial match of the ASCII or hexadecimal match string with the option 60 string. The option 60 string can contain a superset of the ASCII or hexadecimal match string, provided that the leftmost characters of the option 60 string entirely match the characters in the configured match string. When you use the **starts-with** statement, the longest match rule applies; that is, the router matches the string “test123” before it matches the string “test”.

`ascii match-string`—ASCII match string of 1 through 255 alphanumeric characters.

`hexadecimal match-hex`—Hexadecimal match string of 1 through 255 hexadecimal characters (0 through 9, a through f, A through F).

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Topics ■ Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 87

vlan-nas-port-stacked-format

Syntax `vlan-nas-port-stacked-format;`

Hierarchy Level [edit access profile *profile-name* radius options]

Release Information Statement introduced in JUNOS Release 9.1.

Description Configure RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Topics ■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19

wins-server

Syntax `wins-server [hostnames];`

Hierarchy Level [edit access address-assignment pool *pool-name* family inet dhcp-attributes]

Release Information Statement introduced in JUNOS Release 9.0.

Description Specify one or more NetBIOS name servers (NBNS) that the client uses to resolve NetBIOS names. This is equivalent to DHCP option 44.

Options *server-list*—IP addresses of the NetBIOS name servers, listed in order of preference.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Topics ■ Configuring Address-Assignment Pools on page 39

Part 3

Mobile IP Access

- Mobile IP Overview on page 243
- Configuring Mobile IP on page 249
- Summary of Mobile IP Statements on page 257

Chapter 10

Mobile IP Overview

- Mobile IP Home Agent Elements and Behavior on page 243

Mobile IP Home Agent Elements and Behavior

This topic describes Mobile IP home agent for subscriber access.

Mobile IP is a tunneling-based solution that enhances the utility of JUNOS routing platforms at the edge of the network between fixed wire and wireless network domains. This tunneling-based solution enables a router on a user's home subnet to intercept and forward IP packets to users who roam beyond traditional network boundaries. Mobile IP is useful in environments where mobility is desired and the traditional land line dial-in model does not provide an adequate solution, and in environments where a wireless technology is used.

You configure Mobile IP home agent parameters in the `[edit services mobile-ip]` hierarchy.



NOTE: Currently, JUNOS software does not support configuration of the Mobile IP foreign agent.

Traditionally, IP addresses are associated with a fixed network location. To achieve mobility, the mobile node assumes a secondary IP address that matches the new network and redirects the traffic bound to the primary or home address to the mobile node's new network. In the Mobile IP architecture, the two agents that accomplish this task are the home agent and the foreign agent.

When a mobile node roams into a new, foreign network, it negotiates with the foreign agent to get a secondary IP address, which is referred to as the care-of address. The mobile node registers this care-of address with the home agent. The home agent then establishes a tunnel to the care-of address if the tunnel is not established earlier.



NOTE: You need to establish only one tunnel between the home agent and the care-of address. Demultiplexing of the traffic is done through IP address inspection.

Packets sent to the home address of the mobile node are redirected by the home agent through the tunnel to the care-of address at the foreign agent. The foreign agent routes the packets to the mobile node's home address. If the mobile node's

home address is a private address or if the foreign agent implements ingress filtering, a reverse tunnel from the care-of address to the home agent is required.

Mobile nodes typically belong to a virtual network, which is an address range or subnet that is not directly served by any physical, routed interface on the home network. These mobile nodes never return home to attach to a physical interface on the home agent. Traffic destined for the mobile node can be forward over any interface.

You can use the Mobile IP home agent feature to configure the home agent within the default router context. The home agent handles the following tasks:

- Registration
- Routing and forwarding

Mobile IP Registration

The home agent receives the registration requests (RRQs) on UDP port 434. The registration request contains the home agent IP address. The home agent can support static home address allocation and dynamic home address allocation. The home agent can revoke a mobile node's registration. When this happens, the mobility binding is removed and the foreign agent is informed of the revocation so it can free up its resources. The foreign agent can send a registration revocation request to the home agent when the mobile node roams to another area. The revocation request can include a revocation support extension to indicate that it supports the revocation mechanism.

Home Address Assignment

The mobile node's home address can either be preconfigured, or dynamically allocated by the Mobile IP home agent. If a nonzero home address is preconfigured, the home agent processes the registration request using the home address and NAI (if the NAI is present).

If the home address is dynamically allocated, the mobile node submits a zero home address and requests the home agent to assign an IP address. The mobile node then uses the address provided by the home agent for subsequent registration requests, until the mobile node is rebooted or the registration expires.

Home address allocation is done by one of the existing authentication, authorization, and accounting (AAA) server back-end address mechanisms, such as:

- By RADIUS, in the Framed-IP-Address attribute
- From a local address pool returned by RADIUS in the Framed-Pool attribute

Authentication

The home agent authenticates the requests based on RFC 3344—IP Mobility Support for IPv4 (August 2002). By default, a AAA server is used for authentication; alternatively, you can configure local authentication parameters on the home agent. The mobile node authentication is verified and the authentication algorithm and key

are retrieved by checking the security association indexed by the security parameter index (SPI) value. This verification results in the key and the authentication algorithm with which to compute an MD-5 message digest over the registration request. The Mobile IP home agent supports both HMAC-MD5 and keyed-MD5 authentication algorithms. When the result of this computation matches the authenticator, the mobile-home extension is authenticated. For local authentication, the key is limited to a maximum of 128 bits. For AAA authentication, the key can be longer depending on the maximum length configured on the AAA server.

When HA receives the access accept from the AAA, it extracts the MN-HA key from the response. The home agent does the MN-HA authentication extension processing based on the MN-HA key by running authentication algorithm (HMAC-MD5 or Keyed-MD5) on the message to compute a hash (authenticator), which is compared with the hash value in the MN-HA extension. If the hash value matches the RRQ is considered authenticated.

If a security association is configured for the foreign agent, the foreign-home authentication extension is verified; otherwise, authentication success is based only on the mobile-home authenticator.

The home agent checks the identification (ID) field to verify that a registration message has been freshly generated by the mobile node, and is not simply being replayed by an attacker from some previous registration. The ID field represents a 64-bit Network Time Protocol (NTP) formatted time value. The configured replay timestamp defines the tolerance time window in seconds by which a registration request timestamp and the local time of the HA can differ. By default, the timestamp must be within 7 seconds of the replay tolerance configured for the mobile node or, if that is configured, the timestamp tolerance of the home agent itself.

Re-authentication

Re-authentication is not currently supported by the authentication process. Mobile IP caches a security association for each mobile node helps overcome this limitation. When a mobile node requests re-registration or de-registration, Mobile IP refers to the cached security association for that mobile node and performs MD5 message authentication.

When the security association for the mobile node changes after the node is authenticated, the cache entry is not invalidated. Consequently, the mobile node's RRQ is rejected. In this case you must clear the binding with the mobile node so that it can de-register and then log in.

RADIUS server configuration changes relating to the subscriber do not propagate to the cache. In this case you must clear the binding with the mobile node so that it can de-register and then log in.

AAA Authentication

You can store the security associations and configuration information remotely on a RADIUS server. The home agent applies the authentication algorithm and security key to the mobile node's message. The AAA server uses Juniper Networks vendor-specific attributes (VSAs) listed in Table 24 on page 246. These VSAs are mandatory in the reply to provide the appropriate authentication algorithm and the

secure key for the authentication request. If the security parameters are not retrieved, then the request for mobility service is rejected, a security violation error is logged, and no registration reply is generated.

Table 24: Juniper VSAs used by Mobile IP

Attribute Number	Attribute Name	Description	Value
26-84	Mobile-IP-Algorithm	Authentication algorithm used for Mobile-IP registration	integer: 4-octet
26-85	Mobile-IP-SPI	Security parameter index for Mobile IP registration	integer: 4-octet
26-86	Mobile-IP-Key	Security association MD5 key for Mobile IP registration	string: key
26-87	Mobile-IP-Replay	Replay timestamp for Mobile IP registration	integer: 4-octet
26-89	Mobile-IP-Lifetime	Registration lifetime for Mobile IP registration	integer: 4-octet

AAA authentication is accomplished by generating a AAA access-request to a AAA server. This is the default authentication mode, but you can include the **authenticate order aaa** statement at the [edit services mobile-ip] hierarchy level to explicitly configure AAA authentication. You cannot configure a fallback mechanism for AAA authentication. If the AAA request times out, the home agent does not fall back on the local router to determine the authentication parameters. The registration request is rejected. When the message is authenticated, the AAA server always returns either the Framed-IP-Address or Framed-Pool attribute for the user.

The presence of the mobile node's NAI and home IP address in the authentication request that the home agent sends to the AAA server is determined by their presence in the mobile node RRQ received by the home agent:

- When both the NAI and home IP address of the mobile node are present in the registration request, then the authentication request from Mobile IP to AAA has the NAI as the user name.
- When only the NAI is present in the registration request, then the NAI is used as the user name.
- When only the IP address (home address) is present in the registration request, then the IP address is used as the user name.
- When both the NAI address and the IP address are missing from the registration request, then the registration request is rejected.

Local Authentication

As an alternative to the default authentication by AAA server, you can store the security associations and configuration information locally on the router hosting the home agent. Local authentication is accomplished by querying the locally configured

security parameters for the mobile node. The home agent applies the authentication algorithm and security key to the mobile node's message. If the security parameters are not available or do not match the RRQ, then the request for mobility service is rejected, a security violation error is logged, and no registration reply is generated.

For local authentication, include the **authenticate order local** statement at the **[edit services mobile-ip]** hierarchy level. You cannot configure a fallback mechanism for local authentication. If the local authentication fails, the home agent does not fall back on the AAA server to determine the authentication parameters. The registration request is rejected. Use the **peer** statement at the **[edit services mobile-ip]** hierarchy level to configure the authentication attributes on the home agent for a user identified by IP address or network address identifier (NAI). This user can be a mobile node or a foreign agent.

The authentication attributes include a security parameter index (SPI) to identify a particular security context between the home agent and the mobile node or foreign agent among the contexts available in the mobility security association. Associated with each SPI is the MD5 algorithm and key used to authenticate messages from the mobile node or foreign agent. You can also configure the replay timestamp tolerance for the mobile node or foreign agent.

Accounting

The JUNOS Mobile IP home agent application supports time-based accounting for Mobile IP subscribers. Include the **statistics time** statement in the subscriber access profile at the **[edit access profile profile-name accounting]** hierarchy level. Time-based accounting for Mobile IP subscribers also requires that you include the **authenticate order aaa** statement at the **[edit services mobile-ip]** hierarchy level. Accounting begins when the Mobile IP home agent registers the mobile node and creates a binding with the mobile node.

Accounting stops when the binding is deleted. Any of the following actions can cause the binding to be deleted:

- The mobile user logs off.
- The binding lifetime expires.
- The mobile node is deregistered for any reason.
- The foreign agent sends a revocation message.

The Acct-Start message the home agent sends to the AAA server includes the network address identifier (NAI) in the User-Name attribute and the home address of the mobile IP node in the Framed-IP-Address attribute. The Acct-Stop message additionally includes the Acct-Session-Id and Acct-Session-Time attributes.

You cannot currently configure time-based accounting for only the Mobile IP service in a given logical router or routing instance. Enabling time-based accounting for Mobile IP also enables time-based accounting for all other services that are configured in that logical router or routing instance. If you do not want time-based accounting to apply to other services, then you must configure those services in a different logical router or routing instance.

Mobile IP Routing and Forwarding

The mobile node acquires a care-of address from the foreign agent. The care-of address is reachable from the mobile node, and routable from the home agent. The mobile node includes the care-of address in its registration request to the home agent. After AAA or local authentication successfully processes and authenticates the RRQ and provides both the authorization parameters for the mobile node and an IP address, the home agent then sets up the data path for the mobile node and sends back a registration reply (RRP) confirming successful registration of the mobile node.

When the foreign agent receives the successful RRP from the home agent, the FA sets up the data path for the mobile node. Then it sends the RRP to the mobile node to acknowledge that the mobile node is now successfully registered and the data path between the home agent and the mobile node is in place.

The home agent supports generic routing encapsulation (GRE) and IP-in-IP tunnel encapsulation for forward and reverse tunneling. The tunnels must be statically configured. When packets destined for the mobile node reach a home agent, the home agent encapsulates the packets and tunnels them to the care-of address. Packets that exceed the maximum transmission unit (MTU) value of the tunnel are dropped and an ICMP error message is sent to the source IP address. Packets without an access route are returned to the source with an ICMP destination unreachable error message. For reverse tunnels, packets are de-tunneled and forwarded towards the next hop to the destination address.

- Related Topics** ■ For information about the specific Juniper Networks VSAs used for Mobile IP RADIUS-based authentication, see Juniper Networks VSAs Supported by the AAA Service Framework on page 32

Chapter 11

Configuring Mobile IP

- Configuring Mobile IP on page 249
- Tracing Mobile IP Operations on page 250
- Configuring the Mobile IP Authentication Method on page 253
- Configuring the Mobile IP Home Agent on page 253
- Configuring the Local Authentication Attributes for the Mobile Node on page 254
- Configuring Accounting for Mobile IP Subscribers on page 254
- Configuring Dynamic Home Assignment for the Mobile Node on page 255

Configuring Mobile IP

You can configure Mobile IP to provide mobility for subscribers in IP networks. The Mobile IP home agent authenticates registration requests from mobile users and forward traffic to them at their care-of address without having to advertise that address to the wider network.

To configure Mobile IP for mobile subscriber access:

1. Configure trace options for troubleshooting the configuration.

See “Tracing Mobile IP Operations” on page 250.
2. Configure the authentication method for registration requests, local or AAA.

See “Configuring the Mobile IP Authentication Method” on page 253.
3. Configure the Mobile IP home agent.

See “Configuring the Mobile IP Home Agent” on page 253.
4. Configure the authentication attributes for the mobile node.

See “Configuring the Local Authentication Attributes for the Mobile Node” on page 254.
5. Configure accounting for Mobile IP subscribers.

See “Configuring Accounting for Mobile IP Subscribers” on page 254
6. Configure the dynamic reassignment of the mobile node to another home agent.

See “Configuring Dynamic Home Assignment for the Mobile Node” on page 255.

Tracing Mobile IP Operations

Mobile IP supports tracing operations. Mobile IP tracing operations track Mobile IP operations and record them in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

1. Important events are logged in a file called `mipd` located in the `/var/log` directory. You cannot change the directory (`/var/log`) in which trace files are located.
2. When the file `mipd` reaches 128 kilobytes (KB), it is renamed `mipd.0`, then `mipd.1`, and so on, until there are three trace files. Then the oldest trace file (`mipd.2`) is overwritten.

You can optionally configure the maximum file size to be from 10 KB through 1 gigabyte (GB). You can also specify the number of trace files to be from 2 through 1000. (For more information about how log files are created, see the *JUNOS System Log Messages Reference*.)

Log files can be accessed only by the user who configures the tracing operation.

To configure Mobile IP tracing operations:

1. Specify that you want to configure tracing options.

```
[edit services mobile-ip]
user@host# edit traceoptions
```

2. (Optional) Configure the name for the file used for the trace output.

See “Configuring the Mobile IP Trace Log Filename” on page 251.

3. (Optional) Configure the number and size of the log files.

See “Configuring the Number and Size of Mobile IP Log Files” on page 251.

4. (Optional) Configure access to the log file.

See “Configuring Access to the Mobile IP Log File” on page 251.

5. (Optional) Configure a regular expression to filter logging events.

See “Configuring a Regular Expression for Mobile IP Lines to Be Logged” on page 252.

6. (Optional) Configure flags to filter the operations to be logged.

See “Configuring the Mobile IP Tracing Flags” on page 252.

The Mobile IP traceoptions operations are described in the following sections:

- Configuring the Mobile IP Trace Log Filename on page 251
- Configuring the Number and Size of Mobile IP Log Files on page 251
- Configuring Access to the Mobile IP Log File on page 251

- Configuring a Regular Expression for Mobile IP Lines to Be Logged on page 252
- Configuring the Mobile IP Tracing Flags on page 252

Configuring the Mobile IP Trace Log Filename

By default, the name of the file that records trace output for Mobile IP is `mipd`. You can specify a different name with the `file` option.

To configure the filename for Mobile IP tracing operations:

- Specify the name of the file used for the trace output.

```
[edit services mobile-ip traceoptions]
user@host# set file mip_1
```

Configuring the Number and Size of Mobile IP Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed `filename.0`, then `filename.1`, and so on, until there are three trace files. Then the oldest trace file (`filename.2`) is overwritten.

You can optionally configure the maximum file size to be from 10 KB through 1 gigabyte (GB). You can also specify the number of trace files to be from 2 through 1000.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (`filename`) reaches 2 MB, `filename` is renamed `filename.0`, and a new file called `filename` is created. When the new `filename` reaches 2 MB, `filename.0` is renamed `filename.1` and `filename` is renamed `filename.0`. This process repeats until there are 20 trace files. Then the oldest file (`filename.19`) is overwritten by the newest file (`filename.0`).

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output. (Mobile IP supports the `files` and `size` options for the `traceoptions` statement.)

```
[edit services mobile-ip traceoptions]
user@host# set file mip_1 _logfile_1 files 20 size 2097152
```

Configuring Access to the Mobile IP Log File

By default, log files can be accessed only by the user who configures the tracing operation. You can enable all users to read the log file and you can explicitly set the default behavior of the log file.

To specify that all users can read the log file:

- Configure the log file to be world-readable.

```
[edit services mobile-ip traceoptions]
user@host# set file mip_1 _logfile_1 world-readable
```


To explicitly set the default behavior, in which the log file can only be read by the user who configured tracing:

- Configure the log file to be no-world-readable.

```
[edit services mobile-ip traceoptions]
user@host# set file mip_1 _logfile_1 no-world-readable
```

Configuring a Regular Expression for Mobile IP Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events.

You can refine the output by including regular expressions that will be matched.

To configure regular expressions to be matched:

- Configure the regular expression.

```
[edit services mobile-ip traceoptions]
user@host# set file mip_1 _logfile_1 match regex
```

Configuring the Mobile IP Tracing Flags

By default, only important events are logged. You can specify which trace operations are logged by including specific tracing flags. The following table describes the flags that you can include.

Flag	Description
all	Trace all operations
authentication	Trace authentication operations
binding	Trace bindings
configuration	Trace configuration events
event	Trace events
home-agent	Trace home agent operations
interface-database	Trace interface database operations
packet	Trace packet decoding operations
protocol	Trace protocol operations
rtstock	Trace routing socket operations
session-db	Trace session database events
signal	Trace signal operations
subscriber	Trace subscriber events

Flag	Description
trace	Trace changes in tracing
tunnel	Trace tunneling operations

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit services mobile-ip traceoptions]
user@host# set flag home-agent
```

Related Topics ■ Configuring Mobile IP on page 249

Configuring the Mobile IP Authentication Method

You can configure Mobile IP to authenticate registration requests from mobile nodes by either the locally configured attributes or a AAA server. AAA server authentication is the default method.

To configure the Mobile IP authentication method:

- Specify either local or AAA authentication.

```
[edit services mobile-ip]
user@host# set authenticate order local
```

Configuring the Mobile IP Home Agent

To configure the home agent for a Mobile IP virtual network:

1. Configure the loopback IP address that is used as the home agent IP address.

```
[edit services mobile-ip home-agent virtual-network]
user@host# set home-agent-address 10.5.5.0
```

2. (Optional) Configure the maximum lifetime that the home agent accepts in any registration request from a mobile node.

```
[edit services mobile-ip home-agent virtual-network]
user@host# set home-agent-address 10.5.5.0 registration-lifetime 100
```

3. (Optional) Configure a timestamp tolerance for registration replay protection.

```
[edit services mobile-ip home-agent virtual-network]
user@host# set home-agent-address 10.5.5.0 timestamp-tolerance 200
```

4. Configure whether the home agent can revoke a mobile node's registration to deactivate the node.


```
[edit services mobile-ip home-agent virtual-network]
user@host# set home-agent-address 10.5.5.0 revocation-required
```

5. Specify the interfaces on which the home agent accepts registration requests.

```
[edit services mobile-ip home-agent]
user@host# set enable-service ge-0/0/1.0
user@host# set enable-service ge-0/0/2.0
user@host# set enable-service ge-0/0/3.0
user@host# set enable-service ge-0/0/4.0
```

Configuring the Local Authentication Attributes for the Mobile Node

You specify for each mobile node several attributes that enable authentication of registration requests from the node. These attributes include security association context for the peering relationship, the entity type of the node, the encryption algorithm and key used to authenticate the request, and replay protection.

To configure authentication attributes for the mobile node:

1. Configure the peer entity for the security parameter.

```
[edit services mobile-ip]
user@host# set peer ip-address 10.4.2.20 spi 500 entity-type mobility-agent
```

2. Configure the algorithm used for authenticating Mobile IP messages. By default, the hmac-md5 algorithm is used.

```
[edit services mobile-ip]
user@host# set peer ip-address 10.4.2.20 spi 500 algorithm md5
```

3. Configure the authentication key for the security association, in either HEX or ASCII format.

```
[edit services mobile-ip]
user@host# set peer ip-address 10.4.2.20 spi 500 key ascii xf125j9m
```

4. Configure a timestamp tolerance for registration replay protection or specify that the timestamp tolerance be taken from the value configured on the home agent.

```
[edit services mobile-ip]
user@host# set peer ip-address 10.4.2.20 spi 500 replay-method timestamp tolerance 250
```

Configuring Accounting for Mobile IP Subscribers

You can configure time-based accounting to track the subscriber sessions of Mobile IP subscribers.

To configure Mobile IP accounting:

1. Configure the IP address for the RADIUS accounting server.


```
[edit access profile mip-win4]
user@host# set radius accounting server 192.168.20.5
```

2. Specify RADIUS as the accounting method for Mobile IP subscribers.

```
[edit access profile mip-win4 accounting]
user@host# set order radius
```

3. Specify time-based accounting for the access profile used for the subscriber.

```
[edit access profile mip-win4 accounting]
user@host# set statistics time
```

- Related Topics**
- Specifying the Authentication and Accounting Methods for Subscriber Access on page 19
 - Configuring How Accounting Statistics Are Collected for Subscriber Access on page 20
 - Configuring RADIUS Server Parameters for Subscriber Access on page 21

Configuring Dynamic Home Assignment for the Mobile Node

The mobile node can request that the home agent dynamically assign an IP address for the home agent. The mobile node uses this address for the home agent in all subsequent registration requests until the registration expires or the mobile node is rebooted.

To configure the IP address to be used by the mobile node for the home agent:

- Configure the IP address for the specified mobile node.

```
[edit services mobile-ip]
user@host# set dynamic-home-assignment home-agent nai bws@example.com
home-agent 192.168.4.5
```


Chapter 12

Summary of Mobile IP Statements

algorithm

Syntax	algorithm (hmac-md5 md5);
Hierarchy Level	[edit services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>], [edit services mobile-ip peer nai <i>user@domain</i> spi <i>hexadecimal-value</i>]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Configure the algorithm used for authenticating Mobile IP messages.
Default	HMAC-MD5 is used by default.
Options	hmac-md5—Specifies algorithm hmac-md5 md5—Specifies algorithm md5
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring the Mobile IP Home Agent on page 253

authenticate

Syntax	authenticate { order (aaa local); }
Hierarchy Level	[edit services mobile-ip]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Define the authentication method performed for Mobile IP.
Options	The remaining statement is explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring the Mobile IP Home Agent on page 253

dynamic-home-assignment

Syntax	dynamic-home-assignment { home-agent { nai (<i>name@domain.com</i> <i>@domain.com</i>) { home-agent <i>ip-address</i> ; } } }
Hierarchy Level	[edit services mobile-ip]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Define the dynamic assignment rule for the home agent.
Options	The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring the Mobile IP Home Agent on page 253

enable-service

Syntax	enable-service <i>list-of-interfaces</i> ;
Hierarchy Level	[edit services mobile-ip home-agent]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Define the list of interfaces on which the home agent service can be enabled. The system accepts registration requests only if it is on one of these interfaces.
Options	<i>list-of-interfaces</i> —List of interfaces on which the home agent can be enabled.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring the Mobile IP Home Agent on page 253

entity-type

Syntax	entity-type (host mobility-agent);
Hierarchy Level	[edit services mobile-ip peer spi <i>hexadecimal-value</i>]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Configure the security parameter for the peer entity, either a mobile node or the home agent.
Options	host—Mobile node in home agent mobility-agent—Home agent
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring the Mobile IP Home Agent on page 253

home-agent

Syntax	<pre> home-agent { enable-service <i>interface-name</i>; virtual-network { home-agent-address <i>ip-address</i> { registration-lifetime <i>seconds</i>; revocation-required; timestamp-tolerance <i>seconds</i>; } } } </pre>
Hierarchy Level	[edit services mobile-ip]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Define the virtual networks and non-virtual networks for the Mobile IP home agent.
Options	The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring the Mobile IP Home Agent on page 253

home-agent

Syntax	home-agent { nai (<i>name@domain</i> <i>@domain</i>) { home-agent <i>ip-address</i> ; } }
Hierarchy Level	[edit services mobile-ip dynamic-home-assignment]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Configure the IP address to which registration requests are sent as part of the home agent's dynamic assignment rule.
Options	The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring the Mobile IP Home Agent on page 253

home-agent-address

Syntax	home-agent-address <i>ip-address</i> { registration-lifetime <i>seconds</i> ; revocation-required; timestamp-tolerance <i>seconds</i> ; }
Hierarchy Level	[edit services mobile-ip home-agent virtual-network]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Defines addressing for the virtual network of the Mobile IP home agent.
Options	<i>ip-address</i> —For virtual networks, the loopback IP address for the virtual network. For non-virtual networks, a public address. The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring the Mobile IP Home Agent on page 253

key

Syntax	<code>key (hex ascii) <i>string</i>;</code>
Hierarchy Level	[edit services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>], [edit services mobile-ip peer nai <i>user@domain</i> spi <i>hexadecimal-value</i>]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Configure the authentication key for the security association, in either HEX or ASCII format. The resulting 128-bit key is specified as a hexadecimal number with each character in the range 0x0–0xF.
Options	<code>hex <i>string</i></code> —Key specified in HEX format <code>ascii <i>string</i></code> —Key specified in ASCII format
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring the Mobile IP Home Agent on page 253

mobile-ip

Syntax

```
mobile-ip {
  authenticate {
    order (aaa | local);
  }
  dynamic-home-assignment {
    home-agent {
      nai (host@domain.com | @domain.com) {
        home-agent ip-address;
      }
    }
  }
  home-agent {
    enable-service interface-name;
  }
  virtual-network {
    home-agent-address ip-address {
      registration-lifetime seconds;
      revocation-required;
      timestamp-tolerance seconds;
    }
  }
  peer {
    (ip-address address | nai user@domain.com) {
      spi hexadecimal-value {
        algorithm (hmac-md5 | md5);
        entity-type (host | mobility-agent);
        key (hex | ascii) string;
        replay-method (none | timestamp seconds);
      }
    }
  }
  traceoptions {
    file <filename> <files number> <match regular-expression > <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
  }
}
```

Hierarchy Level [edit services]

Release Information Statement introduced in JUNOS Release 9.3.

Description Configure JUNOS Mobile IP features.

Options The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Topics ■ Configuring the Mobile IP Home Agent on page 253

nai

Syntax `nai (name@domain.com | @domain.com) {
 home-agent ip-address;
 }`

Hierarchy Level [edit services mobile-ip dynamic-home-assignment home-agent]

Release Information Statement introduced in JUNOS Release 9.3.

Description Configure the network address identifiers (NAI) to which registration requests are sent as part of the home agent’s dynamic assignment rule .

Options *name@domain.com*—User at a specified domain

 @domain—All users at a specified domain



NOTE: The *name* can include only alphanumeric characters, dots, hyphens, or underscores. The *name* cannot end in *@*; *@* must be used to separate *name* and *domain*. The *domain* can include only alphanumeric characters, dots, or hyphens. The *domain* must be in the format *domain.suffix*, where the *suffix* is com, org, net, and so on. The *suffix* must consist of at least two alphanumeric characters.

The remaining statement is explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Topics ■ Configuring the Mobile IP Home Agent on page 253

order

Syntax	order (aaa local);
Hierarchy Level	[edit services mobile-ip authenticate]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Define the authentication method performed for Mobile IP.
Default	AAA is the default authentication method.
Options	<p>aaa—Authentication is performed by AAA.</p> <p>local—Authentication is performed using parameters defined in the local database.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	■ Configuring the Mobile IP Home Agent on page 253

peer

```

Syntax  peer {
            (ip-address address | nai user@domain) {
                spi hexadecimal-value {
                    algorithm (hmac-md5 | md5);
                    entity-type (host | mobility-agent);
                    key (hex | ascii) string;
                    replay-method (timestamp seconds | none);
                }
            }
        }

```

Hierarchy Level [edit services mobile-ip]

Release Information Statement introduced in JUNOS Release 9.3.

Description Define the authentication configurations for a home agent mobile node. An authentication enables the registration message as acceptable to the final recipient of the registration message.

Options ip-address *address*—IP address of the peer.

nai *name@domain*—Network address identifier (NAI) of the peer. The *name* can include only alphanumeric characters, dots, hyphens, or underscores. The *name* cannot end in @; @ must be used to separate *name* and *domain*. The *domain* can include only alphanumeric characters, dots, or hyphens. The *domain* must be in the format *domain.suffix*, where the *suffix* is com, org, net, and so on. The *suffix* must consist of at least two alphanumeric characters.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Topics ■ Configuring the Mobile IP Home Agent on page 253

registration-lifetime

Syntax	registration-lifetime <i>seconds</i> ;
Hierarchy Level	[edit services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i>]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Configure maximum period for registration lifetime that is accepted by the Mobile IP home agent.
Options	registration-lifetime <i>seconds</i> —Maximum lifetime that the home agent accepts in any registration request. Range: 7 through 65535 seconds Default: 3600 seconds
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring the Mobile IP Home Agent on page 253

revocation-required

Syntax	revocation-rrequired;
Hierarchy Level	[edit services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i>]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Configure the Mobile IP home agent to accept registration revocation requests only when the request includes the revocation extension.
Default	The Mobile IP home agent supports registration revocation requests that include the revocation extension, but it does not require the extension.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring the Mobile IP Home Agent on page 253

replay-method

Syntax	replay-method (none timestamp <i>seconds</i>);
Hierarchy Level	[edit services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>], [edit services mobile-ip peer nai <i>user@domain</i> spi <i>hexadecimal-value</i>]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Configure the replay protection method. The Identification field enables the home agent to verify that a registration message has been recently generated by the mobile node, rather than replayed by an attacker from a previous registration. You can specify a timestamp tolerance for the mobile node, which causes the request to be rejected if the tolerance is exceeded, or you can specify that the tolerance be taken from the value configured on the home agent.
Default	If you do not configure the replay protection method, then the timestamp tolerance is taken from the home agent by default.
Options	<p>none—Timestamp tolerance is obtained from the setting configured for the home agent</p> <p>timestamp <i>seconds</i>—Tolerance time in which a registration request timestamp and the local time of the home agent can differ. Range: 1 through 255 seconds</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	■ Configuring the Mobile IP Home Agent on page 253

spi

Syntax `spi hexadecimal-value {
 algorithm (hmac-md5 | md5);
 entity-type (host | mobility-agent);
 key (hex | ascii) string;
 replay-method (none | timestamp seconds);
 }`

Hierarchy Level [edit services mobile-ip peerip-address *address*],
 [edit services mobile-ip peer nai *user@domain*]

Release Information Statement introduced in JUNOS Release 9.3.

Description Define the security parameter index for identifying a security context between a pair of nodes among the contexts available in the Mobility Security Association. The index selects the authentication algorithm and key.

Options *hexadecimal-value*—Security parameter index identifier.
 Range: 100 to FFFFFFFF

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Topics ■ Configuring the Mobile IP Home Agent on page 253

statistics

Syntax	statistics (time volume-time);
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in JUNOS Release 9.1. volume-time option introduced in JUNOS Release 9.4.
Description	Configure the router to collect time statistics or both volume and time statistics for the sessions being managed by AAA.
Options	time—Collect uptime statistics only. volume-time—Collect both volume and uptime statistics. This option is not available for Mobile IP.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Mobile IP Home Agent Elements and Behavior on page 243 ■ Configuring Authentication and Accounting Parameters for Subscriber Access on page 19

timestamp-tolerance

Syntax	timestamp-tolerance <i>seconds</i> ;
Hierarchy Level	[edit services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i>]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Configure the acceptable difference between a registration request timestamp and the local time of the home agent.
Options	<p>timestamp-tolerance <i>seconds</i>—Acceptable difference in time between a registration request timestamp and the local time of the home agent.</p> <p>Range: 1 through 255 seconds</p> <p>Default: 7 seconds</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring the Mobile IP Home Agent on page 253

traceoptions

Syntax traceoptions {
 file <filename> <files number> <match regular-expression > <size maximum-file-size>
 <world-readable | no-world-readable>;
 flag *flag*;
 level (all | error | info | notice | verbose | warning);
 no-remote-trace;
 }

Hierarchy Level [edit services mobile-ip]

Release Information Statement introduced in JUNOS Release 9.3.

Description Define tracing operations for Mobile IP processes.

Options file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory */var/log*.

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- all—Trace all operations.
- authentication—Trace authentication operations.
- binding—Trace bindings.
- configuration—Trace configuration events.
- event—Trace events.
- home-agent—Trace home agent operations.
- interface-database—Trace interface database operations.
- packet—Trace packet decoding operations.
- protocol—Trace protocol operations.
- rtsock—Trace routing socket operations.
- session-db—Trace session database events.
- signal—Trace signal operations.
- subscriber—Trace subscriber events.
- trace—Trace changes in tracing.
- tunnel—Trace tunneling operations.

level—Level of tracing to perform. You can specify any of the following levels:

- all—Match all levels.
- error—Match error conditions.
- info—Match informational messages.

- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages.
- **warning**—Match verbose messages.

no-remote-trace—Disable remote tracing.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Topics ■ Configuring the Mobile IP Home Agent on page 253

virtual-network

Syntax virtual-network {
 home-agent-address *ip-address* {
 registration-lifetime *seconds*;
 revocation-required;
 timestamp-tolerance *seconds*;
 }
 }

Hierarchy Level [edit services mobile-ip home-agent]

Release Information Statement introduced in JUNOS Release 9.3.

Description Define the virtual network for the Mobile IP home agent. Only one virtual network is supported.

Options The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Topics ■ Configuring the Mobile IP Home Agent on page 253

Part 4

Dynamic Profiles for Access and Services

- Dynamic Profiles Overview on page 275
- Configuring Dynamic Profiles on page 283
- Dynamic Profile Examples on page 293
- Summary of Dynamic Profile Statements on page 297

Chapter 13

Dynamic Profiles Overview

- Dynamic Profiles Overview on page 275
- Dynamic Variables Overview on page 276

Dynamic Profiles Overview

A dynamic profile is a set of characteristics, defined in a type of template, that you can use to provide dynamic subscriber access and services for broadband applications. These services are assigned dynamically to interfaces. The **dynamic-profiles** hierarchy appears at the top level of the CLI hierarchy and contains many Juniper Networks configuration statements that you normally define statically.

Dynamic profile statements appear in the following CLI sub-categories within the **dynamic-profiles** hierarchy:

- Interfaces (supporting static VLAN and LAG on Ethernet interfaces and static IP demux interfaces)
- Protocols (supporting IGMP interface configuration)
- Class of service (supporting traffic classification and scheduling)
- Variables (supporting user-defined variable configuration)

This topic covers:

- Dynamic Profile Interface Support on page 275
- What Dynamic Profiles Do on page 275
- How Dynamic Profiles Work on page 276

Dynamic Profile Interface Support

This release supports identifying subscribers statically or dynamically. To identify subscribers statically, you can reference a static VLAN interface in a dynamic profile. To identify subscribers dynamically, you create variables for IP demux interfaces that are dynamically created when subscribers log in.

What Dynamic Profiles Do

A dynamic profile acts as a kind of template that enables you to create, update, or remove a configuration that includes client access (for example, interface or protocol)

or service (for example, CoS) attributes. Using these profiles enables you to consolidate all of the common attributes of a client (and eventually a group of clients) and apply the attributes simultaneously.

How Dynamic Profiles Work

After they are created, profiles reside on the router in a profile library. These profiles can contain various configurations. For example, you can create a client network access configuration, a services activation configuration, or both. When a router interface receives a join message from a DHCP client, the router applies the values configured in the specified dynamic profile to that router interface. In this release, the profile can contain interface, class of service (CoS), and protocol (IGMP) values that are applied directly to the interface. In addition, the dynamic profile can call input or output firewall filters that reside outside of the dynamic profiles hierarchy.

- Related Topics**
- Configuring a Basic Dynamic Profile on page 283
 - Configuring a Dynamic Profile for Client Access on page 287
 - Configuring a Dynamic Profile for Various Levels of Services on page 288
 - Dynamic Variables Overview on page 276
 - Subscriber Interface Overview on page 305

Dynamic Variables Overview

Variables constitute the dynamic component of a dynamic profile. You use variables in dynamic profiles as placeholders for dynamically obtained information that the dynamic profiles use to configure subscriber interfaces.

- How Dynamic Variables Work on page 276
- JUNOS Predefined Internal Variables on page 277
- User-Defined Variables on page 281

How Dynamic Variables Work

Dynamic variables are data placeholders that you define and place in dynamic profiles. When a particular event occurs on an interface (for example, a DHCP client accesses the interface), the dynamic profiles obtain data to fill these placeholders from one of three possible sources—the interface receiving an incoming client data packet, an externally configured server (for example, RADIUS), an internal default value associated with each user-configurable variable.

For your convenience, JUNOS provides several predefined variables that you can use within a dynamic profile. Most of these variables relate to interface-specific data obtained directly from the interface that receives an incoming client data packets (for example, interface name, interface unit value, and so on). When a client accesses the interface, the router software extracts the necessary interface data, propagates this data to the dynamic profile, and then uses the dynamic profile to configure the interface for the accessing client.

You define user-defined variables for individual dynamic profiles at the [dynamic-profiles *profile-name* variables] hierarchy level. At this hierarchy level, you create an association between a variable call value (for example, *\$junos-igmp-version*) that appears in the body of the dynamic profile and data associated with that call value that is managed in an externally configured server (for example, a RADIUS VSA managed on a RADIUS server) or defined as a default value in the **variables** stanza. When an event occurs on an interface to trigger the instantiation of a dynamic profile for the interface, the JUNOS router software obtains values for each variable from an external server (for example, from RADIUS authentication and authorization VSAs) during the subscriber authentication process or from the default value if the external server is not available or does not contain a value for the variable to use. At run time, the variables are replaced by these actual values and are used to configure the subscriber interface.



NOTE: Most variables have a default value already configured in the JUNOS router software. The purpose of these defaults is to ensure that the dynamic profile contains a valid value if one is not created and assigned during dynamic profile configuration. However, we strongly recommend that you specifically define variables instead and not rely on the existence of an internal JUNOS default.

JUNOS Predefined Internal Variables

JUNOS software contains several predefined variables. The dynamic profile obtains and replaces data for these variables from an incoming client data packet. You can specify these variables in the body of a dynamic profile without first having to define the variables at the [dynamic-profiles *profile-name* variables] hierarchy level. Table 25 on page 277 provides a list of predefined variables, their descriptions, and where in the JUNOS hierarchy you can configure them.

Table 25: JUNOS Predefined Internal Variables and Definitions

Variable	Definition
Subscriber Interfaces — Static VLAN Interfaces	
\$junos-interface-ifd-name	Name of the dynamic interface to which the subscriber access client connects. Its primary use is in creating single or multiple subscribers on a statically created interface. You specify this variable at the [dynamic-profiles <i>profile-name</i> interfaces] hierarchy level.
\$junos-underlying-interface-unit	Unit number for the underlying interface. It specifies the use of the underlying interface for the subscriber. You specify this variable at the [dynamic-profiles <i>profile-name</i> interfaces <i>\$junos-interface-ifd-name</i>] hierarchy for the unit statement.
Subscriber Interfaces — Dynamic IP Demux Interfaces	
\$junos-interface-unit	Creates a unit number for a dynamic demux interface. DHCP supplies this information when the subscriber logs in. You specify this variable at the [dynamic-profiles <i>profile-name</i> interfaces demux0] hierarchy level for the unit statement.

Table 25: JUNOS Predefined Internal Variables and Definitions (continued)

Variable	Definition
\$junos-subscriber-ip-address	IP address of the subscriber. You specify this variable at the [dynamic-profiles <i>profile-name</i> interfaces <i>demux0</i> unit family <i>inet</i> <i>demux-source</i>] hierarchy level.
\$junos-underlying-interface	<p>Creates a logical underlying interface for a dynamic demux interface. DHCP supplies this information when the subscriber logs in. You specify this variable at the [dynamic profiles <i>profile-name</i> interfaces <i>demux0</i> unit "<i>\$junos-interface-unit</i>" <i>demux-options</i>] hierarchy level for the <i>underlying-interface</i> statement.</p> <p>When configured, the underlying interface is used to determine the <i>\$junos-underlying-interface</i>, <i>\$junos-underlying-interface-unit</i>, and <i>\$junos-ifd-name</i> variables. For example, if the receiving logical interface is <i>ge-0/0/0.1</i>, the <i>\$junos-underlying-interface</i> variable is set to <i>ge-0/0/0</i> and the <i>\$junos-underlying-interface-unit</i> variable is set to <i>1</i>.</p>
Dynamic Protocols	
\$junos-interface-name	<p>Name of the dynamic interface to which the subscriber access client connects. Its use is in dynamically enabling IGMP on the subscriber interface. You specify this variable at the [dynamic-profiles <i>profile-name</i> protocols <i>igmp</i>] hierarchy level for the <i>interface</i> statement.</p> <p>The interface name is derived from concatenating the <i>\$junos-interface-ifd-name</i> and the <i>\$junos-underlying-interface-unit</i> variables obtained when a subscriber is created dynamically at the [dynamic-profiles <i>profile-name</i> interfaces] hierarchy level.</p>
Dynamic CoS — RADIUS-obtained Scheduler-Map Name and Traffic-Shaping Parameters	
\$junos-cos-scheduler-map	<p>Scheduler-map name configured in a traffic-control profile in a dynamic profile for used for subscriber access. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the <i>scheduler-map</i> statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>] hierarchy level.</p> <p>NOTE: The scheduler map can be defined dynamically (at the [edit dynamic-profiles <i>profile-name</i> class-of-service scheduler-maps] hierarchy level) or statically (at the [edit class-of-service scheduler-maps] hierarchy level).</p>
\$junos-cos-shaping-rate	<p>Shaping rate configured in a traffic-control profile in a dynamic profile for subscriber access. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the <i>shaping-rate</i> statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>] hierarchy level.</p>

Table 25: JUNOS Predefined Internal Variables and Definitions (continued)

Variable	Definition
\$junos-cos-guaranteed-rate	<p>Guaranteed rate configured in a traffic-control profile in a dynamic profile for subscriber access. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the <code>guaranteed-rate</code> statement at the <code>[edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>]</code> hierarchy level.</p>
\$junos-cos-delay-buffer-rate	<p>Delay-buffer rate configured in a traffic-control profile in a dynamic profile for subscriber access. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the <code>delay-buffer-rate</code> statement at the <code>[edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>]</code> hierarchy level.</p>
Dynamic CoS — RADIUS-obtained Scheduler Name and Parameters	
\$junos-cos-scheduler	<p>Name of a scheduler configured in a dynamic profile for subscriber access. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable at the <code>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers]</code> hierarchy level.</p>
\$junos-cos-scheduler-tx	<p>Transmit rate specified for a scheduler configured in a dynamic profile for subscriber access. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the <code>transmit-rate</code> statement at the <code>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>]</code> hierarchy level.</p>
\$junos-cos-scheduler-bs	<p>Buffer size as a percentage of total buffer, specified for a scheduler configured in a dynamic profile for subscriber access. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the <code>buffer-size</code> statement with the <code>percent</code> option at the <code>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>]</code> hierarchy level.</p>

Table 25: JUNOS Predefined Internal Variables and Definitions (continued)

Variable	Definition
\$junos-cos-scheduler-pri	<p>Packet-scheduling priority value specified for a scheduler configured in a dynamic profile for subscriber access. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the priority statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>] hierarchy level.</p>
\$junos-cos-scheduler-dropfile-low	<p>Name of the drop profile for random early detection (RED) for loss-priority level low specified for a scheduler configured in a dynamic profile for subscriber access. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the drop-profile statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i> drop-profile-map loss-priority low protocol any] hierarchy level.</p> <p>NOTE: The drop profile must be configured statically (at the [edit class-of-service drop-profiles] hierarchy level) for loss-priority low.</p>
\$junos-cos-scheduler-dropfile-medium-low	<p>Name of the drop profile for random early detection (RED) for loss-priority level medium-low specified for a scheduler configured in a dynamic profile for subscriber access. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the drop-profile statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i> drop-profile-map loss-priority medium-low protocol any] hierarchy level.</p> <p>NOTE: The drop profile must be configured statically (at the [edit class-of-service drop-profiles] hierarchy level).</p>
\$junos-cos-scheduler-dropfile-medium-high	<p>Name of the drop profile for random early detection (RED) for loss-priority level medium-high specified for a scheduler configured in a dynamic profile for subscriber access. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the drop-profile statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i> drop-profile-map loss-priority medium-high protocol any] hierarchy level.</p> <p>NOTE: The drop profile must be configured statically (at the [edit class-of-service drop-profiles] hierarchy level).</p>

Table 25: JUNOS Predefined Internal Variables and Definitions (*continued*)

Variable	Definition
\$junos-cos-scheduler-dropfile-high	<p>Name of the drop profile for random early detection (RED) for loss-priority level high specified for a scheduler configured in a dynamic profile for subscriber access. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the drop-profile statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i> drop-profile-map loss-priority high protocol any] hierarchy level.</p> <p>NOTE: The drop profile must be configured statically (at the [edit class-of-service drop-profiles] hierarchy level).</p>
\$junos-cos-scheduler-dropfile-any	<p>Name of the drop profile for random early detection (RED) for loss-priority level any specified for a scheduler configured in a dynamic profile for subscriber access. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the drop-profile statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i> drop-profile-map loss-priority any protocol any] hierarchy level.</p> <p>NOTE: The drop profile must be configured statically (at the [edit class-of-service drop-profiles] hierarchy level).</p>

User-Defined Variables

JUNOS software enables you to configure variables at the [dynamic-profiles *profile-name* variables] hierarchy level and associate those variables with supported RADIUS VSAs. The dynamic profile obtains and replaces data for these variables from an external server (for example, from RADIUS authentication and authorization VSAs) during the subscriber authentication process. At run time, the variables are replaced by these actual values (obtained from default information on the router or from the RADIUS server) and are used to configure the subscriber interface.

For a complete list of supported RADIUS VSAs for which you can create variable associations, see “RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework” on page 29.

You can also configure the user-defined variables with a default value. The default value provides a standalone configuration for the associated statement or a backup for the statement configuration if the RADIUS server is inaccessible or the VSA attribute does not contain a value.

- Related Topics**
- Configuring a Basic Dynamic Profile on page 283
 - Configuring a Dynamic Profile for Client Access on page 287

- Configuring a Dynamic Profile for Various Levels of Services on page 288
- Configuring Predefined Internal Dynamic Variables in Dynamic Profiles on page 284
- Configuring User-Defined Dynamic Variables in Dynamic Profiles on page 285
- Dynamic Profiles Overview on page 275
- Subscriber Interface Overview on page 305
- Example: Firewall Dynamic Profile on page 294
- Example: IGMP Dynamic Profile on page 293
- RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 29

Chapter 14

Configuring Dynamic Profiles

- Configuring a Basic Dynamic Profile on page 283
- Configuring Predefined Internal Dynamic Variables in Dynamic Profiles on page 284
- Configuring User-Defined Dynamic Variables in Dynamic Profiles on page 285
- Configuring a Dynamic Profile for Client Access on page 287
- Configuring a Dynamic Profile for Various Levels of Services on page 288
- Modifying Dynamic Profiles on page 289

Configuring a Basic Dynamic Profile

This topic describes how to create a basic dynamic profile. A basic profile must contain a profile name and have both the **interface-name** and **unit** statements defined with variables in the **dynamic-profiles interfaces** stanza.

Before you configure dynamic profiles for initial client access:

1. Configure the necessary router interfaces that you want DHCP clients to use when accessing the network.

See “Subscriber Interface Overview” on page 305 for information about the types of interfaces you can use with dynamic profiles and how to configure them.

2. Configure all RADIUS values that you want the profiles to use when validating DHCP clients for access to the multicast network.

See “Configuring RADIUS Server Parameters for Subscriber Access” on page 21

To configure a basic dynamic profile:

1. Name the profile.

```
user@host# set dynamic-profiles basic-profile
```

2. Define the **interface-name** statement with the internal **\$junos-interface-ifd-name** variable used by the router to match the interface name of the receiving interface.

```
[edit dynamic-profiles basic-profile]
```

```
user@host# set interfaces $junos-interface-ifd-name
```


3. Define the **unit** statement with the internal `$junos-underlying-interface-unit` variable used by the router to match the unit value of the receiving interface.

```
[edit dynamic-profiles basic-profile]
user@host# set unit $junos-underlying-interface-unit
```

- Related Topics**
- Configuring a Dynamic Profile for Client Access on page 287
 - Configuring a Dynamic Profile for Various Levels of Services on page 288
 - Configuring Predefined Internal Dynamic Variables in Dynamic Profiles on page 284
 - Configuring Static Subscriber Interfaces in Dynamic Profiles on page 311
 - Dynamic Profiles Overview on page 275
 - Dynamic Variables Overview on page 276
 - Example: Firewall Dynamic Profile on page 294
 - Example: IGMP Dynamic Profile on page 293

Configuring Predefined Internal Dynamic Variables in Dynamic Profiles

This topic discusses how to configure predefined internal dynamic variables in a dynamic profile. The dynamic profile obtains and replaces data for these variables from an incoming client data packet. You can specify these variables in the body of a dynamic profile without having to first define the variables at the `[dynamic-profiles profile-name variables]` hierarchy level.

Before you configure dynamic variables:

1. Create a basic dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 283.

2. Ensure that the router hardware is configured in the network to accept subscriber access.

To configure predefined internal variables in a dynamic profile:

1. Access the desired dynamic profile.

```
user@host# edit dynamic-profiles igmpProfile1
[edit dynamic-profiles profile1]
```

2. Configure the necessary internal variables.

```
[edit dynamic-profiles igmpProfile1]
user@host# set protocols igmp interface $junos-interface-name
```

For a complete list of supported predefined internal variables, see “Dynamic Variables Overview” on page 276

- Related Topics**
- Configuring a Basic Dynamic Profile on page 283
 - Configuring User-Defined Dynamic Variables in Dynamic Profiles on page 285
 - Dynamic Profiles Overview on page 275
 - Dynamic Variables Overview on page 276
 - Example: Firewall Dynamic Profile on page 294
 - Example: IGMP Dynamic Profile on page 293

Configuring User-Defined Dynamic Variables in Dynamic Profiles

This topic discusses how to configure the user-defined dynamic variables in a dynamic profile. You define user-defined variables for individual dynamic profiles at the `[dynamic-profiles profile-name variables]` hierarchy level. At this hierarchy level, you create an association between a variable call value (for example, `$junos-igmp-version`) that appears in the body of the dynamic profile and data associated with that call value that is managed in an externally configured server (for example, a RADIUS VSA managed on a RADIUS server) or defined as a default value in the `variables` stanza.

Before you configure dynamic variables:

1. Create a basic dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 283.

2. Ensure that the router is configured to enable communication between the client and the RADIUS server.

See “Specifying the Authentication and Accounting Methods for Subscriber Access” on page 19.

3. Configure all RADIUS values that you want the profiles to use when validating subscribers.

See “Configuring RADIUS Server Parameters for Subscriber Access” on page 21

To configure variables in a dynamic profile:

1. Access the `variables` stanza in the desired dynamic profile.

```
user@host# edit dynamic-profiles profile1 variables
[edit dynamic-profiles profile1 variables]
```

2. Specify a name to identify the variable.

The variable name can be any alphanumeric value. The name is an association to a variable in the dynamic profile configuration. For example, if you specify a variable name of “igmp-version” as the variable name, you must specify the call variable “\$igmp-version” in the dynamic profile configuration for the statement you want the variable to define.

```
[edit dynamic-profiles igmpProfile1variables]
```



```
user@host# set igmp-version
```

3. Configure the variable using one (or both) of the following methods:

- Specify a RADIUS attribute and RADIUS tag (when required) for the variable.

```
[edit dynamic-profiles igmpProfile1 variables]
```

```
user@host# set igmp-version radius vendor-id 4874 attribute 78
```

- Configure a default value for the variable.

```
[edit dynamic-profiles igmpProfile1variables]
```

```
user@host# set igmp-version default-value 3
```



NOTE: You can configure variables by either using the RADIUS method, the default value method, or both. If you choose to configure both a RADIUS attribute and a default value for the variable, the RADIUS attribute takes precedence over the default value. However, the dynamic profile applies the default value if the router cannot contact the RADIUS server or if the RADIUS server does not contain a value for the assigned attribute.

4. Configure the call variable in the dynamic profile.

```
[edit dynamic-profiles igmpProfile1]
```

```
user@host# set protocols igmp interface demux0 version $igmp-version
```



NOTE: The call variable must match the name of the variable that you configured in the `variables` stanza.

Related Topics

- Configuring a Basic Dynamic Profile on page 283
- Example: Configuring Dynamic Scheduling and Queuing for Subscriber Access on page 406
- Configuring Predefined Internal Dynamic Variables in Dynamic Profiles on page 284
- Dynamic Profiles Overview on page 275
- Dynamic Variables Overview on page 276
- Example: Firewall Dynamic Profile on page 294
- Example: IGMP Dynamic Profile on page 293

Configuring a Dynamic Profile for Client Access

This topic describes how to create a basic dynamic profile that enables DHCP clients to dynamically access the multicast network.

Before you configure dynamic profiles for initial client access:

1. Create a basic dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 283.

2. Configure the necessary router interfaces that you want accessing DHCP clients to use.

See “Subscriber Interface Overview” on page 305 for information about the types of interfaces you can use with dynamic profiles and how to configure them.

3. Ensure that the router is configured to enable communication between the client and the RADIUS server.

See “Specifying the Authentication and Accounting Methods for Subscriber Access” on page 19.

4. Configure all RADIUS values that you want the profiles to use when validating DHCP clients for access to the multicast network.

See “Configuring RADIUS Server Parameters for Subscriber Access” on page 21

To configure an initial client access dynamic profile:

1. Access an IGMP access profile.

```
user@host# edit dynamic-profiles access-profile
[edit dynamic-profiles access-profile]
user@host#
```

2. Define the IGMP interface with the interface variable.



NOTE: The variable value is replaced by the name of the interface over which the router received the DHCP message.

```
[edit dynamic-profiles access-profile]
user@host# set protocols igmp interface $junos-underlying-interface
```

3. (Optional) Enable accounting on the IGMP interface.

```
[edit dynamic-profiles access-profile protocols igmp interface
$junos-underlying-interface]
user@host# set accounting
```

4. Set the IGMP interface to remain enabled.

```
[edit dynamic-profiles access-profile protocols igmp interface
$junos-underlying-interface]
user@host# set disable:$junos-igmp-enable
```




NOTE: RADIUS is capable of disabling IGMP. By assigning the enable variable to the disable statement, you can ensure that IGMP remains enabled.

5. (Optional) Specify a group policy for the IGMP interface.

```
[edit dynamic-profiles access-profile protocols igmp interface
$junos-underlying-interface]
user@host# set group-policy report-reject-policy
```

6. (Optional) Enable immediate leave on the IGMP interface.

```
[edit dynamic-profiles access-profile protocols igmp interface
$junos-underlying-interface]
user@host# set immediate-leave:$junos-igmp-immediate-leave
```

7. (Optional) Disable the collection of IGMP join and leave even statistics on the IGMP interface.

```
[edit dynamic-profiles access-profile protocols igmp interface
$junos-underlying-interface]
user@host# set no-accounting
```

8. (Optional) Set the IGMP interface to obtain the IGMP version from RADIUS.

```
[edit dynamic-profiles access-profile protocols igmp interface
$junos-underlying-interface]
user@host# set version:$junos-igmp-version
```

- Related Topics**
- Configuring a Basic Dynamic Profile on page 283
 - Dynamic Profiles Overview on page 275

Configuring a Dynamic Profile for Various Levels of Services

This topic discusses how to create dynamic profiles to define various levels of service for DHCP clients.

Before you configure dynamic profiles for client services:

1. Create a basic dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 283.

2. Configure a dynamic profile that enables DHCP clients access to the network.

See “Configuring a Dynamic Profile for Client Access” on page 287



NOTE: You can create a basic dynamic profile that contains both access configuration and some level of basic service.

3. Ensure that the router is configured to enable communication between the client and the RADIUS server.

See “Specifying the Authentication and Accounting Methods for Subscriber Access” on page 19.

4. Configure all RADIUS values that you want the profiles to use when validating DHCP clients.

See “Configuring RADIUS Server Parameters for Subscriber Access” on page 21

To configure an initial client access dynamic profile:

1. Access the desired service profile.

```
user@host# set dynamic-profiles basic-service-profile
```

2. (Optional) Define any IGMP protocols values as described for creating a basic access profile to combine a basic service with access in a profile.

See “Configuring a Dynamic Profile for Client Access” on page 287.

3. (Optional) Specify any filters for the interface.

See “Dynamically Attaching Statically Created Filters” on page 367 or “Dynamically Attaching Filters Using RADIUS Variables” on page 368.

4. Define any CoS values for the service level you want this profile to configure on the interface.

- Related Topics**
- Configuring a Basic Dynamic Profile on page 283
 - Dynamic Profiles Overview on page 275

Modifying Dynamic Profiles

You use dynamic profiles to configure large groups of subscribers. However, after you have configured and applied dynamic profiles, use caution when modifying any dynamic profiles that are in use by active subscribers on the router. This section provides guidelines and procedures for modifying existing profiles and applying them to subscriber interfaces.

When modifying dynamic profiles, keep the following considerations in mind:

- Do not modify a dynamic profile when it is in use by active subscribers.
- Modifying a dynamic profile when it is in use by active subscribers can lead to unpredictable behavior.

When a dynamic profile is modified and committed, the router:

1. Logs a warning that the profiles are being modified and committed.
2. Determines whether the profile is currently being use by any subscriber.

3. If the profile is in use by a subscriber, the commit fails and the router logs errors to report the conflict.

To properly modify a dynamic profile:

1. Ensure that no subscribers are using the dynamic profile.
2. Create a new dynamic profile with a different name that contains the desired changes:

Original Profile

```
profile1 {
  interfaces {
    "$junos-interface-ifd-name" {
      unit "$junos-underlying-interface-unit" {
        family inet {
          filter {
            input "$junos-input-filter";
          }
        }
      }
    }
  }
}
```

Original DHCP Configuration

```
forwarding-options {
  dhcp-relay {
    traceoptions {
      flag all;
    }
    .....
    dynamic-profile profile1;
    .....
  }
}
```

New Profile

```
profile2 {
  interfaces {
    "$junos-interface-ifd-name" {
      unit "$junos-underlying-interface-unit" {
        family inet {
          filter {
            input "$junos-input-filter";
            output "$junos-output-filter; /* added output filter variable */";
          }
        }
      }
    }
  }
}
```


Modified DHCP Configuration

```

forwarding-options {
  dhcp-relay {
    traceoptions {
      flag all;
    }
    .....
    dynamic-profile profile2; /* Name changed from profile1 */
    .....
  }
}

```

3. Commit the configuration containing the modified profile.

The modified profile is used for any new subscribers that access the router.

- Related Topics**
- Configuring a Basic Dynamic Profile on page 283
 - Dynamic Profiles Overview on page 275

Chapter 15

Dynamic Profile Examples

- Example: IGMP Dynamic Profile on page 293
- Example: Firewall Dynamic Profile on page 294

Example: IGMP Dynamic Profile

In this example, IGMP is configured for subscriber access using user-defined variables and JUNOS internal variables.

The user-defined variables equate to RADIUS settings as follows:

User-Defined Variable Name	JUNOS Variable	RADIUS VSA Name	RADIUS Attribute Number	RADIUS Setting
var-igmp-version	\$var-igmp-version	IGMP-Version	26-78	3
var-igmp-access-grp	\$var-igmp-access-grp	IGMP-Access-Group-Name	26-71	"reject_igmp_225"
var-igmp-access-src-grp	\$var-igmp-access-src-grp	IGMP-Access-Source-Group-Name	26-72	"reject_igmp_115"

```
[edit dynamic-profiles profile-name]  
variables {  
  var-igmp-version {  
    mandatory;  
    radius {  
      vendor-id 4874 attribute 78;  
    }  
  }  
  var-igmp-access-grp {  
    mandatory;  
    radius {  
      vendor-id 4874 attribute 71;  
    }  
  }  
  var-igmp-access-src-grp {  
    mandatory;  
    radius {  
      vendor-id 4874 attribute 72;  
    }  
  }  
}
```



```

}
interfaces {
  demux0 {
    unit "$junos-interface-unit" {
      demux-options {
        underlying-interface "$junos-underlying-interface";
      }
      family inet {
        demux-source {
          $junos-subscriber-ip-address;
        }
        unnumbered-address lo0.0 preferred-source-address 20.21.0.1;
      }
    }
  }
}
protocols {
  igmp {
    interface "$junos-interface-name" {
      version "$var-igmp-version";
      group-policy [ "$var-igmp-access-grp" "$var-igmp-access-src-grp" ];
    }
  }
}

```



NOTE: You must also configure any global IGMP parameters.

Example: Firewall Dynamic Profile

In this example, dynamic firewall is configured for subscriber access using user-defined variables and JUNOS internal variables.

The user-defined variables equate to RADIUS settings as follows:

User-Defined Variable Name	JUNOS Variable	RADIUS VSA Name	RADIUS Attribute Number	RADIUS Setting
inputFilterName	\$inputFilterName	Ingress-Policy-Name	26-10	upstrm1
outputFilterName	\$outputFilterName	Egress-Policy-Name	26-11	dnstrm1

```

variables {
  inputFilterName {
    radius {
      vendor-id 4874 attribute 10;
    }
  }
  outputFilterName {
    radius {
      vendor-id 4874 attribute 11;
    }
  }
}

```



```

    }
  }
  interfaces {
    demux0 {
      unit "$junos-interface-unit" {
        demux-options {
          underlying-interface "$junos-underlying-interface";
        }
        family inet {
          demux-source {
            $junos-subscriber-ip-address;
          }
          filter {
            input "$inputFilterName";
            output "$outputFilterName";
          }
          unnumbered-address lo0.0 preferred-source-address 20.21.0.1;
        }
      }
    }
  }
}

```



NOTE: You must also configure any global firewall parameters.

Chapter 16

Summary of Dynamic Profile Statements

attribute

Syntax	<code>attribute attribute-number;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> variables radius vendor-id]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Configure a RADIUS attribute as a variable in a dynamic profile.
Options	<i>attribute-number</i> —Number of the RADIUS attribute.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 397

default-value

Syntax	<code>default-value default-value;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> variables <i>variable-name</i>]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Configure a default value for a user-defined variable in a dynamic profile. The values that the system uses for these variables are applied when the subscriber authenticates.
Options	<i>default-value</i> —Default value for the variable.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 397

dynamic-profiles

```

Syntax  dynamic-profiles {
            profile-name {
              class-of-service {
                interfaces {
                  interface-name {
                  }
                  unit logical-unit-number {
                    output-traffic-control-profile profile-name;
                  }
                }
              }
              traffic-control-profiles profile-name {
                delay-buffer-rate (percent percentage | rate);
                guaranteed-rate (percent percentage | rate);
                scheduler-map map-name;
                shaping-rate (percent percentage | rate);
              }
            }
            interfaces {
              interface-name {
                unit logical-unit-number {
                  family family {
                    address address;
                    filter {
                      input filter-name;
                      output filter-name;
                    }
                    unnumbered-address interface-name {
                      preferred-source-address address;
                    }
                  }
                }
                vlan-id;
              }
              vlan-tagging;
            }
          }
          protocols {
            igmp {
              interface interface-name {
                accounting;
                disable;
                group-policy policy-name;
                immediate-leave;
                no-accounting;
                promiscuous-mode;
                ssm-map ssm-map-name;
                static {
                  group group {
                    source source;
                  }
                }
                version version;
              }
            }
          }
        }

```



```

variables {
  statement-name {
    default-value default-value;
    radius {
      vendor-id id {
        attribute attribute-number;
        tag tag-number;
      }
    }
  }
}

```

Hierarchy Level [\[edit\]](#)

Release Information Statement introduced in JUNOS Release 9.2.

Description Create dynamic profiles for use with DHCP client access.

Options *profile-name*—Name of the dynamic profile.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics

- Dynamic Profiles Overview on page 275
- Configuring a Basic Dynamic Profile on page 283

mandatory

Syntax	mandatory;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> variables <i>variable-name</i>]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	<p>Configure RADIUS to return a value for a user-defined variable. If RADIUS does not return a value for the variable, the dynamic profile fails.</p> <p>When a dynamic profile has mandatory and non-mandatory variables, configure mandatory variables first in the profile.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	■ Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 397

radius

Syntax	<pre>radius { vendor-id <i>id</i> { attribute <i>attribute-number</i>; tag <i>tag-number</i>; } }</pre>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> variables]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	<p>Configure RADIUS attribute variables in a dynamic profile.</p> <p>The statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	■ Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 397

tag

Syntax	<code>tag tag-number;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> variables radius vendor-id]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Configure a tag for a RADIUS attribute as a variable in a dynamic profile.
Options	<i>tag-number</i> —Tag number for the RADIUS attribute.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 397

variables

Syntax	<pre> variables { variable-name { mandatory; default-value default-value; radius { vendor-id id { attribute attribute-number; tag tag-number; } } } } </pre>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i>]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Configure user-defined variables in a dynamic profile. The values that the system uses for these variables are applied when the subscriber authenticates.
Options	<i>variable-name</i> —Name of the variable. The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 397

vendor-id

Syntax	vendor-id <i>id</i> ;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> variables radius]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Configure the vendor ID as a variable in a dynamic profile.
Options	<i>id</i> —Vendor ID for the RADIUS attribute. The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 397

Part 5

Subscriber Interfaces

- Subscriber Interface Overview on page 305
- Configuring Subscriber Interfaces for Dynamic Profiles on page 311
- Subscriber Interface Examples on page 319
- Subscriber Interfaces over Aggregated Ethernet Overview on page 323
- Configuring Subscriber Interfaces over Aggregated Ethernet on page 329
- Subscriber Interfaces over Aggregated Ethernet Examples on page 337
- Summary of Subscriber Interface Statements on page 343

Chapter 17

Subscriber Interface Overview

- Subscriber Interface Overview on page 305
- Static Subscriber Interfaces and VLAN Overview on page 306
- Subscriber Interfaces and IP Demux Overview on page 307
- MAC Address Validation for Subscriber Interfaces Overview on page 309

Subscriber Interface Overview

In this release, you can identify subscribers statically or dynamically.

To identify subscribers statically, you can reference a static VLAN interface in a dynamic profile. To identify subscribers dynamically, you create variables for IP demux interfaces that are dynamically created by DHCP when subscribers log in.

Statically Identifying Subscribers

Before you can configure static subscriber interfaces in a dynamic profile, you must first configure the logical interfaces on the router to which you expect clients to connect. After you have created the static interfaces, you can modify them by using dynamic profiles to apply configuration parameters.

You can also configure subscribers by creating sets of static IP demux interfaces that are not referenced in a dynamic profile.

When configuring the interfaces stanza within a dynamic profile, you use variables to specify the interface name and the logical unit value. When a DHCP subscriber sends a DHCP request to the interface, the dynamic profile replaces the **interface-name** and **unit** variables with the actual interface name and logical unit number of the interface that received the DHCP request. After this association is made, the router configures the interface with any CoS or protocol (that is, IGMP) configuration within the dynamic profile, or applies any input or output filter configuration that you have associated with that dynamic profile.

```
[edit dynamic-profiles]
interface-name {
  unit logical-unit-number {
    family family {
      address address;
      filter {
        input filter-name;
```



```

        output filter-name;
    }
    unnumbered-address interface-name {
        preferred-source-address address;
    }
    vlan-id;
}
vlan-tagging;
}

```

Dynamically Identifying Subscribers

You can configure IP demux interfaces to represent a subscriber interface in a dynamic profile. When a subscriber logs in using a DHCP access method, the demux interface is dynamically created.

You specify variables for the unit number, the name of the underlying interface, and the IP address in the dynamic profile. These variables are replaced with the values that are supplied by DHCP when the subscriber logs in.

- Related Topics**
- Static Subscriber Interfaces and VLAN Overview on page 306
 - Subscriber Interfaces and IP Demux Overview on page 307

Static Subscriber Interfaces and VLAN Overview

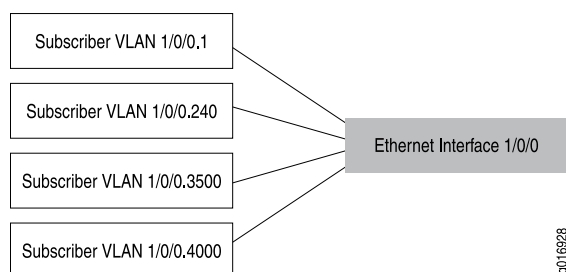
This topic describes the topology for configuring subscriber interfaces over static VLAN interfaces in the current release.

In a dynamic profile, you can configure VLAN subscriber interfaces over the following statically created logical interface types:

- GE—Gigabit Ethernet
- XE—10-Gigabit Ethernet
- AE—Aggregated Ethernet

We recommend that you configure each subscriber on a statically created VLAN.

Figure 5 on page 307 shows an example of subscriber interfaces on an individual VLAN.

Figure 5: VLAN Subscriber Interfaces

You can further separate VLANs on subscriber interfaces by configuring a VLAN interface as the underlying interface for a set of IP demux interfaces.

- Related Topics**
- Configuring a Subscriber Interface with a Static VLAN Interface on page 312
 - For more information about IP demux interfaces, see Subscriber Interfaces and IP Demux Overview on page 307

Subscriber Interfaces and IP Demux Overview

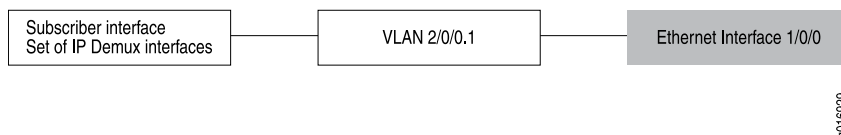
You can create logical subscriber interfaces using static or dynamic IP demux interfaces. IP demultiplexing (demux) interfaces are logical interfaces that share a common, underlying logical interface. IP demux interfaces can be used to identify specific subscribers or to separate individual circuits.

The subscriber interfaces can provide different levels of services for individual subscribers in an access network. For example, you can apply CoS parameters for each subscriber.

Interface Sets of Static Demux Interfaces

Static demux interfaces can be grouped to create individual subscriber interfaces using interface sets. Interface sets enable you to provide the same level of service for a group of subscribers; for example, all residential subscribers who receive the basic data service.

Figure 6 on page 307 shows a subscriber interface configured using a set of IP demux interfaces with an underlying VLAN interface.

Figure 6: IP Demux Subscriber Interface

Dynamic Demux Interfaces

You can configure IP demux interfaces to represent a dynamic subscriber interface in a dynamic profile.

Demux interfaces are dynamically created by a DHCP access method when the underlying interface for the demux interface is configured for the access method. The DHCP access model creates the demux interface with the subscriber's assigned IP address.

To configure the demux interface in the dynamic profile, you specify variables for the unit number, the name of the underlying interface, and the IP address. These variables are replaced with the values that are supplied by DHCP when the subscriber logs in.

Guidelines for Configuring IP Demux Interfaces for Subscriber Access

When you configure static or dynamic IP demux interfaces for subscriber access, consider the following guidelines:

- You can only configure interface sets of static IP demux interfaces and dynamic demux interfaces on MX-series routers. Hierarchical and per-unit scheduling is supported for dynamically created demux interfaces on the EQ DPC.
- You can configure only one **demux0** interface per chassis, but you can define logical demux interfaces on top of it (for example, **demux0.1**, **demux0.2**, and so on).
- You must associate demux interfaces with an underlying logical interface.



NOTE: IP demux interfaces currently support only Gigabit Ethernet, Fast Ethernet, and 10-Gigabit Ethernet underlying interfaces.

- You cannot use a dynamic demux interface to represent multiple subscribers in a dynamic profile attached to an interface. One dynamic demux interface represents one subscriber. Do not configure the **aggregate-clients** option when attaching a dynamic profile to a demux interface for DHCP.

Related Topics

- [Configuring a Subscriber Interface Using a Set of Static IP Demux Interfaces on page 313](#)
- [Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 314](#)
- [CoS and Static IP Demux Interface Set Overview on page 378](#)
- For more information about static IP demux interfaces and other configuration guidelines, see the *JUNOS Network Interfaces Configuration Guide*

MAC Address Validation for Subscriber Interfaces Overview

MAC address validation enables the router to validate that received packets contain a trusted IP source and an Ethernet MAC source address.

Configuring MAC address validation can provide additional validation when subscribers access billable services. MAC address validation provides additional security by enabling the router to drop packets that do not match, such as packets with spoofed addresses.

When subscribers log in, they are automatically assigned IP addresses by DHCP. The router detects the valid IP source and MAC source addresses for incoming packets and forwards the packets regardless of which subscriber originated the packet.

Supported Types of Subscriber Interfaces

MAC address validation is supported on statically created Ethernet interfaces and dynamically created IP demux interfaces on MX-series routers.

Trusted Addresses

A trusted address tuple is a 32-bit IP address and a 48-bit MAC address. Prefixes and ranges are not supported.

The IP source address and the MAC source address used for validation must be from a trusted source.

All static ARP addresses configured through the CLI are trusted addresses; dynamic ARP addresses are not considered trusted addresses.

Addresses dynamically created through a DHCP local server or DHCP relay are also trusted addresses. When a DHCP server and client negotiate an IP address, the resulting IP address and MAC address tuple is trusted. Each DHCP subscriber can generate more than one address tuple.

Each MAC address can have more than one IP address, which can result in more than one valid tuple. Each IP address must map to one MAC address.

Types of MAC Address Validation

You can configure two types of MAC address validation:

- Loose—Forwards packets when both the IP source address and the MAC source address match one of the trusted address tuples.

Drops packets when the IP source address matches one of the trusted tuples, but the MAC address does not support the MAC address of the tuple. The system processes this packet as spoofed.

Continues to forward packets when the source address of the incoming packet does not match any of the trusted IP addresses.

- **Strict**—Forwards packets when both the IP source address and the MAC source address match one of the trusted address tuples.

Drops packets when the MAC address does not match the tuple's MAC source address, or when IP source address of the incoming packet does not match any of the trusted IP addresses.

When you configure MAC address validation for demux interfaces in a dynamic profile and specify either **loose** or **strict** validation, the resulting behavior is always loose validation. To enable strict behavior for a dynamic demux interface, you must configure strict validation for the underlying interface.

Related Topics ■ [Configuring MAC Address Validation for Subscriber Interfaces on page 315](#)

Chapter 18

Configuring Subscriber Interfaces for Dynamic Profiles

- Configuring Static Subscriber Interfaces in Dynamic Profiles on page 311
- Configuring a Subscriber Interface Using a Set of Static IP Demux Interfaces on page 313
- Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 314
- Configuring MAC Address Validation for Subscriber Interfaces on page 315

Configuring Static Subscriber Interfaces in Dynamic Profiles

In this release, you can use dynamic profiles to configure statically created logical interfaces. Dynamic profiles enable you to dynamically apply configured values (including CoS, IGMP, or filter configuration) to the static interfaces, making them easier to manage.

To configure static interfaces, you must first configure the interfaces on the router to which you expect subscribers to connect.

The subscriber access feature supports the following statically-created interface types in dynamic profiles:

- GE—Gigabit Ethernet
- XE—10 Gigabit Ethernet
- AE—Aggregated Ethernet

This topic contains the following sections:

- Configuring a Subscriber Interface with a Static VLAN Interface on page 312
- Associating Dynamic Profiles with Statically Created Interfaces on page 312

Configuring a Subscriber Interface with a Static VLAN Interface

This topic describes how to configure a subscriber interface with a static VLAN interface.

After you configure the static VLAN interface, you can reference it in a dynamic profile.

To configure a subscriber interface over a VLAN:

1. Configure the static VLAN interface and enable VLAN tagging.

```
[edit interfaces]
ge-5/0/0 {
  vlan-tagging;
}
```

2. Configure the units and assign the VLAN IDs.

```
unit 1 {
  proxy-arp;
  vlan-id 1;
  family inet {
    unnumbered-address lo0.0 preferred-source-address 192.1.1.1;
  }
}
unit 2 {
  proxy-arp;
  vlan-id 2;
  family inet {
    unnumbered-address lo0.0 preferred-source-address 192.1.1.1;
  }
}
```

Associating Dynamic Profiles with Statically Created Interfaces

When configuring the interfaces stanza within a dynamic profile, you use variables to specify the interface name and the logical unit value. When a DHCP subscriber sends a DHCP request to the interface, the dynamic profile replaces the `interface-name` and `unit` variables with the actual interface name and logical unit number of the interface that received the DHCP request.



NOTE: Configuration of the `interface-name` and `unit` statements within the `interfaces` stanza is required for a dynamic profile to function.

To configure the dynamic profile `interfaces` stanza with `interface-name` and `unit` variables:

1. Access the profile.

```
user@host# edit dynamic-profiles basic-profile
```


2. Specify the `interface-name` variable.

```
[edit dynamic-profiles basic-profile]
user@host# set interfaces $junos-interface-ifd-name
```

3. Specify the unit variable.

```
[edit dynamic-profiles basic-profile]
user@host# set unit $junos-underlying-interface-unit
```

- Related Topics**
- Static Subscriber Interfaces and VLAN Overview on page 306
 - For information about configuring logical interfaces and static VLAN interfaces, see the *JUNOS Network Interfaces Configuration Guide*

Configuring a Subscriber Interface Using a Set of Static IP Demux Interfaces

You can create logical subscriber interfaces from IP demux interfaces. IP demultiplexing (demux) interfaces are logical interfaces that share a common, underlying logical interface. IP demux interfaces can be used to identify specific subscribers or to separate individual circuits.

You can group individual subscriber interfaces using interface sets to provide the same level of service for a group of subscribers; for example, all residential subscribers who receive the basic data service. Interface sets can be defined as a list of logical interfaces (unit 0, unit 1, and so on).

To configure a group of static IP demux interfaces:

1. Configure the interface set.

```
interfaces {
  interface-set demux-set {
    interface demux0 {
      unit 0;
      unit 1;
    }
  }
}
```

2. Define the units of the interface set.

```
demux0 {
  unit 0 {
    demux-options {
      underlying-interface ge-2/0/1.1;
    }
    family inet {
      demux-source {
        1.1.1.0/24;
      }
      address 1.1.1.1/24;
    }
  }
}
```



```

unit 1 {
    demux-options {
        underlying-interface ge-2/0/1.1;
    }
    family inet {
        demux-source {
            1.1.2.0/24;
        }
        address 1.1.2.1/24;
    }
}

```

- Related Topics**
- Configuring CoS on a Set of Static IP Demux Interfaces on page 400
 - Subscriber Interfaces and IP Demux Overview on page 307
 - For information about the `edit interfaces` hierarchy and the `interface-set` statement, see the *JUNOS Network Interfaces Configuration Guide*

Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles

You can configure dynamic subscriber interfaces using IP demux interfaces.

To enable the dynamic demux interface to be created by DHCP, you configure the demux options in a dynamic profile. Dynamic profiles enable you to dynamically apply configured values (including CoS, IGMP, or filter configuration) to the dynamic interfaces, making them easier to manage.

Before you begin:

- Configure the dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 283.

To configure dynamic subscriber interfaces:

1. Specify that you want to configure the `demux0` interface in the dynamic profile.

```
user@host# edit dynamic-profiles business-profile interfaces demux0
```

2. Configure the unit for the `demux0` interface.

- a. Configure the variable for the unit number of the `demux0` interface.

The variable is dynamically replaced with the unit number that DHCP supplies when the subscriber logs in.

```

[edit dynamic-profiles business-profile demux0]
user@host# edit unit "$junos-interface-unit"

```

- b. Configure the variable for the underlying interface of the demux interfaces.

The variable is dynamically replaced with the underlying interface that DHCP supplies when the subscriber logs in.

```
[edit dynamic-profiles business-profile unit "$junos-interface-unit"]
user@host# set demux-options underlying-interface
"$junos-underlying-interface"
```

3. Configure the family for the demux interfaces.
 - a. Specify that you want to configure the family.

```
[edit dynamic-profiles business-profile interfaces demux0 unit
"$junos-interface-unit"]
user@host# edit family inet
```

- b. Configure the unnumbered address for the family.

```
[edit dynamic-profiles business-profile interfaces demux0 unit
"$junos-interface-unit" family inet]
user@host# set unnumbered-address 100.0
```

- c. Configure the variable for the IP address of the demux interface.

The variable is dynamically replaced with the IP address that DHCP supplies when the subscriber logs in.

```
[edit dynamic-profiles business-profile unit "$junos-interface-unit"]
user@host# set demux-source "$junos-subscriber-ip-address"
```

- Related Topics**
- Subscriber Interfaces and IP Demux Overview on page 307
 - Configuring MAC Address Validation for Dynamic Subscriber Interfaces on page 317
 - Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 62
 - Example: Configuring Dynamic Subscriber Interfaces on IP Demux Interfaces on page 320

Configuring MAC Address Validation for Subscriber Interfaces

This topic describes how to configure MAC address validation for subscriber interfaces in dynamic profiles on MX-series routers.

The subscriber interfaces can be statically created and associated with a dynamic profile (for example, VLAN interfaces) or dynamically created in the dynamic profile (such as IP demux interfaces).

By default, MAC address validation is disabled.

This topic contains the following sections:

- Configuring MAC Address Validation for Static Subscriber Interfaces on page 316
- Configuring MAC Address Validation for Dynamic Subscriber Interfaces on page 317

Configuring MAC Address Validation for Static Subscriber Interfaces

This topic describes how to configure MAC address validation for static subscriber interfaces in dynamic profiles on MX-series routers.

Before you begin:

- Configure the dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 283.

To configure MAC address validation on static subscriber interfaces:

1. Configure the static VLAN interface.

```
[edit interfaces]
user@host# set fe-0/0/0 unit 0 family inet
```

2. Configure the type of MAC address validation for the interface.

- To configure loose validation:

```
[edit interfaces fe-0/0/0 unit 0 family inet]
user@host# set mac-validate loose
```

- To configure strict validation:

```
[edit interfaces fe-0/0/0 unit 0 family inet]
user@host# set mac-validate strict
```


After you configure MAC address validation:

- Associate the static VLAN interface with the dynamic profile.

See “Associating Dynamic Profiles with Statically Created Interfaces” on page 312.

Configuring MAC Address Validation for Dynamic Subscriber Interfaces

This topic describes how to configure MAC address validation for subscriber interfaces created on demux interfaces in dynamic profiles on MX-series routers.

When you configure MAC address validation for demux interfaces in a dynamic profile and specify either **loose** or **strict** validation, the resulting behavior is always loose validation. To enable strict behavior for a dynamic demux interface, you must configure strict validation for the underlying interface.

Before you begin:

- Configure the dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 283.

- Configure the dynamic demux interface.

See “Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles” on page 314.

To configure MAC address validation for a dynamic subscriber interface:

1. Configure loose validation for the demux interface.

```
[edit dynamic-profiles interfaces unit “$junos-interface-unit” family inet]
user@host# set mac-validate loose
```

2. (Optional) Configure strict validation for the underlying interface.

```
[edit interfaces fe-0/0/0 unit 0 family inet]
user@host# set mac-validate strict
```

- Related Topics**
- MAC Address Validation for Subscriber Interfaces Overview on page 309
 - Example: Configuring Dynamic Subscriber Interfaces on IP Demux Interfaces on page 320

Chapter 19

Subscriber Interface Examples

- Example: Configuring a Static Subscriber Interface on a Gigabit Ethernet VLAN Interface (Multiple Logical Units) on page 319
- Example: Configuring a Static Subscriber Interface on a Gigabit Ethernet VLAN Interface on page 319
- Example: Configuring a Static Subscriber Interface on a Gigabit Ethernet VLAN Interface (No Autonegotiation) on page 320
- Example: Configuring a Static Subscriber Interface with a Loopback on page 320
- Example: Configuring Dynamic Subscriber Interfaces on IP Demux Interfaces on page 320

Example: Configuring a Static Subscriber Interface on a Gigabit Ethernet VLAN Interface (Multiple Logical Units)

```
[edit interfaces]
ge-5/0/0 {
  vlan-tagging;
  unit 1 {
    proxy-arp;
    vlan-id 1;
    family inet {
      unnumbered-address lo0.0 preferred-source-address 192.1.1.1;
    }
  }
  unit 2 {
    proxy-arp;
    vlan-id 2;
    family inet {
      unnumbered-address lo0.0 preferred-source-address 192.1.1.1;
    }
  }
}
```

Related Topics ■ Configuring Static Subscriber Interfaces in Dynamic Profiles on page 311

Example: Configuring a Static Subscriber Interface on a Gigabit Ethernet VLAN Interface

```
[edit interfaces]
```



```

ge-5/2/0 {
  vlan-tagging;
  unit 1 {
    vlan-id 1;
    family inet {
      address 192.2.1.1/24;
    }
  }
}

```

Related Topics ■ [Configuring Static Subscriber Interfaces in Dynamic Profiles on page 311](#)

Example: Configuring a Static Subscriber Interface on a Gigabit Ethernet VLAN Interface (No Autonegotiation)

```

[edit interfaces]
ge-5/1/9 {
  vlan-tagging;
  gigether-options {
    no-auto-negotiation;
  }
  unit 2004 {
    vlan-id 2004;
    family inet {
      address 222.0.0.1/22;
    }
  }
}

```

Related Topics ■ [Configuring Static Subscriber Interfaces in Dynamic Profiles on page 311](#)

Example: Configuring a Static Subscriber Interface with a Loopback

```

lo0 {
  unit 0 {
    family inet {
      address 192.1.1.1/32;
    }
  }
}

```

Related Topics ■ [Configuring Static Subscriber Interfaces in Dynamic Profiles on page 311](#)

Example: Configuring Dynamic Subscriber Interfaces on IP Demux Interfaces

This example shows how to configure dynamic subscriber interfaces on IP demux interfaces.

DHCP dynamically creates the demux interface when a subscriber logs in.

To configure subscribers on dynamic demux interfaces:

1. Configure the static VLAN as the underlying interface.

```

interfaces {
  ge-0/3/0 {
    vlan-tagging;
    unit 0 {
      vlan-id 0;
      demux-source inet;
      family inet {
        unnumbered-address lo0.0;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 90.1.1.1/24;
      }
    }
  }
}

```

2. Configure the creation of demux interfaces in the dynamic profile.

```

dynamic-profiles {
  subscriber profile {
    interfaces {
      demux0 {
        "$junos-interface-ifd-name" {
          unit "$junos-interface-unit" {
            demux-options {
              underlying-interface "$junos-underlying-interface";
            }
            family inet {
              demux-source {
                $junos-subscriber-ip-address;
              }
              filter {
                input ingressFilter;
                output egressFilter;
              }
              mac-validate loose;
            }
          }
        }
      }
    }
  }
}

```

3. Configure the access method to dynamically create the demux interface.

DHCP relay is the access method used in this example.

```

forwarding-options {
  dhcp-relay {

```



```

traceoptions {
  flag all;
}
server-group {
  router {
    100.20.42.1;
  }
  dynamic-profile subscriber-profile aggregate-clients;
  active-server-group erx;
  group one {
    interface ge-0/0/2.0 upto ge-0/0/2.4000;
    interface-client-limit 200
  }
}
}

```

4. Configure the interface for DHCP.

```

interfaces {
  traceoptions {
    flag all;
  }
  ge-0/0/2 {
    unit 0 {
      demux-source inet;
      family inet {
        unnumbered-address lo0.0;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 100.20.32.2/32;
      }
    }
  }
}

```

- Related Topics**
- Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 314
 - Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 62

Chapter 20

Subscriber Interfaces over Aggregated Ethernet Overview

- Static VLAN Subscriber Interfaces over Aggregated Ethernet Overview on page 323
- Static or Dynamic IP Demux Subscriber Interfaces over Aggregated Ethernet Overview on page 325

Static VLAN Subscriber Interfaces over Aggregated Ethernet Overview

Beginning with this release of JUNOS software, you can configure static or dynamic hierarchical class of service (CoS) on a subscriber interface represented by a static virtual LAN (VLAN) stacked on a two-link aggregated Ethernet logical interface. You must configure the aggregated Ethernet logical interface on Enhanced Queuing Dense Port Concentrators (EQ DPCs) in an MX-series router. Prior to this release of JUNOS software, static VLAN subscriber interfaces were supported only over Gigabit Ethernet, Fast Ethernet, and 10-Gigabit Ethernet links that were not part of an aggregated Ethernet bundle.

A static VLAN subscriber interface over aggregated Ethernet can also support one-to-one active/backup link redundancy, depending on how you configure the underlying aggregated Ethernet interface.

To configure a static VLAN subscriber interface over aggregated Ethernet, make sure you understand the following concepts.

- Guidelines for Configuring a Static VLAN Subscriber Interface over Aggregated Ethernet for Static or Dynamic CoS Support on page 324
- Guidelines for Configuring an Aggregated Ethernet Logical Interface to Support a Static VLAN Subscriber Interface on page 324

Guidelines for Configuring a Static VLAN Subscriber Interface over Aggregated Ethernet for Static or Dynamic CoS Support

Keep the following guidelines in mind when configuring static or dynamic CoS for a subscriber interface on a static VLAN stacked on a two-link aggregated Ethernet logical interface:

- Configure the aggregated Ethernet logical interface over two physical interfaces capable of performing hierarchical scheduling, which is only supported for ports on EQ DPCs in MX-series routers.
- Configure the aggregated Ethernet logical interface to operate in hierarchical scheduler mode instead of in the default per-unit scheduler mode.
- Configure the aggregated Ethernet logical interface with both underlying links operating in link-protect mode.
- Configure the aggregated Ethernet logical interface with the Link Aggregation Control Protocol (LACP) active.
- You can apply static or dynamic CoS characteristics to a scheduler node at the aggregated Ethernet logical interface or its underlying physical interface, but not at an interface set.



NOTE: For this release of JUNOS software, hierarchical CoS is not supported for dynamic VLAN interfaces over aggregated Ethernet links, nor for IP demultiplexing (demux) interfaces over aggregated Ethernet links.

Guidelines for Configuring an Aggregated Ethernet Logical Interface to Support a Static VLAN Subscriber Interface

The following guidelines for configuring an aggregated Ethernet logical interface also apply to configuring a static VLAN subscriber interface stacked on a two-link aggregated Ethernet logical interface:

- If you need to support one-to-one active/backup link redundancy, configure the aggregated Ethernet interface in link protection mode, which requires that the two underlying physical interfaces be designated as primary and backup links.
- In addition, if you need to support one-to-one active/backup link redundancy at the DPC level, configure the aggregated Ethernet interface on physical interfaces that reside on different EQ DPCs.



NOTE: One-to-one active/backup DPC redundancy is also supported with firewall filters and policy filters for static non-VLAN interfaces configured on an aggregated Ethernet logical interfaces, provided LACP is not active.

Related Topics

- Static Subscriber Interfaces and VLAN Overview on page 306
- Configuring a Static VLAN Subscriber Interface over Aggregated Ethernet on page 329

- Example: Configuring a Static Subscriber Interface on a VLAN Interface over Aggregated Ethernet on page 337
- Guidelines for Configuring CoS for Subscriber Access on page 388
- CoS for Subscriber Access Overview on page 377

Static or Dynamic IP Demux Subscriber Interfaces over Aggregated Ethernet Overview

Beginning with this release of JUNOS software, you can configure a subscriber interface using a static or dynamic IP demultiplexing (demux) logical interface stacked on an aggregated Ethernet logical interface. You must configure the aggregated Ethernet logical interface on Enhanced Queuing Dense Port Concentrators (EQ DPCs) in an MX-series router. Prior to this release of JUNOS software, IP demux subscriber interfaces were supported only over Gigabit Ethernet, Fast Ethernet, and 10-Gigabit Ethernet links that were not part of an aggregated Ethernet bundle.

Subscriber interfaces on static or dynamic IP demux interfaces can be used to identify specific subscribers (authenticated users) in an access network or to separate individual circuits. A subscriber interface on a static or dynamic IP demux interface over aggregated Ethernet can support one-to-one active/backup link redundancy or traffic load balancing, depending on how you configure the underlying aggregated Ethernet interface.

To configure a static or dynamic IP demux subscriber interface over aggregated Ethernet, make sure you understand the following concepts:

- Relationship Between an IP Demux Subscriber Interface and the Underlying Aggregated Ethernet Logical Interface on page 325
- Options for Aggregated Ethernet Logical Interfaced That Support IP Demux Subscriber Interfaces on page 326
- Features Supported with Static or Dynamic IP Demux Subscriber Interfaces over Aggregated Ethernet on page 326

Relationship Between an IP Demux Subscriber Interface and the Underlying Aggregated Ethernet Logical Interface

The following points describe the relationship between a static or dynamic IP demux subscriber interface and the underlying aggregated Ethernet logical interface:

- An aggregated Ethernet logical interface is considered active when it has two or more active members. Otherwise, the aggregated Ethernet logical interface is considered inactive.
- A static or dynamic IP demux subscriber interface stacked on an aggregated Ethernet logical interface is considered active — and the subscriber interface demultiplexes packets received on all child interfaces in the aggregated Ethernet bundle — when the underlying Ethernet bundle is active.

Options for Aggregated Ethernet Logical Interfaced That Support IP Demux Subscriber Interfaces

Traffic forwarding through a IP demux logical interface is dependent on the configuration of the underlying logical interface. Using an aggregated Ethernet logical interface as the underlying interface for a static or dynamic IP demux subscriber interface provides you with the following options:

1:1 Active/Backup Link Redundancy

If you need to support one-to-one active/backup link redundancy, configure the aggregated Ethernet interface in link protection mode, which requires that two underlying physical interfaces be designated as primary and backup links. In addition, if you need to support one-to-one active/backup link redundancy at the DPC level, configure the aggregated Ethernet interface on physical interfaces that reside on different EQ DPCs.

Load Balancing

If you need to support traffic load balancing instead of redundancy, configure the aggregated Ethernet interface to operate in Link Aggregation Control Protocol (LACP) active mode. When using LACP link protection, you can configure only two member links to an aggregated Ethernet interface: one active and one standby. The JUNOS implementation of the IEEE 802.3ad standard balances traffic across the member links within an aggregated Ethernet bundle based on the Layer 3 information carried in the packet.

For more information about aggregated Ethernet interfaces, see the *JUNOS Network Interfaces Configuration Guide*.

Features Supported with Static or Dynamic IP Demux Subscriber Interfaces over Aggregated Ethernet

Table 26 on page 326 lists key subscriber access features supported with static or dynamic IP demux subscriber interfaces, organized by type of underlying logical interface:

- Aggregated Ethernet
- Non-aggregated Ethernet (Gigabit Ethernet, Fast Ethernet, or 10-Gigabit Ethernet)

In this release of JUNOS software, no feature limitations are specific to IP demultiplexing. Instead, IP demux interfaces over aggregated Ethernet are subject to the same scaling and configuration limitations inherent to aggregated Ethernet logical interfaces.

Table 26: Features Supported with Static or Dynamic IP Demux Subscriber Interfaces

Feature	Static or Dynamic IP Demux Subscriber Interface	
	Aggregated Ethernet Underlying Interface	Non-aggregated Underlying Logical Interface
Protocol family support	IPv4 only	IPv4 only
Per-subscriber firewall filtering and statistics	Supported	Supported
Hierarchical CoS	No	Supported

Table 26: Features Supported with Static or Dynamic IP Demux Subscriber Interfaces (*continued*)

Feature	Static or Dynamic IP Demux Subscriber Interface	
	Aggregated Ethernet Underlying Interface	Non-aggregated Underlying Logical Interface
Per-subscriber CoS parameters within the [edit dynamic-profiles <i>profile-name</i> protocols] hierarchy	No	Supported
Per-subscriber IGMP configuration within the [edit dynamic-profiles <i>profile-name</i> protocols] hierarchy	No	No

- Related Topics**
- Subscriber Interfaces and IP Demux Overview on page 307
 - Configuring a Static or Dynamic IP Demux Subscriber Interface over Aggregated Ethernet on page 331
 - Example: Configuring a Static Subscriber Interface on an IP Demux Interface over Aggregated Ethernet on page 340

Chapter 21

Configuring Subscriber Interfaces over Aggregated Ethernet

- Configuring a Static VLAN Subscriber Interface over Aggregated Ethernet on page 329
- Configuring a Static or Dynamic IP Demux Subscriber Interface over Aggregated Ethernet on page 331

Configuring a Static VLAN Subscriber Interface over Aggregated Ethernet

You can configure static or dynamic hierarchical class of service (CoS) on a subscriber link represented by a static virtual LAN (VLAN) stacked on a two-link aggregated Ethernet logical interface.

To configure a subscriber interface using a static VLAN interface over a two-link aggregated Ethernet logical interface:

1. Define the number of aggregated Ethernet interfaces on the router:

```
[edit]
chassis {
  aggregated-devices {
    ethernet {
      device-count number;
    }
  }
}
```

2. Configure the two-link aggregated Ethernet logical interface to serve as the underlying interface for the static VLAN subscriber interface.

```
[edit]
interfaces {
  ethernet-interface-name { # Configure the first link
    (fastether-options | gige-ether-options) { # Specify the EQ DPC port type
      802.3ad { # Specify the aggregated Ethernet logical interface
        aex; # Specify 0 through 15
        primary; # Optional: to support 1:1 active/backup redundancy
      }
    }
  }
  ethernet-interface-name { # Configure the second link
```



```

(fastether-options | ggether-options) {
  802.3ad {
    aex;
    backup; # Optional: to support 1:1 active/backup redundancy
  }
}
}

```



NOTE: Optionally, you can configure the aggregated Ethernet logical interface to support one-to-one active/backup link redundancy. However, you cannot configure the aggregated Ethernet logical interface to support load balancing with hierarchical CoS. For more information about configuring aggregated Ethernet interfaces, see the *JUNOS Network Interfaces Configuration Guide*.

3. Configure the two-link aggregated Ethernet logical interface to serve as the underlying interface for the static VLAN interface.

For the static VLAN interface to support static or dynamic hierarchical CoS, the link aggregation (LAG) bundle must operate in hierarchical scheduler mode, both links must operate in link-protect mode, and the Link Aggregation Control Protocol (LACP) must be active:

```

[edit]
interfaces {
  aex { # Configure the LAG bundle
    hierarchical-scheduler; # Enable hierarchical scheduler mode
    aggregated-ether-options {
      link-protection; # Enable static link protection
      minimum-links number;
      link-speed speed;
      lacp { # LACP "active" for hierarchical CoS
        active; # But LACP "passive" for firewall filters and policy filters
      }
    }
  }
}

```

4. Attach static or dynamic traffic shaping and scheduling parameters at the aggregated Ethernet logical interface or its underlying physical interface:

```

class-of-service { # H-CoS on AE with 1:1 link protection
  schedulers {
    scheduler-name { # Configure a scheduler
      ... scheduler_configuration ...
    }
    ... additional_scheduler_configurations ...
  }
  scheduler-maps {
    scheduler-map-name { # Configure a scheduler map
      forwarding-class class-name scheduler scheduler-name;
      ... additional_queue_configurations ...
    }
    ... additional_scheduler_map_configurations ...
  }
}

```



```

}
traffic-control-profiles {
  profile-name { # Configure a traffic-control profile
    scheduler-map scheduler-map-name;
    ... other_traffic_shaping_parameters ...
  }
  ... additional_traffic_control_profile_configurations ...
}
interfaces {
  aex { # Attach CoS parameters this AE bundle
    output-traffic-control-profile profile-name; # Underlying physical interface(s)
    unit logical-unit-number {
      output-traffic-control-profile profile-name; # Logical interface
    }
  }
}
}

```

You can include the statements at one of the following hierarchy levels:

- [edit]
- [edit dynamic-profiles *profile-name*]

- Related Topics**
- Static VLAN Subscriber Interfaces over Aggregated Ethernet Overview on page 323
 - Example: Configuring a Static Subscriber Interface on a VLAN Interface over Aggregated Ethernet on page 337
 - Guidelines for Configuring CoS for Subscriber Access on page 388
 - CoS for Subscriber Access Overview on page 377

Configuring a Static or Dynamic IP Demux Subscriber Interface over Aggregated Ethernet

You can configure a subscriber interface using a static or dynamic IP demultiplexing (demux) logical interface stacked on an aggregated Ethernet logical interface. Optionally, you can configure the aggregated Ethernet logical interface to support one-to-one active/backup link redundancy or traffic load balancing.

This topic includes the following tasks:

- Configuring the Number of Aggregated Ethernet Logical Interfaces on the Router on page 332
- Configuring Ethernet Links as Members of an Aggregated Ethernet Logical Interface for a Static or Dynamic IP Demux Subscriber Interface on page 332
- Configuring an Aggregated Ethernet Logical Interface to Support a Static or Dynamic IP Demux Subscriber Interface on page 333
- Configuring a Static IP Demux Subscriber Interface over an Aggregated Ethernet Logical Interface on page 334

- Configuring a Dynamic IP Demux Subscriber Interface over an Aggregated Ethernet Logical Interface on page 335
- Displaying Configuration Information About IP Demux Interfaces over Aggregated Ethernet on page 336

Configuring the Number of Aggregated Ethernet Logical Interfaces on the Router

To configure the underlying aggregated Ethernet logical interface for a static or dynamic IP demultiplexing (demux) subscriber interface:

- Define the number of aggregated Ethernet interfaces on the router:

```
[edit]
chassis {
  aggregated-devices {
    ethernet {
      device-count number;
    }
  }
}
```

Configuring Ethernet Links as Members of an Aggregated Ethernet Logical Interface for a Static or Dynamic IP Demux Subscriber Interface

To enable Ethernet links as members of an aggregated Ethernet logical interface that is to serve as the underlying interface for a static or dynamic IP demux subscriber interface:

- For each Ethernet link, specify the aggregated Ethernet logical interface name, *aex*. To configure, include the **802.3ad** configuration statement with the *aex* option at the [edit interfaces *ethernet-interface-name* fastether-options] or [edit interfaces *ethernet-interface-name* gigheter-options] hierarchy level:

```
[edit]
interfaces {
  ethernet-interface-name { # Configure the first link
    (fastether-options | gigheter-options) {
      802.3ad aex;
    }
  }
  ethernet-interface-name { # Configure the second link
    (fastether-options | gigheter-options) {
      802.3ad aex;
    }
  }
}
```




NOTE: Optionally, you can configure the aggregated Ethernet logical interface to support one-to-one active/backup link redundancy or traffic load balancing. For more information about configuring link protection (for active/backup link redundancy) or configuring multiple active links (for load balancing), see the *JUNOS Network Interfaces Configuration Guide*.

Configuring an Aggregated Ethernet Logical Interface to Support a Static or Dynamic IP Demux Subscriber Interface

To configure an aggregated Ethernet logical interface so that it can be used as the underlying logical interface for a static or dynamic IP demux interface:

- Enable demultiplexing of incoming traffic to the Ethernet links based on IPv4 destination or source addresses in the incoming packets. To configure, include either the `demux-destination (Underlying Interface)` configuration statement with the `inet` option or the `demux-source (Underlying Interface)` configuration statement with the `inet` option.
- Configure the IP address of each link in the aggregated Ethernet logical interface:
 - To configure the IP address, include the `address` configuration statement with the `inet` option.
 - To enable the local address to be derived from the specified interface, include the `unnumbered-address (IP Demux)` configuration statement with the `interface-name <preferred-source-address address>` option.

You can include these statements at the `[edit interfaces aex unit logical-unit-number]` hierarchy level for each Ethernet link.



NOTE: IP demux interfaces currently support only the Internet Protocol version 4 (IPv4) suite (`family inet`).

```
[edit]
interfaces {
  aex { # Example: 'ae5'
    unit logical-unit-number { # Specify the first link
      (demux-destination inet | demux-source inet);
      family inet {
        (address number | unnumbered-address interface-name
          <preferred-source-address address>);
      }
    }
    unit logical-unit-number { # Specify the second link
      (demux-destination inet | demux-source inet);
      family inet {
        (address number | unnumbered-address interface-name
          <preferred-source-address address>);
      }
    }
  }
}
```



```

    }
  }
}

```

For general information about configuring an IP demux underlying interface, or for specific information about configuring a preferred source address for unnumbered Ethernet or demux interfaces, see the *JUNOS Network Interfaces Configuration Guide*.

Configuring a Static IP Demux Subscriber Interface over an Aggregated Ethernet Logical Interface

To configure a static IP demux subscriber interface using an appropriately configured aggregated Ethernet logical interface as the underlying logical interface:

- Configure the IP demux interface on a physical device (of the underlying logical interface) represented by a logical unit number. To configure, include the `unit` configuration statement with the interface unit number at the static `[edit interface demux0]` hierarchy level.
- Specify the underlying interface on which the IP demux interface is running. To configure, include the `underlying-interface` configuration statement with the name of the aggregated Ethernet logical interface at the static `[edit interface demux0 unit logical-unit-number demux-options]` hierarchy level.
- Specify how ingress IPv4 traffic is to be demultiplexed based on packet destination or source addresses. To configure, include either the `demux-destination` (Demux Interface) or the `demux-source` statement (but not both) with one or more logical demultiplexing destination or source prefixes at the static `[edit interface demux0 unit logical-unit-number family inet]` hierarchy level. The prefixes are matched against the destination or source address of packets that the underlying interface receives. When a match occurs, the packet is processed as if it was received on the IP demux interface.
- (Optional) Specify a filter to apply when a packet is received or transmitted on the interface. To configure, include the `input` statement with one input firewall filter name or the `output` statement with one egress firewall filter name (or both statements) at the static `[edit interface demux0 unit logical-unit-number family inet filter]` hierarchy level.



NOTE: IP demux interfaces currently support only the Internet Protocol version 4 (IPv4) suite (`family inet`).

```

[edit]
interfaces {
  demux0 {
    unit logical-unit-number {
      demux-options {
        underlying-interface logical-interface-name;
      }
      family inet {
        (demux-destination destination-prefix | demux-source source-prefix);
        filter { # Optional

```



```

        input input-filter-name;
        output output-filter-name;
    }
}
}
}
}

```

For general information about configuring an IP demux underlying interface, see the *JUNOS Network Interfaces Configuration Guide*. For general information about configuring firewall filters, see the *JUNOS Policy Framework Configuration Guide*.

Configuring a Dynamic IP Demux Subscriber Interface over an Aggregated Ethernet Logical Interface

To configure a dynamic IP demux subscriber interface using an appropriately configured aggregated Ethernet logical interface as the underlying logical interface:

- Specify that the router is to configure the IP demux interface on a physical device (of the underlying logical interface) represented by a logical unit number obtained from DHCP when the subscriber logs in. To configure, include the `unit` configuration statement with the JUNOS internal variable `$junos-interface-unit` at the `[edit dynamic-profiles profile-name interface demux0]` hierarchy level.
- Specify that the underlying interface on which the IP demux interface is to run. To configure, include the `underlying-interface` configuration statement with the JUNOS internal variable `$junos-underlying-interface` at the `[edit dynamic-profiles profile-name interface demux0 unit $junos-interface-unit demux-options]` hierarchy level.
- Specify that router is to configure the subscriber interface with an IP address obtained from the DHCP server when the subscriber logs in. To configure, include the `demux-source` statement with the JUNOS internal variable `$junos-subscriber-ip-address` at the `[edit dynamic-profiles profile-name interface demux0 unit logical-unit-number family inet]` hierarchy level.
- (Optional) Specify a filter to apply when a packet is received or transmitted on the interface. To configure, include the `input` statement with one input firewall filter name or the `output` statement with one egress firewall filter name (or both statements) at the `[edit dynamic-profiles profile-name interface demux0 unit logical-unit-number family inet filter]` hierarchy level.



NOTE: IP demux interfaces currently support only the Internet Protocol version 4 (IPv4) suite (family inet).

For general information about configuring firewall filters, see the *JUNOS Policy Framework Configuration Guide*.

```

[edit]
dynamic-profiles {
  dynamic-profile-name {
    interfaces {

```



```

demux0 {
  unit "$junos-interface-unit" {
    demux-options {
      underlying-interface "$junos-underlying-interface";
    }
    family inet {
      demux-source {
        $junos-subscriber-ip-address;
      }
      filter {
        input input-filter-name;
        output output-filter-name;
      }
    }
  }
}

```

Displaying Configuration Information About IP Demux Interfaces over Aggregated Ethernet

To display configuration information that pertains to IP demux interfaces over aggregated Ethernet, issue any of the following operational commands:

- The output of the `show interfaces demux0` (Demux Interfaces) operational command can display an aggregated Ethernet logical interface as an underlying interface for an IP demux interface
- The output of the `show interfaces (Aggregated Ethernet)` operational command can indicate that an aggregated Ethernet logical unit is being used as an underlying interface for an IP demux interface and displays the logical demultiplexing destination or source family type. However, the command output does not display the supported IP demux logical interface.

Related Topics

- Subscriber Interfaces and IP Demux Overview on page 307
- Static or Dynamic IP Demux Subscriber Interfaces over Aggregated Ethernet Overview on page 325
- Example: Configuring a Static Subscriber Interface on an IP Demux Interface over Aggregated Ethernet on page 340

Chapter 22

Subscriber Interfaces over Aggregated Ethernet Examples

- Example: Configuring a Static Subscriber Interface on a VLAN Interface over Aggregated Ethernet on page 337
- Example: Configuring a Static Subscriber Interface on an IP Demux Interface over Aggregated Ethernet on page 340

Example: Configuring a Static Subscriber Interface on a VLAN Interface over Aggregated Ethernet

This example shows how you can configure a subscriber interface using a static virtual LAN (VLAN) stacked on a two-link aggregated Ethernet logical interface. In this example, the underlying aggregated Ethernet logical interface is configured for one-to-one active/backup redundancy at the DPC level, and per-subscriber static hierarchical class-of-service (CoS) is configured by applying CoS parameters at the aggregated Ethernet logical interface.

1. Define the number of aggregated Ethernet interfaces on the router.

In this example, only one aggregated Ethernet logical interface is configured on the router.

```
[edit]
chassis {
  aggregated-devices {
    ethernet {
      device-count 1;
    }
  }
}
```

2. Configure **ae0**, a two-link aggregated Ethernet logical interface to serve as the underlying interface for the static VLAN subscriber interface. In order to support hierarchical CoS, the physical ports must be on EQ DPCs in an MX-series router

In this example, the LAG bundle is configured for one-to-one active/backup link redundancy. To support link redundancy at the DPC level, the LAG bundle attaches ports from two different EQ DPCs.

```
[edit]
interfaces {
  ge-5/0/3 {
```



```

    gigaether-options {
      802.3ad {
        ae0;
        primary;
      }
    }
    ge-5/1/2 {
      gigaether-options {
        802.3ad {
          ae0;
          backup;
        }
      }
    }
  }
}

```

3. Configure ae0 to serve as the underlying interface for the static VLAN interface.

```

[edit]
interfaces {
  ae0 {
    hierarchical-scheduler;
    aggregated-ether-options {
      link-protection;
      minimum-links 1;
      link-speed 1g;
      lacp {
        active;
      }
    }
  }
}

```

4. Configure static traffic-shaping and scheduling parameters.

```

[edit]
class-of-service {
  forwarding-classes { # Associate queue numbers with class names
    queue 0 be;
    queue 1 e;
    queue 2 af;
    queue 3 nc;
  }
  schedulers { # Define output queue properties
    scheduler_be {
      transmit-rate percent 30;
      buffer-size percent 30;
    }
    scheduler_ef {
      transmit-rate percent 40;
      buffer-size percent 40;
    }
    scheduler_af {
      transmit-rate percent 25;
      buffer-size percent 25;
    }
  }
}

```



```

    }
    scheduler_nc {
        transmit-rate percent 5;
        buffer-size percent 5;
    }
}
scheduler-maps { # Associate queues with schedulers
    smap_2 {
        forwarding-class be scheduler_be;
        forwarding-class ef scheduler_ef;
        forwarding-class af scheduler_af;
        forwarding-class nc scheduler_nc;
    }
}
}

```

5. Attach static CoS to the physical and logical interfaces of the aggregated Ethernet interface.

In this example, three traffic control profiles are defined, but only two profiles are applied to the static VLAN subscriber interface over aggregated Ethernet:

- The `tcp_for_ae_device_pir_500m` profile defines a shaping rate, and it is applied to both of the underlying physical interfaces (`ge-5/0/3` and `ge-5/1/2`).
- The `tcp-for-ae_smap_video_pir_20m_delay_30m` profile defines a scheduler map, a shaping rate, and a delay buffer rate, and it is applied to one of the logical interfaces on the aggregated Ethernet bundle (`ae0.0`).

```

[edit]
class-of-service {
    traffic-control-profiles { # Configure traffic shaping and scheduling profiles
        tcp_for_ae_device_pir_500m {
            shaping-rate 20m;
        }
        tcp_for_ae_smap_video_pir_20m_delay_30m {
            scheduler-map smap_video;
            shaping-rate 20m;
            delay-buffer-rate 30m;
        }
        tcp_for_ae_smap_video_cir_50m_delay_75m {
            scheduler-map smap_video;
            guaranteed-rate 50m;
            delay-buffer-rate 75m;
        }
    }
}
interfaces { # Apply two traffic-control profiles to the LAG
    ae0 { # Two underlying physical interfaces on separate EQ DPCs
        output-traffic-control-profile tcp-for-ae_device_pir_500m;
        unit 0 { # One of the two logical interfaces on 'ae0'
            output-traffic-control-profile tcp-for-ae_smap_video_pir_20m_delay_30m;
        }
    }
}
}

```


- Related Topics**
- Static VLAN Subscriber Interfaces over Aggregated Ethernet Overview on page 323
 - Configuring a Static VLAN Subscriber Interface over Aggregated Ethernet on page 329
 - Guidelines for Configuring CoS for Subscriber Access on page 388
 - CoS for Subscriber Access Overview on page 377

Example: Configuring a Static Subscriber Interface on an IP Demux Interface over Aggregated Ethernet

This example shows how you can configure a subscriber interface using a static IP demultiplexing (demux) interface stacked on a two-link aggregated Ethernet logical interface. In this example, the underlying aggregated Ethernet logical interface is configured for one-to-one active/backup redundancy at the DPC level.

1. Define the number of aggregated Ethernet interfaces on the router.

In this example, only one aggregated Ethernet logical interface is configured on the router:

```
[edit]
chassis {
  aggregated-devices {
    ethernet {
      device-count 1;
    }
  }
}
```

2. Configure ae0, a two-link aggregated Ethernet logical interface to serve as the underlying interface for the static IP demux subscriber interface.

In this example, the LAG bundle is configured for one-to-one active/backup link redundancy. To support link redundancy at the DPC level, the LAG bundle attaches ports from two different EQ DPCs.

```
[edit]
interfaces {
  ge-5/0/3 {
    gigether-options {
      802.3ad {
        ae0;
        primary;
      }
    }
  }
  ge-5/1/2 {
    gigether-options {
      802.3ad {
        ae0;
        backup;
      }
    }
  }
}
```



```
}

```

3. Configure the aggregated Ethernet logical interface with link protection enabled, and specify the logical demultiplexing source family type for both the active and backup links.

```
[edit]
interfaces {
  ae0 {
    aggregated-ether-options {
      link-protection;
      minimum-links 1;
      link-speed 1g;
    }
    unit 0 {
      demux-source inet {
        family inet {
          address 20.1.1.0/24;
        }
      }
    }
    unit 1 {
      demux-source inet {
        family inet {
          address 20.1.1.1/24;
        }
      }
    }
  }
}
```

4. Configure the IP demux interface over the aggregated Ethernet logical interface.

```
[edit]
interfaces {
  demux0 {
    unit 101 {
      demux-options {
        underlying-interface ae0.0;
      }
      family inet {
        demux-source 10.1.0.0/16;
        address 1.1.1.0/24;
      }
    }
    unit 101 {
      demux-options {
        underlying-interface ae0.1;
      }
      family inet {
        demux-source 10.1.0.1/16;
        address 1.1.1.1/24;
      }
    }
  }
}
```

Related Topics ■ Subscriber Interfaces and IP Demux Overview on page 307

- Static or Dynamic IP Demux Subscriber Interfaces over Aggregated Ethernet Overview on page 325
- Configuring a Static or Dynamic IP Demux Subscriber Interface over Aggregated Ethernet on page 331

Chapter 23

Summary of Subscriber Interface Statements

address

Syntax address *address*;

Hierarchy Level [edit dynamic-profiles interfaces *interface-name* unit *logical-unit-number* family *family*],
[edit interfaces *interface-name* unit *logical-unit-number* family *family*],
[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*
family *family*],
[edit dynamic-profiles *profile-name* interfaces demux0 unit *logical-unit-number* family
family]

Release Information Statement introduced before JUNOS Release 7.4.
The [edit dynamic-profiles interfaces *interface-name* unit *logical-unit-number* family *family*]
hierarchy added in JUNOS Release 9.2.

Description Configure the interface address.

Options *address*—Address of the interface.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Topics ■ “Configuring the Protocol Family,” in *JUNOS Network Interfaces Configuration Guide*.
■ *JUNOS System Basics Configuration Guide*

demux0

Syntax

```

demux0 {
  unit logical-unit-number {
    demux-options {
      underlying-interface interface-name
    }
    family family {
      address address;
      demux-source {
        source-prefix;
      }
      filter {
        input filter-name;
        output filter-name;
      }
      mac-validate (loose | strict);
      unnumbered-address interface-name {
        preferred-source-address address;
      }
    }
  }
}

```

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces]

Release Information Statement introduced in JUNOS Release 9.0.
The [edit dynamic-profiles *profile-name*] hierarchy added in JUNOS Release 9.3.

Description Configure the logical demultiplexing (demux) interface in a dynamic profile.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Topics

- Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 314
- For information about static IP demux interfaces, see the *JUNOS Network Interfaces Configuration Guide*

demux-options

Syntax	demux-options { underlying-interface <i>interface-name</i> }
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces demux0 <i>interface-name</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced in JUNOS Release 9.0. The [edit dynamic-profiles <i>profile-name</i>] hierarchy added in JUNOS Release 9.3.
Description	Configure logical demultiplexing (demux) interface options in a dynamic profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 314 ■ For information about static IP demux interfaces, see the <i>JUNOS Network Interfaces Configuration Guide</i>

demux-source

Syntax	demux-source { <i>source-address</i> ; }
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family <i>family</i>]
Release Information	Statement introduced in JUNOS Release 9.0. The [edit dynamic-profiles <i>profile-name</i>] hierarchy added in JUNOS Release 9.3.
Description	Configure a logical demultiplexing (demux) source address for a subscriber in a dynamic profile.
Options	<p><i>source-address</i>—Either the specific source address you want to assign to the subscriber interface or the source address variable (\$junos-subscriber-ip-address). The source address for the interface is dynamically supplied by DHCP when the subscriber accesses the router.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 314 ■ For information about static IP demux interfaces, see the <i>JUNOS Network Interfaces Configuration Guide</i>

family

Syntax family *family* {
 address *address*;
 filter {
 input *filter-name*;
 output *filter-name*;
 }
 unnumbered-address *interface-name* {
 preferred-source-address *address*;
 }
 }

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces *interface-name* unit *logical-unit-number*]

Release Information Statement introduced before JUNOS Release 7.4.
 The [edit dynamic-profiles interfaces *interface-name* unit *logical-unit-number*] hierarchy added in JUNOS Release 9.2.

Description Configure protocol family information for the logical interface.

Options *family*—Protocol family:

- inet—Internet Protocol version 4 suite

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

- Related Topics**
- For general information about configuring static interfaces, see the *JUNOS Network Interfaces Configuration Guide*.
 - “Configuring the Protocol Family,” in *JUNOS Network Interfaces Configuration Guide*.

family

Syntax

```
family family {
    address address;
    demux-source {
        source-address;
    }
    filter {
        input filter-name;
        output filter-name;
    }
    mac-validate (loose | strict):
    unnumbered-address interface-name {
        preferred-source-address address;
    }
}
```

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces demux0 unit *logical-unit-number*]

Release Information Statement introduced before JUNOS Release 7.4.
The [edit dynamic-profiles interfaces demux0 unit *logical-unit-number*] hierarchy added in JUNOS Release 9.3.

Description Configure protocol family information for the logical interface.

Options *family*—Protocol family:

- *inet*—Internet Protocol version 4 suite

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

- Related Topics**
- Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 314
 - For information about static IP demux interfaces, see the *JUNOS Network Interfaces Configuration Guide*

filter

Syntax	<pre> filter { input { filter-name; precedence precedence; } output { filter-name; precedence precedence; } } </pre>
Hierarchy Level	<p>[edit dynamic-profiles family <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>family <i>family</i>],</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family <i>family</i>],</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>family <i>family</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>]</p>
Release Information	<p>Statement introduced before JUNOS Release 7.4.</p> <p>The [edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>] hierarchy added in JUNOS Release 9.2.</p>
Description	Apply a filter to an interface. When you configure filters, you can configure the family inet only.
Options	<p>input <i>filter-name</i>—Name of one filter to evaluate when packets are received on the interface.</p> <p>output <i>filter-name</i>—Name of one filter to evaluate when packets are transmitted on the interface.</p> <p>The remaining statement is explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ For general information about configuring firewall filters, see the <i>JUNOS Policy Framework Configuration Guide</i> ■ Dynamic Firewall Filters Overview on page 363 ■ Guidelines for Creating and Applying Filters for Subscriber Interfaces on page 365 ■ Basic Filter Syntax on page 365

interfaces

Syntax

```

interfaces {
  interface-name {
    unit logical-unit-number {
      family family {
        address address;
        filter {
          input filter-name;
          output filter-name;
        }
        unnumbered-address interface-name {
          preferred-source-address address;
        }
      }
      vlan-id;
    }
    vlan-tagging;
  }
}

```

Hierarchy Level [edit dynamic-profiles *profile-name*]

Release Information Statement introduced before JUNOS Release 7.4.
The [edit dynamic-profiles *profile-name*] hierarchy added in JUNOS Release 9.2.

Description Define interfaces for dynamic profiles.

Options *interface-name*—The interface variable (\$junos-interface-ifd-name). The interface variable is dynamically replaced with the interface the DHCP client accesses when connecting to the router.



NOTE: Though we do not recommend it, you can also enter the specific name of the interface you want to assign to the dynamic profile.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics

- Relationship Between Subscribers and Interfaces in an Access Network on page 5
- Subscriber Interface Overview on page 305
- Configuring Static Subscriber Interfaces in Dynamic Profiles on page 311
- For general information about configuring static interfaces, see the *JUNOS Network Interface Configuration Guide*

interfaces

```
Syntax interfaces {
    demux0 {
        unit logical-unit-number {
            demux-options {
                underlying-interface interface-name
            }
            family family {
                address address;
                demux-source {
                    source-prefix;
                }
                filter {
                    input filter-name;
                    output filter-name;
                }
                mac-validate (loose | strict):
                unnumbered-address interface-name {
                    preferred-source-address address;
                }
            }
        }
    }
}
```

Hierarchy Level [edit dynamic-profiles *profile-name*]

Release Information Statement introduced before JUNOS Release 7.4.
The [edit dynamic-profiles *profile-name*] hierarchy added in JUNOS Release 9.2.

Description Define interfaces for dynamic profiles.

Options *interface-name*—The interface variable (\$junos-interface-ifd-name). The interface variable is dynamically replaced with the interface the DHCP client accesses when connecting to the router.



NOTE: Though we do not recommend it, you can also enter the specific name of the interface you want to assign to the dynamic profile.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

- Related Topics**
- Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 314
 - For information about static IP demux interfaces, see the *JUNOS Network Interfaces Configuration Guide*

mac-validate

Syntax	mac-validate (loose strict);
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> demux0 unit <i>logical-unit-number</i> family <i>family</i>]
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Enable IP and MAC address validation for dynamic IP demux interfaces in a dynamic profile. Supported on MX-series routers only.
Options	<p>loose—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the IP source address matches one of the trusted tuples, but the MAC address does not match the MAC address of the tuple. Continues to forward incoming packets when the source address of the incoming packet does not match any of the trusted IP addresses.</p> <p>strict—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the MAC address does not match the tuple's MAC source address, or when IP source address of the incoming packet does not match any of the trusted IP addresses.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring MAC Address Validation for Subscriber Interfaces on page 315

precedence

Syntax	<code>precedence precedence;</code>
Hierarchy Level	[edit dynamic-profiles family <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> inet filter], [edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family <i>family</i> inet filter],
Release Information	Statement introduced in JUNOS Release 9.3.
Description	Apply a precedence to a dynamic filter.
Options	<i>precedence</i> —Precedence value for the filter. The lower the precedence value, the higher the precedence. Default: 0 Range: 0 through 250
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ For general information about configuring firewall filters, see the <i>JUNOS Policy Framework Configuration Guide</i> ■ Dynamic Firewall Filters Overview on page 363 ■ Guidelines for Creating and Applying Filters for Subscriber Interfaces on page 365 ■ Basic Filter Syntax on page 365

preferred-source-address

Syntax	<code>preferred-source-address address;</code>
Hierarchy Level	<p>[edit dynamic-profiles interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet unnumbered-address <i>interface-name</i>],</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family <i>family</i>],</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet unnumbered-address <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet unnumbered-address <i>interface-name</i>]</p>
Release Information	<p>Statement introduced in JUNOS Release 9.0.</p> <p>The [edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet unnumbered-address <i>interface-name</i>] hierarchy added in JUNOS Release 9.2.</p>
Description	<p>For unnumbered Ethernet interfaces configured with a loopback interface as the donor interface, specify one of the loopback interface's secondary addresses as the preferred source address for the unnumbered Ethernet interface. Configuring the preferred source address enables you to use an IP address other than the primary IP address on some of the unnumbered Ethernet interfaces in your network.</p> <p>Currently, configuration of a preferred source address for unnumbered Ethernet interfaces is supported only for the IPv4 address family.</p>
Options	<i>address</i> —Secondary IP address of the donor loopback interface.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ “Configuring a Preferred Source Address for Unnumbered Ethernet Interfaces,” in <i>JUNOS Network Interfaces Configuration Guide</i>. ■ <code>address</code> ■ <i>JUNOS System Basics Configuration Guide</i>

underlying-interface

Syntax	<code>underlying-interface <i>underlying-interface-name</i>;</code>
Hierarchy Level	<code>[edit dynamic-profiles <i>profile-name</i> interfaces demux0 <i>interface-name</i> unit unit <i>logical-unit-number</i> demux-options]</code>
Release Information	Statement introduced before JUNOS Release 7.4. The <code>[edit dynamic-profiles <i>profile-name</i> interfaces demux0]</code> hierarchy added in JUNOS Release 9.3. Support for aggregated Ethernet added in JUNOS Release 9.4.
Description	Configure the underlying interface on which the demultiplexing (demux) interface is running.
Options	<i>underlying-interface-name</i> —Either the specific name of the interface on which the DHCP discover packet arrives or the interface variable (<code>\$junos-underlying-interface</code>). The variable is used to specify the underlying interface when a new demux interface is dynamically created. The variable is dynamically replaced with the underlying interface that DHCP supplies when the subscriber logs in.



NOTE: Logical demux interfaces are currently supported only on Gigabit Ethernet, Fast Ethernet, 10-Gigabit Ethernet, or aggregated Ethernet interfaces.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 314 ■ For information about static underlying interfaces, see the <i>JUNOS Network Interfaces Configuration Guide</i>

unit

Syntax unit *logical-unit-number* {
 family *family* {
 address *address*;
 filter {
 input *filter-name*;
 output *filter-name*;
 }
 unnumbered-address *interface-name* {
 preferred-source-address *address*;
 }
 }
 vlan-id;
 }

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces *interface-name*]

Release Information Statement introduced before JUNOS 7.4.
 The [edit dynamic-profiles *profile-name* interfaces *interface-name*] hierarchy added in JUNOS Release 9.2.

Description Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

Options *logical-unit-number*—Either the specific unit number of the interface you want to assign to the dynamic profile or the static unit number variable (\$junos-underlying-interface-unit). The static unit number variable is dynamically replaced with the client unit number when the client session begins. The client unit number is specified by the DHCP client when it accesses the subscriber network.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

unit

Syntax

```
unit logical-unit-number {
    demux-options {
        underlying-interface interface-name
    }
    family family {
        address address;
        demux-source {
            source-address;
        }
        filter {
            input filter-name;
            output filter-name;
        }
        mac-validate (loose | strict):
        unnumbered-address interface-name {
            preferred-source-address address;
        }
    }
}
```

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces demux0]

Release Information Statement introduced before JUNOS 7.4.
The [edit dynamic-profiles *profile-name* interfaces demux0] hierarchy added in JUNOS Release 9.3.

Description Configure a dynamic logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

Options *logical-unit-number*—Either the specific unit number of the interface or the unit number variable (\$junos-interface-unit). The variable is used to specify the unit of the interface when a new demux interface is dynamically created. The static unit number variable is dynamically replaced with the unit number that DHCP supplies when the subscriber logs in.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Topics

- Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 314
- For information about static IP demux interfaces, see the *JUNOS Network Interfaces Configuration Guide*

unnumbered-address

Syntax	<code>unnumbered-address interface-name <preferred-source-address address>;</code>
Hierarchy Level	<p>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>],</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family <i>family</i>],</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet]</p>
Release Information	<p>Statement introduced in JUNOS Release 8.2.</p> <p><code>preferred-source-address</code> option introduced in JUNOS Release 9.0.</p> <p>The [edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>] hierarchy added in JUNOS Release 9.2.</p>
Description	For Ethernet interfaces, enable the local address to be derived from the specified interface. Configuring an unnumbered Ethernet interface enables IP processing on the interface without assigning an explicit IP address to the interface.
Options	<p><i>interface-name</i>—Name of the interface from which the local address is derived. The specified interface must have a logical unit number and a configured IP address, and must not be an unnumbered interface.</p> <p>The <code>preferred-source-address</code> statement is explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ “Configuring an Unnumbered Interface,” in <i>JUNOS Network Interfaces Configuration Guide</i>. ■ <code>address</code> ■ <i>JUNOS System Basics Configuration Guide</i>

vlan-id

Syntax	<code>vlan-id <i>number</i>;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced before JUNOS Release 7.4. The [edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>] hierarchy added in JUNOS Release 9.2.
Description	For Fast Ethernet, Gigabit Ethernet, and Aggregated Ethernet interfaces only, bind a 802.1Q VLAN tag ID to a logical interface.
Options	<i>number</i> —A valid VLAN identifier. Range: For aggregated Ethernet, 4-port, 8-port, and 12-port Fast Ethernet PICs, and for management and internal Ethernet interfaces, 1 through 1023. For 48-port Fast Ethernet and Gigabit Ethernet PICs, 1 through 4094. VLAN ID 0 is reserved for tagging the priority of frames.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

vlan-tagging

Syntax	vlan-tagging;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i>], [edit interfaces <i>interface-name</i>]
Release Information	Statement introduced before JUNOS Release 7.4. The [edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i>] hierarchy added in JUNOS Release 9.2.
Description	For Fast Ethernet and Gigabit Ethernet interfaces and aggregated Ethernet interfaces configured for VPLS, enable the reception and transmission of 802.1Q VLAN-tagged frames on the interface.



NOTE: For Ethernet, Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet, 10-Gigabit Ethernet, and aggregated Ethernet interfaces supporting VPLS, the JUNOS software supports a subset of the IEEE 802.1Q standard for channelizing an Ethernet interface into multiple logical interfaces, allowing many hosts to be connected to the same Gigabit Ethernet switch, but preventing them from being in the same routing or bridging domain.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
---------------------------------	---

Part 6

Dynamic Firewall Services for Subscriber Access

- Dynamic Firewall Services Overview on page 363
- Configuring Filters for Dynamic Profiles on page 367
- Firewall Filter Examples on page 371

Chapter 24

Dynamic Firewall Services Overview

- Dynamic Firewall Filters Overview on page 363
- Guidelines for Creating and Applying Filters for Subscriber Interfaces on page 365
- Basic Filter Syntax on page 365

Dynamic Firewall Filters Overview

Firewall filters provide rules that define whether to permit or deny packets that are transiting an interface on a router. You configure firewall filters to determine whether to permit or deny traffic before it enters or exits an interface to which the firewall filter is applied. An *input* (or *ingress*) firewall filter is one that is applied to packets that are entering a network. An *output* (or *egress*) firewall filter is one that is applied to packets that are exiting a network. You can configure firewall filters to subject packets to filtering or class-of-service (CoS) marking (grouping similar types of traffic together and treating each type of traffic as a class with its own level of service priority).

What makes firewall filters “dynamic” is the ability of the router to apply them to interfaces dynamically. This dynamic application is performed by associating input or output dynamic filters to a dynamic profile. When triggered, a dynamic profile can apply a named filter or a filter specified in RADIUS to an interface.

This overview covers:

- Firewall Filter Types on page 363
- Firewall Filter Components on page 364
- Firewall Filter Processing on page 364

Firewall Filter Types

The following firewall filter types are supported:

- Port (Layer 2) firewall filter—Port firewall filters apply to Layer 2 switch ports. You can apply port firewall filters only in the ingress direction on a physical port.
- VLAN firewall filter—VLAN firewall filters provide access control for packets that enter a VLAN, are bridged within a VLAN, and leave a VLAN. You can apply VLAN firewall filters in both ingress and egress directions on a VLAN. VLAN firewall filters are applied to all packets that are forwarded to or forwarded from the VLAN.

- Router (Layer 3) firewall filter—You can apply a router firewall filter in both ingress and egress directions on Layer 3 (routed) interfaces.



NOTE: Firewall filters are not supported on aggregated Ethernet interfaces.

To apply a firewall filter, you must:

1. Configure the firewall filter.
2. Apply the firewall filter.

Firewall Filter Components

When creating a firewall filter, you first define the family address type (**inet**) and then you define one or more terms that specify the filtering criteria and the action to take if a match occurs.

Each term consists of the following components:

- Match conditions—Specifies values or fields that the packet must contain. You can define various match conditions, including the IP source address field, IP destination address field, Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source port field, IP protocol field, Internet Control Message Protocol (ICMP) packet type, TCP flags, and interfaces.
- Actions—Specifies what to do if a match condition occurs. Possible actions are to accept or discard a packet. In addition, packets can be counted to collect statistical information. If no action is specified for a term, the default action is to accept the packet.

Firewall Filter Processing

The order of the terms within a firewall filter is important. Packets are tested against each term in the order in which the terms are listed in the firewall filter configuration. When a firewall filter contains multiple terms, the router takes a top-down approach and compares a packet against the first term in the firewall filter. If the packet matches the first term, the router executes the action defined by that term to either permit or deny the packet, and no other terms are evaluated. If the router does not find a match between the packet and first term, it then compares the packet to the next term in the firewall filter by using the same match process. If no match occurs between the packet and the second term, the router continues to compare the packet to each successive term defined in the firewall filter until a match is found. If a packet does not match any terms in a firewall filter, the default action is to discard the packet.

In addition to the top-down term processing within filters, you can specify a precedence (from 0 through 255) for input and output filters within a dynamic profile to force filter processing in a particular order. Setting a lower precedence value for a filter gives it a higher precedence within the dynamic profile. In other words, filters with lower precedence values are applied to interfaces before filters with higher precedence values. A precedence of zero (the default) gives the filter the highest

precedence. If no precedence is specified, the filter receives a precedence of zero (highest precedence). Filters with matching precedence (zero or otherwise) are applied in random order.

- Related Topics**
- Guidelines for Creating and Applying Filters for Subscriber Interfaces on page 365
 - Dynamically Attaching Statically Created Filters on page 367
 - Dynamically Attaching Filters Using RADIUS Variables on page 368

Guidelines for Creating and Applying Filters for Subscriber Interfaces

This release does not support the dynamic configuration of firewall filters. However, you can create static firewall filters for interfaces as you do normally and dynamically apply those filters to statically created interfaces using dynamic profiles. You can also use dynamic profiles to attach input and output filters through RADIUS.

When creating and applying filters, keep the following in mind:

- This release supports dynamic application of only input and output filters.
- The filters must be interface-specific.
- This release supports only **family inet** filters.
- You can attach only input and output filters to an interface.
- You can chain up to five input filters and four output filters together.
- If you do not configure and apply a filter, the interface uses the default group filter configuration.
- You cannot modify a firewall filter while subscribers on the same logical interface are bound.

- Related Topics**
- Dynamic Firewall Filters Overview on page 363
 - Dynamically Attaching Statically Created Filters on page 367
 - Dynamically Attaching Filters Using RADIUS Variables on page 368
 - For information about JUNOS default groups, see the *JUNOS CLI User Guide*

Basic Filter Syntax

This section provides the basic filter CLI statement syntax. The first part of this syntax provides the CLI statements to associate an input and output filter to a dynamic profile. The second part of this syntax represents the configured input and output filters associated to the dynamic profile. When a DHCP event occurs, the dynamic profile applies the specified filters to the DHCP client interface on the router.

```
[edit]
dynamic-profiles {
  profile-name {
    interfaces {
      $junos-interface-ifd-name {
        unit $junos-underlying-interface-unit {
```



```

        family inet {
            filter {
                input {
                    filter-name;
                    precedence precedence;
                }
                output filter-name;
                filter-name;
                precedence precedence;
            }
        }
    }
}
[edit]
firewall {
    family inet {
        filter filter-name {
            [desired filter configuration]
        }
        filter filter-name {
            [desired filter configuration]
        }
    }
}

```

- Related Topics**
- Dynamically Attaching Statically Created Filters on page 367
 - Dynamic Firewall Filters Overview on page 363

Chapter 25

Configuring Filters for Dynamic Profiles

- Dynamically Attaching Statically Created Filters on page 367
- Dynamically Attaching Filters Using RADIUS Variables on page 368
- Defining Dynamic Filter Processing Order on page 369

Dynamically Attaching Statically Created Filters

Before you can attach a statically created filter using a dynamic profile.

1. Create the filters you want to attach.

See the *JUNOS Policy Framework Configuration Guide* for detailed information about firewall filters and how to create them.

2. Create a basic dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 283.

To dynamically attach statically created input and output filters:

1. Specify the input filter in the dynamic profile.

```
[edit dynamic-profiles access-profile interfaces ge-1/1/1 unit 1 family inet]  
user@host# set filter input static-input-filter
```

2. Specify the output filter in the dynamic profile.



NOTE: The following example specifies an optional precedence value for the output filter.

```
[edit dynamic-profiles access-profile interfaces ge-1/1/1 unit 1 family inet]  
user@host# set filter output static-output-filter precedence 50
```

- Related Topics**
- Guidelines for Creating and Applying Filters for Subscriber Interfaces on page 365
 - Dynamically Attaching Filters Using RADIUS Variables on page 368
 - For information about JUNOS default groups, see the *JUNOS CLI User Guide*
 - For information about firewall filters, see the *JUNOS Policy Framework Configuration Guide*

Dynamically Attaching Filters Using RADIUS Variables

You can attach filters to static interfaces by using dynamic profiles. By specifying a variable for the input and output filters, the dynamic profile uses RADIUS VSA attributes for ingress and egress policy.

RADIUS VSA	Attribute Name	Variable
26-10	ingress-policy-name	\$junos-input-policy
26-11	egress-policy-name	\$junos-output-policy

Before you can attach a filter using RADIUS.

1. Create a basic dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 283.

2. Ensure that RADIUS ingress and egress policies are configured appropriately.

See “Configuring RADIUS Server Parameters for Subscriber Access” on page 21

To dynamically attach input and output filters using RADIUS:

1. Specify the input filter variable in the dynamic profile.

```
[edit dynamic-profiles access-profile interfaces ge-1/1/1 unit 1 family inet]
user@host# set filter input $junos-input-filter
```

2. Specify the output filter variable in the dynamic profile.

```
[edit dynamic-profiles access-profile interfaces ge-1/1/1 unit 1 family inet]
user@host# set filter output $junos-output-filter
```

- Related Topics**
- Guidelines for Creating and Applying Filters for Subscriber Interfaces on page 365
 - Dynamically Attaching Statically Created Filters on page 367
 - For more information about JUNOS default groups, see the *JUNOS CLI User Guide*
 - For more information about firewall filters, see the *Policy Framework Configuration Guide*

Defining Dynamic Filter Processing Order

You can force filter processing to occur in a particular order by using the **precedence** statement. You specify a precedence for input and output filters within a dynamic profile at the [edit dynamic-profiles family *profile-name* interfaces *interface-name* unit *logical-unit-number* family *family*] and [edit dynamic-profiles *profile-name* interfaces demux0 unit *logical-unit-number* family *family*] hierarchy level.

The precedence range is from 0 to 250. Setting a lower precedence value for a filter gives it a higher precedence within the dynamic profile. A precedence of zero (the default) gives the filter the highest precedence. If no precedence is specified, the filter receives a precedence of zero (highest precedence). Filters with matching precedence (zero or otherwise) are applied in random order.

Before you define a precedence for a filter in a dynamic profile.

1. Create the filters you want to attach to the dynamic profile.

See the *JUNOS Policy Framework Configuration Guide* for detailed information about firewall filters and how to create them.

2. Create a basic dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 283.

3. Attach the filters to the dynamic profile.

See “Dynamically Attaching Statically Created Filters” on page 367 or “Dynamically Attaching Filters Using RADIUS Variables” on page 368.

To define a precedence for an input and output filter:

1. Specify the input filter precedence in the dynamic profile.

```
[edit dynamic-profiles access-profile interfaces ge-1/1/1 unit 1 family inet filter]
user@host# set filter input precedence 50
```

2. Specify the output filter precedence in the dynamic profile.

```
[edit dynamic-profiles access-profile interfaces ge-1/1/1 unit 1 family inet filter]
user@host# set filter output precedence 5
```

- Related Topics**
- Guidelines for Creating and Applying Filters for Subscriber Interfaces on page 365
 - For information about firewall filters, see the *JUNOS Policy Framework Configuration Guide*

Chapter 26

Firewall Filter Examples

- Static Filter Examples on page 371

Static Filter Examples

This topic provides some static filter configuration examples.

```
firewall {
  policer p1 {
    if-exceeding {
      bandwidth-limit 5m;
      burst-size-limit 10m;
    }
    then discard;
  }
  family inet {
    filter dfwd {
      interface-specific;
      term 1 {
        from {
          source-address {
            192.1.1.0/24;
          }
        }
        then {
          count c1;
          next term;
        }
      }
      term 2 {
        from {
          source-address {
            192.2.1.0/24;
          }
        }
        then count c2;
      }
      term 3 {
        then accept;
      }
    }
    filter dfwd1 {
      interface-specific;
```



```

    term 1 {
        from {
            address {
                192.1.1.0/24;
            }
        }
        then {
            discard;
        }
    }
}
filter tos {
    interface-specific;
    term 1 {
        from {
            precedence priority;
        }
        then forwarding-class assured-forwarding;
    }
    term 2 {
        then {
            log;
            accept;
        }
    }
}
filter dfwd2 {
    interface-specific;
    term 1 {
        from {
            forwarding-class best-effort;
        }
        then {
            sample;
            forwarding-class expedited-forwarding;
        }
    }
    term 2 {
        then accept;
    }
}
filter nodhcp {
    term dhcpdiscover {
        from {
            protocol udp;
            source-port 68;
            destination-port 67;
        }
        then {
            discard;
        }
    }
    term others {
        then accept;
    }
}
}

```



```

filter p1 {
  interface-specific;
  term 1 {
    from {
      precedence priority;
    }
    then {
      policer p1;
      log;
    }
  }
  term 2 {
    then accept;
  }
}
filter dscp {
  interface-specific;
  term 1 {
    from {
      dscp af11;
    }
    then log;
  }
  term 2 {
    then accept;
  }
}
filter tcm {
  interface-specific;
  term 1 {
    from {
      dscp af11;
    }
    then policer p1;
  }
  term 2 {
    then accept;
  }
}
}
traceoptions {
  flag dynamic;
}
}

```

Related Topics ■ Dynamically Attaching Statically Created Filters on page 367

Part 7

Class of Service for Subscriber Access

- Class of Service for Subscriber Access Overview on page 377
- Configuring Class of Service for Subscriber Access on page 389
- Class of Service for Subscriber Access Examples on page 403
- Class of Service Shaping-Rate Adjustments Overview on page 413
- Configuring Class of Service Shaping-Rate Adjustments on page 417
- Class of Service Shaping-Rate Adjustments Examples on page 425
- Summary of Class of Service for Subscriber Access Statements on page 429

Chapter 27

Class of Service for Subscriber Access Overview

- CoS for Subscriber Access Overview on page 377
- CoS and Static IP Demux Interface Set Overview on page 378
- Subscriber Interfaces that Provide Initial CoS Parameters Dynamically Obtained from RADIUS Overview on page 378
- Changing CoS Services Overview on page 385
- Guidelines for Configuring CoS for Subscriber Access on page 388

CoS for Subscriber Access Overview

This topic describes class-of-service (CoS) functionality for dynamic subscriber access.

JUNOS CoS enables you to divide traffic into classes and offer various levels of throughput and packet loss when congestion occurs. This allows packet loss to happen according to rules that you configure. The JUNOS CoS features provide a set of mechanisms that you can use to provide differentiated services when best-effort traffic delivery is insufficient.

In a subscriber access environment, service providers want to provide video, voice, and data services over the same network for subscribers. You can configure the router to provide hierarchical scheduling for subscribers by dynamically adding or deleting queues when subscribers require services.

In this network, subscribers are mapped to IP demux interfaces or VLANs. Depending on your deployment, you configure CoS parameters in the static `[edit class-of-service]` hierarchy and in the `[edit dynamic profiles class-of-service]` hierarchy.

Hardware Requirements for CoS for Dynamic Subscriber Access

To configure CoS for dynamic subscriber access, you must have a Enhanced Queuing Distributed Port Controllers (EQ DPC) on the MX-series router.

- Related Topics** ■ [Configuring Static Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 389](#)

CoS and Static IP Demux Interface Set Overview

This topic describes the scenario for configuring hierarchical scheduling on a set of statically created IP demux interfaces.

An interface set enables you to group IP demux interfaces into logical groups, and shape that group by binding a traffic control-profile to the interface set. You can also configure the remaining traffic on interface set to shape IP demux interfaces without traffic-control profiles to an aggregate rate.

Table 27 on page 378 shows the scheduler mapping for interface sets of IP demux interfaces.

Table 27: Scheduler Mapping for Interface Sets

Level	Type	Mapping
L4	Queues	Demux interface
L3	Scheduler	Demux interface
L2	Scheduler	Interface set of IP demux interfaces
L1	Scheduler	Underlying demux interface

- Related Topics** ■ [Configuring CoS on a Set of Static IP Demux Interfaces on page 400](#)

Subscriber Interfaces that Provide Initial CoS Parameters Dynamically Obtained from RADIUS Overview

You can configure interface-specific CoS parameters that the router obtains when subscribers log in at appropriately configured static or dynamic subscriber interfaces. This feature is supported only for interfaces on Enhanced Queuing Dense Port Concentrators (EQ DPCs) in MX-series routers.

To configure a client dynamic profile to providing initial CoS Services, make sure you understand the following concepts:

- [Dynamic Configuration of Initial CoS in Client Profiles on page 379](#)
- [Internal Variables for Dynamic Configuration of Initial Traffic Shaping on page 379](#)
- [Internal Variables for Dynamic Configuration of Initial Scheduling and Queuing on page 381](#)

Dynamic Configuration of Initial CoS in Client Profiles

When a router interface receives a join message from a DHCP client, the JUNOS software applies the values configured in the client dynamic profile associated with that router interface. You can associate a dynamic profile with a subscriber interface on the router by including statements at the `[edit dynamic-profiles profile-name class-of-service interfaces]` hierarchy level. A dynamic profile that is activated through its association with a subscriber interface is known as a *client profile*.

This release supports a set of internal variables for obtaining a scheduler-map name and traffic-shaping parameters from the RADIUS authentication server, and another set of internal variables for obtaining a scheduler name and scheduler parameters from the RADIUS authentication server. When a client authenticates over a router interface associated with the client dynamic profile, the router replaces the internal variables with interface-specific values obtained from the RADIUS server.



NOTE: For this release of the JUNOS software, configure dynamic configuration of initial CoS features in a *client* dynamic profile by referencing *JUNOS internal variables*; do not define and reference *user-defined variables* in a client dynamic profile.

Internal Variables for Dynamic Configuration of Initial Traffic Shaping

To provide a scheduler map name and traffic shaping parameters obtained from the RADIUS authentication server when a subscriber authenticates, you can reference the following JUNOS internal variables for CoS at the `[edit dynamic-profiles profile-name class-of-service traffic-control-profiles profile-name]` hierarchy level for the *client* dynamic profile associated with the subscriber interface:

- `$junos-cos-scheduler-map` — Reference from the `scheduler-map` statement.
- `$junos-cos-shaping-rate` — Reference from the `shaping-rate` statement.
- `$junos-cos-guaranteed-rate` — Reference from the `guaranteed-rate` statement.
- `$junos-cos-delay-buffer-rate` — Reference from the `delay-buffer-rate` statement.

Table 28 on page 380 provides detailed descriptions of the JUNOS internal variables for CoS that you can reference in a client dynamic profile to dynamically configure an initial traffic-control profile when a subscriber logs in.

Table 28: JUNOS Internal Variables for Dynamic Configuration of Initial Traffic Shaping

Internal Variable Name and Description	Static and Dynamic Statement Syntax Options
<p>\$junos-cos-scheduler-map</p> <p>Scheduler-map name configured in a traffic-control profile in a client dynamic profile. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the client dynamic profile is attached.</p> <p>You reference this variable from the scheduler-map statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>] hierarchy level.</p> <p>NOTE: The scheduler map referenced by the scheduler-map statement can be defined dynamically (at the [edit dynamic-profiles <i>profile-name</i> class-of-service scheduler-maps] hierarchy level) or statically (at the [edit class-of-service scheduler-maps] hierarchy level).</p>	<ul style="list-style-type: none"> ■ scheduler-map <i>scheduler-name</i>; ■ scheduler-map \$junos-cos-scheduler-map;
<p>\$junos-cos-shaping-rate</p> <p>Shaping rate configured in a traffic-control profile in a client dynamic profile. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the client dynamic profile is attached.</p> <p>You reference this variable from the shaping-rate statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>] hierarchy level.</p>	<ul style="list-style-type: none"> ■ shaping-rate <i>shaping-rate</i>; ■ shaping-rate \$junos-cos-shaping-rate;
<p>\$junos-cos-guaranteed-rate</p> <p>Guaranteed rate configured in a traffic-control profile in a client dynamic profile. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the client dynamic profile is attached.</p> <p>You reference this variable from the guaranteed-rate statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>] hierarchy level.</p>	<ul style="list-style-type: none"> ■ guaranteed-rate <i>guaranteed-rate</i>; ■ guaranteed-rate \$junos-cos-guaranteed-rate;
<p>\$junos-cos-delay-buffer-rate</p> <p>Delay-buffer rate configured in a traffic-control profile in a client dynamic profile. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the client dynamic profile is attached.</p> <p>You reference this variable in the delay-buffer-rate statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>] hierarchy level.</p>	<ul style="list-style-type: none"> ■ delay-buffer-rate <i>delay-buffer-rate</i>; ■ delay-buffer-rate \$junos-cos-guaranteed-rate;

Internal Variables for Dynamic Configuration of Initial Scheduling and Queuing

To provide a scheduler name and parameters obtained from a RADIUS authentication server when a subscriber logs in, you can reference the following JUNOS internal variables for CoS in the [edit dynamic-profiles *profile-name* class-of-service schedulers] configuration for the *client* dynamic profile associated with the subscriber interface:

- \$junos-cos-scheduler — Reference from the scheduler statement.
- \$junos-cos-scheduler-tx — Reference from the transmit-rate statement.
- \$junos-cos-scheduler-bs — Reference from the buffer-size statement.
- \$junos-cos-scheduler-pri — Reference from the priority statement.
- \$junos-cos-scheduler-dropfile-low — Reference from the drop-profile-map loss-priority low protocol any statement.
- \$junos-cos-scheduler-dropfile-medium-low — Reference from the drop-profile-map loss-priority medium-low protocol any statement.
- \$junos-cos-scheduler-dropfile-medium-high — Reference from the drop-profile-map loss-priority medium-high protocol any statement.
- \$junos-cos-scheduler-dropfile-high — Reference from the drop-profile-map loss-priority high protocol any statement.
- \$junos-cos-scheduler-dropfile-any — Reference from the drop-profile-map loss-priority any protocol any statement.

Table 29 on page 381 provides detailed descriptions of the JUNOS internal variables for CoS that you can reference in a client dynamic profile to dynamically configure an initial scheduler when a subscriber logs in .

Table 29: JUNOS Internal Variables for Dynamic Configuration of Initial Scheduling and Queuing

Internal Variable Name and Description	Static and Dynamic Statement Syntax Options
<div>\$junos-cos-scheduler</div> <div>Name of a scheduler configured in a client dynamic profile. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the client dynamic profile is attached.</div> <div>You reference this variable from the scheduler statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service schedulers] hierarchy level.</div>	<div>■ schedulers <i>scheduler-name</i>;</div> <div>■ schedulers \$junos-cos-scheduler;</div>

Table 29: JUNOS Internal Variables for Dynamic Configuration of Initial Scheduling and Queuing (*continued*)

Internal Variable Name and Description	Static and Dynamic Statement Syntax Options
<p>\$junos-cos-scheduler-tx</p> <p>Transmit rate specified for a scheduler configured in a client dynamic profile. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the client dynamic profile is attached.</p> <p>You reference this variable from the <code>transmit-rate</code> statement at the <code>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>]</code> hierarchy level.</p>	<ul style="list-style-type: none"> ■ <code>transmit-rate <i>transmit-rate</i>;</code> ■ <code>transmit-rate \$junos-cos-scheduler-tx;</code>
<p>\$junos-cos-scheduler-bs</p> <p>Buffer size as a percentage of total buffer, specified for a scheduler configured in a client dynamic profile. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the client dynamic profile is attached.</p> <p>You reference this variable from the <code>buffer-size</code> statement with the <code>percent</code> option at the <code>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>]</code> hierarchy level.</p>	<ul style="list-style-type: none"> ■ <code>buffer-size percent <i>percentage</i>;</code> ■ <code>buffer-size percent \$junos-cos-scheduler-bs;</code>
<p>\$junos-cos-scheduler-pri</p> <p>Packet-scheduling priority value specified for a scheduler configured in a client dynamic profile. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the client dynamic profile is attached.</p> <p>You reference this variable from the <code>priority</code> statement at the <code>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>]</code> hierarchy level.</p>	<ul style="list-style-type: none"> ■ <code>priority (low medium-low medium-high high strict-high);</code> ■ <code>priority \$junos-cos-scheduler-pri;</code>

Table 29: JUNOS Internal Variables for Dynamic Configuration of Initial Scheduling and Queuing (*continued*)

Internal Variable Name and Description	Static and Dynamic Statement Syntax Options
<p><code>\$junos-cos-scheduler-dropfile-low</code></p> <p>Name of the drop profile for RED for loss-priority level low specified for a scheduler configured in a client dynamic profile. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the client dynamic profile is attached.</p> <p>You reference this variable from the <code>drop-profile</code> statement at the <code>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i> drop-profile-map loss-priority low protocol any]</code> hierarchy level.</p> <p>NOTE: The drop profile must be configured statically (at the <code>[edit class-of-service schedulers <i>scheduler-name</i> drop-profiles]</code> hierarchy level) for loss-priority low.</p>	<ul style="list-style-type: none"> ■ <code>drop-profile low</code> ■ <code>drop-profile</code> <code>\$junos-cos-scheduler-dropfile-low;</code>
<p><code>\$junos-cos-scheduler-dropfile-medium-low</code></p> <p>Name of the drop profile for RED for loss-priority level medium-low specified for a scheduler configured in a client dynamic profile. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the client dynamic profile is attached.</p> <p>You reference this variable from the <code>drop-profile</code> statement at the <code>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i> drop-profile-map loss-priority medium-low protocol any]</code> hierarchy level.</p> <p>NOTE: The drop profile must be configured statically (at the <code>[edit class-of-service schedulers <i>scheduler-name</i> drop-profiles]</code> hierarchy level).</p>	<ul style="list-style-type: none"> ■ <code>drop-profile <i>profile-name</i>;</code> ■ <code>drop-profile</code> <code>\$junos-cos-scheduler-dropfile-medium-low;</code>

Table 29: JUNOS Internal Variables for Dynamic Configuration of Initial Scheduling and Queuing (*continued*)

Internal Variable Name and Description	Static and Dynamic Statement Syntax Options
<p><code>\$junos-cos-scheduler-dropfile-medium-high</code></p> <p>Name of the drop profile for RED for loss-priority level <code>medium-high</code> specified for a scheduler configured in a client dynamic profile. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the client dynamic profile is attached.</p> <p>You reference this variable from the <code>drop-profile</code> statement at the <code>[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name drop-profile-map loss-priority medium-high protocol any]</code> hierarchy level.</p> <p>NOTE: The drop profile must be configured statically (at the <code>[edit class-of-service schedulers scheduler-name drop-profiles]</code> hierarchy level).</p>	<ul style="list-style-type: none"> ■ <code>drop-profile profile-name;</code> ■ <code>drop-profile</code> <code>\$junos-cos-scheduler-dropfile-medium-high;</code>
<p><code>\$junos-cos-scheduler-dropfile-high</code></p> <p>Name of the drop profile for RED for loss-priority level <code>high</code> specified for a scheduler configured in a client dynamic profile. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the client dynamic profile is attached.</p> <p>You reference this variable from the <code>drop-profile</code> statement at the <code>[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name drop-profile-map loss-priority high protocol any]</code> hierarchy level.</p> <p>NOTE: The drop profile must be configured statically (at the <code>[edit class-of-service schedulers scheduler-name drop-profiles]</code> hierarchy level).</p>	<ul style="list-style-type: none"> ■ <code>drop-profile profile-name;</code> ■ <code>drop-profile</code> <code>\$junos-cos-scheduler-dropfile-high;</code>

Table 29: JUNOS Internal Variables for Dynamic Configuration of Initial Scheduling and Queuing *(continued)*

Internal Variable Name and Description	Static and Dynamic Statement Syntax Options
<p><code>\$junos-cos-scheduler-dropfile-any</code></p> <p>Name of the drop profile for RED for loss-priority level any specified for a scheduler configured in a client dynamic profile. The JUNOS software obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the client dynamic profile is attached.</p> <p>You reference this variable from the <code>drop-profile</code> statement at the <code>[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name drop-profile-map loss-priority any protocol any]</code> hierarchy level.</p> <p>NOTE: The drop profile must be configured statically (at the <code>[edit class-of-service schedulers scheduler-name drop-profiles]</code> hierarchy level).</p>	<ul style="list-style-type: none"> ■ <code>drop-profile profile-name;</code> ■ <code>drop-profile \$junos-cos-scheduler-dropfile-any;</code>

- Related Topics**
- Activating Subscribers and Managing Services in an Access Network on page 7
 - Dynamic Profiles Overview on page 275
 - Dynamic Variables Overview on page 276
 - Configuring a Subscriber Interface to Provide Initial CoS Parameters Dynamically Obtained from RADIUS on page 394
 - Example: Configuring a Subscriber Interface to Provide Initial CoS Parameters Dynamically Obtained from RADIUS on page 410

Changing CoS Services Overview

This topic describes how to provide CoS when subscribers dynamically upgrade or downgrade services in an access environment.

You can configure your network with an access profile that provides all subscribers with default CoS parameters when they log in. For example, all subscribers can receive a basic data service. By configuring the access profile with JUNOS internal dynamic variables for RADIUS-provided CoS parameters, you also enable the service to be activated for those subscribers at login.

To enable subscribers to activate a service or upgrade to different services through RADIUS change-of-authorization (CoA) messages after login, configure a service profile that includes user-defined variables.

Types of CoS Variables Used in a Dynamic Service Profile

You can configure variables for the following CoS parameters in a dynamic service profile:

- Shaping rate
- Delay buffer rate
- Guaranteed rate
- Scheduler map

For each CoS parameter, you must associate a RADIUS vendor ID. For each vendor ID, you must assign an attribute number and a tag. The tag is used to differentiate between values for different CoS variables when you specify the same attribute number for those variables. These values are matched with the values supplied by RADIUS during subscriber authentication. All of the values in the dynamic profile must be defined in RADIUS or none of the values are passed.

Optionally, you can configure default values for each parameter. Configuring default values is beneficial if you do not configure RADIUS to enable service changes. During service changes, RADIUS takes precedence over the default value that is configured.

Static and Dynamic CoS Configurations

Depending on how you configure CoS parameters in the access and service profiles, certain CoS parameters are replaced or merged when subscribers change or activate new services.

Static configuration is when you configure the scheduler map and schedulers in the static `[edit class-of-service]` hierarchy and reference the scheduler map in the dynamic profile. Dynamic configuration is when you configure the scheduler map and schedulers within the dynamic profile.

The CoS configuration also depends on whether you have enabled multiple subscribers on the same logical interface using the `aggregate-clients` option in the dynamic profile referenced by DHCP. When you specify the `aggregate-clients` option, the scheduler map names specified in the dynamic profile are appended. If the length of the scheduler map name exceeds 128 characters, subscribers cannot log in.

Scenarios for Static and Dynamic Configuration of CoS Parameters

Table 30 on page 387 lists the scenarios for static and dynamic configuration of CoS parameters in access profiles and service profiles at subscriber login. The table also lists the behavior for each configuration for service activation and service modification using RADIUS CoA messages.

Table 30: CoS Services and Variables

Scenario	Static CoS Configuration	Dynamic CoS Configuration	Dynamic CoS Configuration (Multiple Subscribers Enabled on a Logical Interface)
Subscriber login	<ul style="list-style-type: none"> ■ Configure RADIUS values or default values for all parameters in access profile ■ Configure scheduler map in edit class-of-service hierarchy and reference in access profile 	<ul style="list-style-type: none"> ■ Configure RADIUS values or default values for all parameters in access profile ■ Configure scheduler map and schedulers in access profile 	<ul style="list-style-type: none"> ■ Configure RADIUS values or default values for all parameters in access profile ■ Configure scheduler map and schedulers in access profile
	Static CoS Behavior	Dynamic CoS Behavior	Dynamic CoS Behavior (Multiple Subscribers Enabled on Logical Interface)
RADIUS CoA for service or variable change	Replaces the following parameters: <ul style="list-style-type: none"> ■ Delay buffer rate ■ Guaranteed rate ■ Scheduler map ■ Shaping rate 	Replaces the following parameters: <ul style="list-style-type: none"> ■ Delay buffer rate ■ Guaranteed rate ■ Shaping rate Does not replace the scheduler map	Combines the values of the following parameters to their maximum scalar value: <ul style="list-style-type: none"> ■ Delay buffer rate ■ Guaranteed rate ■ Shaping rate Replaces the scheduler map parameter
RADIUS CoA for service activation	Does not merge queues	Merge queues if the queue specified in the service profile is not already in use for the subscriber NOTE: Do not instantiate a CoA request using a service dynamic profile that is already in use on the same logical interface.	Merge queues if the queue specified in the service profile is not already in use for the subscriber NOTE: Do not instantiate a CoA request using a service dynamic profile that is already in use on the same logical interface.

- Related Topics**
- Configuring Static Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 389
 - Configuring Dynamic Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 391
 - Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview on page 52
 - RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 29
 - Guidelines for Configuring CoS for Subscriber Access on page 388

Guidelines for Configuring CoS for Subscriber Access

When configuring CoS for subscriber access, consider the following guidelines:

- In the current release, you configure the traffic scheduling and shaping parameters in a traffic-control profile within the dynamic profile. You can configure the scheduler map and schedulers in a dynamic profile or in the **[edit class-of-service]** hierarchy. You must statically configure the remaining CoS parameters, such as hierarchical scheduling, classifiers, drop profiles, and forwarding classes, in the **[edit class-of-service]** hierarchy.
- You must enable hierarchical scheduling in the static CLI for the interface referenced in the dynamic profile. If not, the dynamic profile fails.
- You can configure only one traffic-control-profile under a dynamic profile.
- You must define the output-traffic-control-profile that binds the traffic-control profile to the interface within the same dynamic profile as the interface.
- We recommend that you provide different names for the schedulers defined in dynamic profiles that are used for access and services. For example, if there are two dynamic profiles, voice-profile and video-profile, provide unique names for the schedulers defined under those profiles.
- You must use a service dynamic profile with a different profile name for each RADIUS CoA request over the same logical interface.

Related Topics ■ [Configuring Static Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 389](#)

Chapter 28

Configuring Class of Service for Subscriber Access

- Configuring Static Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 389
- Configuring Dynamic Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 391
- Configuring Traffic Shaping and Scheduling in a Dynamic Profile on page 392
- Configuring Schedulers in a Dynamic Profile on page 393
- Configuring a Subscriber Interface to Provide Initial CoS Parameters Dynamically Obtained from RADIUS on page 394
- Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 397
- Applying CoS to an Interface in a Dynamic Profile on page 400
- Configuring CoS on a Set of Static IP Demux Interfaces on page 400

Configuring Static Scheduling and Queuing in a Dynamic Profile for Subscriber Access

You can configure CoS in dynamic profile for subscriber access.

To configure CoS in a dynamic profile for subscriber access:

1. Configure static CoS parameters in the [edit class-of-service] hierarchy.
 - a. Configure the scheduler map, forwarding classes, and schedulers.

You reference the scheduler map in the dynamic profile.
 - b. Configure drop profiles.
 - c. Enable the hierarchical scheduler for the interface.

See the *JUNOS Class of Service Configuration Guide* for information about configuring static CoS parameters.

2. Configure a static or dynamic subscriber interface.

See “Configuring Static Subscriber Interfaces in Dynamic Profiles” on page 311 and “Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles” on page 314.

3. Configure CoS parameters in a dynamic profile.

a. Configure the dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 283.

b. Configure traffic shaping and scheduling parameters in the dynamic profile using a traffic-control profile.

Reference the scheduler map you configured in the static `[edit class-of-service]` hierarchy.

See “Configuring Traffic Shaping and Scheduling in a Dynamic Profile” on page 392.

c. Apply CoS parameters to a subscriber interface by referencing an interface in the dynamic profile.

See “Applying CoS to an Interface in a Dynamic Profile” on page 400.

4. To configure default values for subscribers on login, and enable subscribers to replace other CoS parameters when replacing services, configure variables in the dynamic profile.

See “Configuring User-Defined CoS Variables in a Dynamic Service Profile” on page 397.

- Related Topics**
- CoS for Subscriber Access Overview on page 377
 - Example: Configuring Static Scheduling and Queuing for Subscriber Access on page 403

Configuring Dynamic Scheduling and Queuing in a Dynamic Profile for Subscriber Access

You can configure dynamic scheduling and queuing in dynamic profile for subscriber access.

To configure dynamic scheduling and queuing for subscriber access:

1. Configure a static or dynamic subscriber interface.

See “Configuring Static Subscriber Interfaces in Dynamic Profiles” on page 311 and “Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles” on page 314.

2. Configure CoS parameters in a dynamic profile.

- a. Configure the dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 283.

- b. Configure traffic shaping and scheduling parameters in the dynamic profile using a traffic-control profile.

See “Configuring Traffic Shaping and Scheduling in a Dynamic Profile” on page 392.

- c. Configure the schedulers and scheduler map in the dynamic profile.

See “Configuring Schedulers in a Dynamic Profile” on page 393.

- d. Apply CoS parameters to a subscriber interface by referencing an interface in the dynamic profile.

See “Applying CoS to an Interface in a Dynamic Profile” on page 400.

3. (Optional) Configure variables in access and service profiles to enable RADIUS to activate subscriber and upgrade services through CoA.



NOTE: Do not instantiate a CoA request using a service dynamic profile that is already in use on the same logical interface.

Because you have configured the scheduler map in the dynamic profile, queues are merged when subscribers change services. Other CoS parameters are replaced.

When multiple subscribers are enabled on a DHCP subscriber interface, the system does not replace the parameters. Instead, it combines the values of the parameters to their maximum scalar value.

- a. Configure CoS variables in a dynamic profile.

See “Configuring User-Defined CoS Variables in a Dynamic Service Profile” on page 397

- b. (Optional) Enable multiple subscribers on a logical interface by configuring the **aggregate-clients** option for the dynamic profile attached to a DHCP subscriber interface.

See “Attaching Dynamic Profiles to DHCP Subscriber Interfaces” on page 62.

4. Configure the remaining static CoS parameters in the [edit class-of-service] hierarchy.
 - a. Configure the drop profiles. The scheduler map and schedulers are already configured in the dynamic profile.

See the *JUNOS Class of Service Configuration Guide* for information about configuring the scheduler map.

- b. Enable the hierarchical scheduler for the interface.

See the *JUNOS Class of Service Configuration Guide* for information about configuring the remaining CoS parameters.

- Related Topics**
- CoS for Subscriber Access Overview on page 377
 - Example: Configuring Dynamic Scheduling and Queuing for Subscriber Access on page 406

Configuring Traffic Shaping and Scheduling in a Dynamic Profile

You use traffic-control profiles to configure traffic shaping and scheduling properties. When you reference a traffic-control profile in a dynamic profile, you can provide hierarchical shaping and scheduling for a subscriber interface.

To configure traffic-control profiles in a dynamic profile:

1. Create the traffic-control profile and assign a name.

```
[edit dynamic-profiles business-profile class-of-service]
user@host# edit traffic-control-profiles tcp-data
```

2. Reference a scheduler map in the dynamic profile. The scheduler map is statically configured in the [edit class-of-service] hierarchy.

```
[edit dynamic-profiles business-profile class-of-service traffic-control-profiles]
user@host# set scheduler-map data-map
```

3. Configure the shaping rate to be used in the dynamic profile.

```
[edit dynamic-profiles business-profile class-of-service traffic-control-profiles]
user@host# set shaping-rate 10m
```

4. Configure the guaranteed rate to be used in the dynamic profile.

```
[edit dynamic-profiles business-profile class-of-service traffic-control-profiles]
user@host# set guaranteed-rate 10m
```


5. (Optional) Configure the delay-buffer rate. If you do not include this statement, the delay-buffer rate is based on the guaranteed rate if one is configured, or the shaping rate if no guaranteed rate is configured.

```
[edit dynamic-profiles business-profile class-of-service traffic-control-profiles]
user@host# set delay-buffer-rate 10m
```

- Related Topics**
- Configuring Static Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 389
 - CoS for Subscriber Access Overview on page 377

Configuring Schedulers in a Dynamic Profile

This topic describes how to configure schedulers in a dynamic profile for subscriber access.

You use schedulers to define the parameters of output queues. These properties include the amount of interface bandwidth assigned to the queue, the size of the memory buffer allocated for storing packets, the priority of the queue, and the tail drop profiles associated with the queue.

You can configure up to four schedulers in a dynamic profile.

To configure scheduling and queuing in a dynamic profile:

1. Configure the scheduler and queuing parameters.
 - a. Specify the scheduler for which you want to configure parameters.

```
[edit dynamic-profiles class-of-service]
user@host# set schedulers be-sch
```

- b. Configure the buffer size.

```
[edit dynamic-profiles class-of-service schedulers be-sch]
user@host# set buffer-size remainder
```

- c. Configure the drop-profile map and drop profile.

```
[edit dynamic-profiles class-of-service schedulers be-sch]
user@host# set drop-profile-map loss-priority any protocol any drop-profile d3
```

- d. Configure the priority.

```
[edit dynamic-profiles class-of-service schedulers be-sch]
user@host# set priority low
```

- e. Configure the transmit rate.

```
[edit dynamic-profiles class-of-service schedulers be-sch]
user@host# set transmit-rate percent 40
```


2. Associate the scheduler with a scheduler map.

- a. Configure the scheduler map name.

```
[edit dynamic-profiles class-of-service]
user@host# set scheduler-maps data-smap
```

- b. Configure the forwarding class.

```
[edit dynamic-profiles class-of-service scheduler-maps data-smap]
user@host# set forwarding-class be
```

- c. Configure the scheduler.

```
[edit dynamic-profiles class-of-service scheduler-maps data-smap]
user@host# set scheduler be_sch
```

Related Topics ■ Changing CoS Services Overview on page 385

Configuring a Subscriber Interface to Provide Initial CoS Parameters Dynamically Obtained from RADIUS

You can configure a subscriber interface so that subscribers receive initial CoS parameters that the router obtains from the RADIUS authentication server when subscribers log in using that logical interface on the router.

This topic includes the following tasks:

1. Configuring RADIUS With Initial CoS Values for CoS Parameters on page 394
2. Configuring a Subscriber Interface That Supports Hierarchical CoS on page 395
3. Associate a Client Dynamic Profile with the Subscriber Interface on page 395
4. Configuring Initial Traffic-Shaping Parameters to be Obtained from RADIUS on page 395
5. Configuring Static Forwarding Classes and Scheduler Maps on page 396
6. Configuring Initial Scheduling and Queuing Parameters to be Obtained from RADIUS on page 396
7. Associating RADIUS-obtained CoS Parameters to the Subscriber Interface on page 397

Configuring RADIUS With Initial CoS Values for CoS Parameters

Configure external RADIUS server return VSA 26–108 with traffic-shaping parameters and VSA 26–146 with scheduler parameters for a router interface you expect subscribers to log in on.

- To configure a RADIUS authentication server to include CoS traffic-shaping parameters in authentication grants on certain subscriber interfaces, configure Juniper Networks VSA 26–108.

- To configure a RADIUS authentication server to include CoS scheduling and queuing parameters in authentication grants a certain subscriber interfaces, configure Juniper Networks VSA 28–146.

See “Router Interaction with RADIUS Servers Overview” on page 18 and “Configuring RADIUS Server Parameters for Subscriber Access” on page 21.

See “Extended DHCP Local Server Overview” on page 48 and “Juniper Networks VSAs Supported by the AAA Service Framework” on page 32.

Configuring a Subscriber Interface That Supports Hierarchical CoS

Configure a subscriber interface that supports hierarchical CoS. The following types of subscriber interfaces support hierarchical CoS:

- Static VLAN interfaces — “Configuring Static Subscriber Interfaces in Dynamic Profiles” on page 311.
- Static VLAN interfaces over aggregated Ethernet — “Configuring a Static VLAN Subscriber Interface over Aggregated Ethernet” on page 329.
- Static IP demux interface sets — see “Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles” on page 314.
- Dynamic IP demux interface sets — see “Configuring a Subscriber Interface Using a Set of Static IP Demux Interfaces” on page 313

For general information about configuring interfaces, see the *JUNOS Network Interfaces Configuration Guide*.

Associate a Client Dynamic Profile with the Subscriber Interface

Attach a client dynamic profile to a subscriber interface that supports hierarchical CoS. To configure, include statements at the [edit dynamic-profiles *client-profile-name* interfaces] hierarchy level:

```
[edit]
interfaces {
  . . . supported_interface_configuration . . .
}
```

For general information about configuring interfaces, see the *JUNOS Network Interfaces Configuration Guide*.

Configuring Initial Traffic-Shaping Parameters to be Obtained from RADIUS

Attach a client dynamic profile to a subscriber interface that supports hierarchical CoS. To configure, include statements at the [edit dynamic-profiles *client-profile-name* interfaces] hierarchy level:

```
[edit]
dynamic-profiles {
  client-profile-name {
    class-of-service {
```



```

traffic-control-profiles {
  tc-profile-name {
    scheduler-map "$juno-cos-scheduler-map";
    shaping-rate "$junos-cos-shaping-rate";
    guaranteed-rate "$junos-cos-guaranteed-rate";
    delay-buffer-rate "$junos-cos-delay-buffer-rate";
  }
}

```

Configuring Static Forwarding Classes and Scheduler Maps

Configure scheduler maps in the static [edit class-of-service scheduler-maps] hierarchy level:

```

[edit]
class-of-service {
  forwarding-class ( # Associate queue numbers with class names
    queue number scheduler-name;
    queue number scheduler-name;
  )
  scheduler-maps { # Associates queues with scheduler
    smap-name {
      forwarding-class class-name scheduler scheduler-name;
    }
  }
}

```

Configuring Initial Scheduling and Queuing Parameters to be Obtained from RADIUS

Attach a client dynamic profile to a subscriber interface that supports hierarchical CoS. To configure, include statements at the [edit dynamic-profiles *client-profile-name* interfaces] hierarchy level:

```

[edit]
dynamic-profiles {
  client-profile-name {
    class-of-service {
      schedulers {
        scheduler $junos-cos-scheduler {
          transmit-rate "$juno-cos-scheduler-tx";
          buffer-size "$junos-cos-scheduler-bs";
          priority "$junos-cos-scheduler-pri";
          drop-profile-map loss-priority low protocol any "$junos-cos-scheduler-low";
          drop-profile-map loss-priority medium-low protocol any
            "$junos-cos-scheduler-medium-low";
          drop-profile-map loss-priority medium-high protocol any
            "$junos-cos-scheduler-medium-high";
          drop-profile-map loss-priority high protocol any "$junos-cos-scheduler-high";
          drop-profile-map loss-priority any protocol any "$junos-cos-scheduler-any";
        }
      }
    }
  }
}

```



```

    }
  }
}

```

Associating RADIUS-obtained CoS Parameters to the Subscriber Interface

To associate the RADIUS-obtained CoS parameters with the subscriber interface when a subscriber logs in, include the `output-traffic-control-profile` in the `[edit dynamic-profiles client-profile-name class-of-service interfaces]` hierarchy level:

```

[edit]
dynamic-profiles {
  client-profile-name {
    class-of-service {
      interfaces {
        ...
        ...
        output-traffic-control-profile client-profile-name;
      }
    }
  }
}

```

- Related Topics**
- Activating Subscribers and Managing Services in an Access Network on page 7
 - Dynamic Profiles Overview on page 275
 - Dynamic Variables Overview on page 276
 - Subscriber Interfaces that Provide Initial CoS Parameters Dynamically Obtained from RADIUS Overview on page 378
 - Example: Configuring a Subscriber Interface to Provide Initial CoS Parameters Dynamically Obtained from RADIUS on page 410

Configuring User-Defined CoS Variables in a Dynamic Service Profile

You can configure user-defined variables in the dynamic service profile for traffic scheduling and shaping parameters.



NOTE: The JUNOS internal variables for dynamic CoS are only to be used in dynamic access profiles and not in dynamic service profiles.

You can use variables in a dynamic service profile in two ways:

- To enable subscribers to upgrade or downgrade services after login using a RADIUS change of authorization (CoA), configure user-defined variables for CoS parameters as RADIUS attributes.
- To provide subscribers with default values for CoS parameters, configure user-defined variables for CoS parameters with static default values. If you have configured values to be supplied by a RADIUS CoA, subscribers can receive the previously configured default value when deactivating a service.

You activate the variables by referencing them in the traffic control profile configured in the dynamic service profile.

To configure user-defined variables for CoS in a dynamic profile:

1. Specify that you want to configure variables in the dynamic profile.

```
[edit dynamic-profiles residential-silver variables]
```

2. Do one of the following to configure variables for the shaping rate:
 - Enable RADIUS to modify the shaping rate based on service changes.

- a. Configure the attribute:

```
[edit dynamic-profiles residential-silver variables]
user@host# set srate radius vendor-id 4874 attribute 108
```

- b. Configure the tag:

```
[edit dynamic-profiles residential-silver variables]
user@host# set srate radius vendor-id 4874 tag 1
```

- Configure a default value for the shaping rate.

```
[edit dynamic-profiles residential-silver variables]
user@host# set srate default-value 10m
```

3. Do one of the following to configure variables for the guaranteed rate.
 - Enable RADIUS to modify the guaranteed rate based on service changes.

- a. Configure the attribute:

```
[edit dynamic-profiles residential-silver variables]
user@host# set grate radius vendor-id 4874 attribute 108
```

- b. Configure the tag:

```
[edit dynamic-profiles residential-silver variables]
user@host# set grate radius vendor-id 4874 tag 2
```

- Configure a default value for the guaranteed rate.

```
[edit dynamic-profiles residential-silver variables]
user@host# set grate default-value 5m
```

4. Do one of the following to configure variables for the delay buffer rate:
 - Enable RADIUS to modify the delay buffer rate based on service changes.

- a. Configure the attribute:

```
[edit dynamic-profiles residential-silver variables]
user@host# set dbrate radius vendor-id 4874 attribute 108
```

- b. Configure the tag:

```
[edit dynamic-profiles residential-silver variables]
```



```
user@host# set dbrate radius vendor-id 4874 tag 3
```

- Configure a default value for the delay buffer rate.

```
[edit dynamic-profiles residential-silver variables]
user@host# set dbrate default-value 10m
```

5. Do one of the following to configure variables for the scheduler map.

- Enable RADIUS to modify the scheduler map based on service changes.
 - a. Configure the attribute:

```
[edit dynamic-profiles residential-silver variables]
user@host# set smap radius vendor-id 4874 attribute 108
```

- b. Configure the tag:

```
[edit dynamic-profiles residential-silver variables]
user@host# set smap radius vendor-id 4874 tag 4
```

- Configure a default value for the scheduler map.

```
[edit dynamic-profiles residential-silver variables]
user@host# set smap default-value triple-play
```

6. Configure the variables for the CoS parameters in the traffic control profile.

Either the shaping rate or the guaranteed rate are required in the traffic control profile.

- a. Specify that you want to configure CoS parameters in the dynamic profile.

```
user@host# edit dynamic-profiles residential-silver class-of-service  
traffic-control-profiles tcp1
```

- b. Configure the scheduler map variable.

```
[edit dynamic-profiles residential-silver class-of-service traffic-control-profiles  
tcp1]
user@host# set scheduler-map "$smap"
```

- c. Configure the shaping rate variable.

```
[edit dynamic-profiles residential-silver class-of-service traffic-control-profiles  
tcp1]
user@host# set shaping-rate "$srate"
```

- d. Configure the guaranteed rate variable.

```
[edit dynamic-profiles residential-silver class-of-service traffic-control-profiles  
tcp1]
user@host# set guaranteed-rate "$grate"
```

- e. Configure the delay buffer rate variable.


```
[edit dynamic-profiles residential-silver class-of-service traffic-control-profiles
tcp1]
user@host# set delay-buffer-rate "$dbrate"
```

- Related Topics**
- Changing CoS Services Overview on page 385
 - Guidelines for Configuring CoS for Subscriber Access on page 388

Applying CoS to an Interface in a Dynamic Profile

After you configure the CoS parameters in a dynamic profile, you apply them to an interface. The output-traffic control profile enables you to provide traffic scheduling to the interface.

To apply CoS attributes to an interface in a dynamic profile:

1. Specify that you want to apply CoS attributes to an interface in the dynamic profile.

```
user@host# edit dynamic-profiles business-data class-of-service
```

2. Configure the interface name and logical interface using a variable, and apply the output-traffic control profile to the interface.

Reference the name of the traffic-control profile that contains the scheduling properties that you want to use.

```
[edit dynamic-profiles business-data class-of-service interfaces]
user@host# set interfaces $junos-interface-ifd-name unit
$junos-underlying-interface-unit output-traffic-control-profile data-tcp
```

- Related Topics**
- Configuring Static Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 389
 - CoS for Subscriber Access Overview on page 377

Configuring CoS on a Set of Static IP Demux Interfaces

You can configure CoS on a set of static IP demux interfaces. The static IP demux interface represents a subscriber.

Although the interface set is applied at the [edit interfaces] hierarchy level, the CoS parameters for the interface set are defined at the [edit class-of-service interfaces] hierarchy level, usually with the output-traffic control profile statement.

Before you configure CoS on a static subscriber interface:

- Configure the static IP demux interface.

See Configuring Static IP Demux Interfaces for Subscribers.

To configure CoS on a set of static IP demux interfaces:

1. Define the CoS parameters for the interface set.

```
class-of-service {
  traffic-control-profiles {
    voice {
      scheduler-map voice;
      shaping-rate 64k;
    }
    video {
      scheduler-map video;
      shaping-rate 5m;
    }
    data {
      scheduler-map data;
      shaping-rate 3m;
    }
    t2 {
      shaping-rate 7m;
    }
  }
}
```

2. Apply the CoS parameters to the interface set.

```
interfaces {
  demux-set1 {
    output-traffic-control-profile T2;
  }
  demux-set2 {
    output-traffic-control-profile T2;
  }
  demux0 {
    unit 0 {
      output-traffic-control-profile Voice;
    }
    unit 1 {
      output-traffic-control-profile Video;
    }
    unit 2 {
      output-traffic-control-profile Data;
    }
    unit 3 {
      output-traffic-control-profile Voice;
    }
    unit 4 {
      output-traffic-control-profile Video;
    }
    unit 5 {
      output-traffic-control-profile Data;
    }
  }
}
```



```
}
scheduler-maps {
  voice {
    forwarding-class assured-forwarding scheduler s0;
  }
  video {
    forwarding-class expedited-forwarding scheduler s0;
  }
  data {
    forwarding-class best-effort scheduler s0;
  }
}
schedulers {
  s0 {
    transmit-rate percent 100;
    buffer-size percent 100;
  }
}
```

Related Topics ■ For more information about interface sets and hierarchical scheduling for VLANs, see the *JUNOS Class of Service Configuration Guide*

Chapter 29

Class of Service for Subscriber Access Examples

- Example: Configuring Static Scheduling and Queuing for Subscriber Access on page 403
- Example: Configuring Aggregate Scheduling of Queues for Residential Subscribers on Static IP Demux Interfaces on page 404
- Example: Configuring Dynamic Scheduling and Queuing for Subscriber Access on page 406
- Example: Configuring a Subscriber Interface to Provide Initial CoS Parameters Dynamically Obtained from RADIUS on page 410

Example: Configuring Static Scheduling and Queuing for Subscriber Access

This example shows you how to configure CoS for a subscriber in a dynamic profile. The CoS parameters configure a best-effort, data service for subscribers.

1. Configure the static CoS parameters in the [edit class-of-service] hierarchy.

You must configure the scheduler maps in this hierarchy; it will get referenced in the dynamic profile.

```
class-of-service {
  forwarding-classes {
    queue 0 best-effort;
    queue 1 expedited-forwarding;
    queue 3 network-control;
    queue 2 assured-forwarding;
  }
  scheduler-maps {
    data_smap {
      forwarding-class best-effort scheduler be_sch;
    }
  }
  schedulers {
    be_sch {
      transmit-rate percent 10;
      buffer-size remainder;
      priority low;
    }
  }
}
```



```
}
```

2. Configure the subscriber interface in the [edit interfaces] hierarchy. Enable hierarchical scheduling for the interface.

```
interfaces {
  ge-2/2/0 {
    hierarchical-scheduler;
    vlan-tagging;
    unit 100 {
      vlan-id 100;
      family inet {
        unnumbered-address lo0.0 preferred-source-address 100.0.0.1;
      }
    }
  }
}
```

3. Configure CoS in the dynamic profile.

```
dynamic-profiles {
  data-service {
    interfaces {
      "$junos-interface-ifd-name" {
        unit "$junos-underlying-interface-unit" {
          family inet;
        }
      }
    }
  }
  class-of-service {
    traffic-control-profiles {
      tcp1 {
        scheduler-map data_smap;
        shaping-rate 50k;
        guaranteed-rate 10k;
      }
    }
    interfaces {
      "$junos-interface-ifd-name" {
        unit "$junos-underlying-interface-unit" {
          output-traffic-control-profile tcp1;
        }
      }
    }
  }
}
```

Example: Configuring Aggregate Scheduling of Queues for Residential Subscribers on Static IP Demux Interfaces

In this example, scheduling is configured for a residential subscriber. Each forwarding class represents a multiplay service (voice, video and data), and is equivalent to a queue.

An interface set of IP demux interfaces represents a DSLAM, and provides shaping of subscribers services to a DSLAM aggregate rate.

```

interfaces {
  interface-set demux-set {
    interface demux0 {
      unit 0;
      unit 1;
    }
  }
  ge-2/0/1 {
    vlan-tagging;
    unit 1 {
      per-session-scheduler;
      vlan-id 1;
      demux-source inet;
      family inet {
        address 4.4.4.4/24;
      }
    }
  }
  demux0 {
    unit 0 {
      demux-options {
        underlying-interface ge-2/0/1.1;
      }
      family inet {
        demux-source {
          1.1.1.0/24;
        }
        address 1.1.1.1/24;
      }
    }
    unit 1 {
      demux-options {
        underlying-interface ge-2/0/1.1;
      }
      family inet {
        demux-source {
          1.1.2.0/24;
        }
        address 1.1.2.1/24;
      }
    }
  }
}
class-of-service {
  traffic-control-profiles {
    T1 {
      scheduler-map m1;
      shaping-rate 5m;
    }
    T2 {
      shaping-rate 60m;
    }
  }
}

```



```

interfaces {
  demux-set {
    output-traffic-control-profile T2;
  }
  demux0 {
    unit 0 {
      output-traffic-control-profile T1;
    }
    unit 1 {
      output-traffic-control-profile T1;
    }
  }
  scheduler-maps {
    m1 {
      forwarding-class best-effort scheduler s0;
      forwarding-class expedited-forwarding scheduler s1;
      forwarding-class assured-forwarding scheduler s2;
      forwarding-class network-control scheduler s3;
    }
  }
  schedulers {
    s0 {
      transmit-rate percent 10;
      buffer-size percent 10;
    }
    s1 {
      transmit-rate percent 20;
      buffer-size percent 20;
    }
    s2 {
      transmit-rate percent 30;
      buffer-size percent 30;
    }
    s3 {
      transmit-rate percent 40;
      buffer-size percent 40;
    }
  }
}

```

Example: Configuring Dynamic Scheduling and Queuing for Subscriber Access

In this example, subscribers are provided with a data and voice service defined in an access profile when they initially log in. The service activation is performed at login.

After the initial login, the subscriber adds an assured forwarding service that is not defined in the original access profile. A service profile is used to configure the schedulers and a RADIUS CoA activates the service. The queues defined for the schedulers in the initial scheduler map and the new scheduler map are merged.

In addition, the values for the initial data and voice service are upgraded by the RADIUS administrator through a separate RADIUS CoA message.

To configure the initial service and enable the activation through a RADIUS CoA:

1. Configure the access profile for the service activation.
 - a. Configure the RADIUS attribute variables in the initial dynamic profile.

```
dynamic-profiles access-profile {
  variables {
    smap {
      radius {
        vendor-id 4874 {
          attribute 108;
          tag 4;
        }
      }
    }
    srate {
      radius {
        vendor-id 4874 {
          attribute 108;
          tag 1;
        }
      }
    }
    grate {
      radius {
        vendor-id 4874 {
          attribute 108;
          tag 2;
        }
      }
    }
    dbrate {
      radius {
        vendor-id 4874 {
          attribute 108;
          tag 3;
        }
      }
    }
  }
}
```

Table 31 on page 407 lists the initial values defined by the RADIUS administrator for the tags used in this example.

Table 31: Initial CoS Values for Subscriber Login

Variable	RADIUS Tag	Value
Shaping rate	T01	6m
Guaranteed rate	T02	4m
Delay buffer rate	T03	1m
Scheduler map	T04	data_voice_smap

- b. Configure the class of service parameters in the access profile.

Include the configurations for the interfaces, schedulers, and the scheduler maps.

```
dynamic-profiles access-profile {
  class-of-service {
    traffic-control-profiles {
      tcp1 {
        scheduler-map "$smap";
        shaping-rate "$srate";
        guaranteed-rate "$grate";
        delay-buffer-rate "$dbrate";
      }
    }
    interfaces {
      "$junos-interface-ifd-name" {
        unit "$junos-underlying-interface-unit" {
          output-traffic-control-profile tcp1;
        }
      }
    }
    scheduler-maps {
      data_voice_smap {
        forwarding-class be scheduler be_sch;
        forwarding-class ef scheduler ef_sch;
      }
    }
    schedulers {
      be_sch {
        transmit-rate percent 40;
        buffer-size remainder;
        priority low;
        drop-profile-map loss-priority any protocol any drop-profile d3;
      }
      ef_sch {
        transmit-rate percent 20;
        buffer-size remainder;
        priority low;
        drop-profile-map loss-priority any protocol any drop-profile d2;
      }
    }
  }
}
```

2. Configure the interfaces for the access profile.

```
dynamic-profiles access-profile {
  interfaces {
    "$junos-interface-ifd-name" {
      unit "$junos-underlying-interface-unit" {
        family inet;
      }
    }
  }
}
```

3. Configure the forwarding classes in the static [edit class-of-service] hierarchy.


```

class-of-service {
  drop-profiles {
    d0 {
      fill-level 25 drop-probability 100;
      fill-level 0 drop-probability 0;
    }
    d1 {
      fill-level 50 drop-probability 100;
      fill-level 0 drop-probability 0;
    }
    d2 {
      fill-level 75 drop-probability 100;
      fill-level 0 drop-probability 0;
    }
    d3 {
      fill-level 0 drop-probability 0;
      fill-level 100 drop-probability 100;
    }
  }
  forwarding-classes {
    queue 0 be;
    queue 1 ef;
    queue 2 af;
    queue 3 nc;
  }
  interfaces {
    ge-1/2/9 {
      shaping-rate 100m;
    }
  }
}

```

4. Configure the service profile to enable RADIUS to activate the assured forwarding service after login.

```

dynamic profiles service-af {
  class-of-service {
    scheduler-maps {
      service-af-smap {
        forwarding-class af scheduler af_sched;
      }
    }
    schedulers {
      af_sched {
        transmit-rate percent 30;
        buffer-size remainder;
        priority low;
        drop-profile-map loss-priority any protocol any drop-profile d1;
      }
    }
  }
}

```


Subscribers receive upgraded values for the initial data and voice service when RADIUS sends a change of authorization (CoA). In this case, the CoS parameters are replaced, because multiple subscribers were not enabled on the logical interface.

Table 32 on page 410 lists the upgraded values defined by the RADIUS administrator.

Table 32: Upgraded CoS Values for the Video Service

Variable	RADIUS Tag	Value
Shaping rate	T01	14m
Guaranteed rate	T02	13m
Delay buffer rate	T03	12m
Scheduler map	T04	data_voice_smap

- Related Topics**
- Changing CoS Services Overview on page 385
 - Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 397

Example: Configuring a Subscriber Interface to Provide Initial CoS Parameters Dynamically Obtained from RADIUS

The following configuration is an example of a client dynamic profile in which JUNOS internal variables for dynamic CoS are used to obtain CoS variables from the RADIUS server when a subscriber authenticates over a logical interface to which this dynamic profile is applied. The traffic-control profile `tcp1` references internal variables to specify a RADIUS-obtained scheduler-map name and traffic-shaping parameter values. The scheduler configuration uses internal variables to specify a RADIUS-obtained scheduler name and parameter values:

```
[edit]
dynamic-profiles {
  residential-silver {
    interfaces {
      "$junos-interface-ifd-name" {
        unit "$junos-underlying-interface-unit" {
          family inet;
        }
      }
    }
  }
  class-of-service {
    interfaces {
      "$junos-interface-ifd-name" {
        unit "$junos-underlying-interface-unit" {
          output-traffic-control-profile tcp1;
        }
      }
    }
  }
  traffic-control-profiles {
    tcp1 {
      scheduler-map "$junos-cos-scheduler-map";
    }
  }
}
```



```

        shaping-rate "$junos-cos-shaping-rate";
        guaranteed-rate "$junos-cos-guaranteed-rate";
        delay-buffer-rate "$junos-cos-delay-buffer-rate";
    }
}
scheduler-maps {
    business_smap_1 {
        forwarding-class fc_a scheduler af_scheduler;
    }
    business_smap_2 {
        forwarding-class fc_b scheduler be_scheduler;
    }
    business_smap_3 {
        forwarding-class fc_c scheduler ef_scheduler;
    }
    business_smap_4 {
        forwarding-class fc_d scheduler nc_scheduler;
    }
}
schedulers {
    $junos-cos-scheduler {
        transmit-rate "$junos-cos-scheduler-tx";
        buffer-size "$junos-cos-scheduler-bs";
        priority "$junos-cos-scheduler-pri";
        drop-profile-map loss-priority low protocol any drop-profile
            $junos-cos-scheduler-dropfile-low;
        drop-profile-map loss-priority medium-low protocol any drop-profile
            $junos-cos-scheduler-dropfile-medium-low;
        drop-profile-map loss-priority medium-high protocol any drop-profile
            $junos-cos-scheduler-dropfile-medium-high;
        drop-profile-map loss-priority high protocol any drop-profile
            $junos-cos-scheduler-dropfile-high;
    }
}
}
}
}
}

```

For this example, assume the following:

- Subscribers authenticate over an EQ DPC logical interface to which this dynamic profile is applied.
- The scheduler map specified by the RADIUS server is one of the four maps configured in this client dynamic profile.
- The forwarding classes referenced by the scheduler-maps in this client dynamic profile are configured at the static [edit class-of-service forwarding-classes] hierarchy level.
- The drop profiles referenced by the RADIUS-specified scheduler are configured at the static [edit class-of-service drop-profiles] hierarchy level.

Related Topics

- Activating Subscribers and Managing Services in an Access Network on page 7
- Dynamic Profiles Overview on page 275
- Dynamic Variables Overview on page 276

- Subscriber Interfaces that Provide Initial CoS Parameters Dynamically Obtained from RADIUS Overview on page 378
- Configuring a Subscriber Interface to Provide Initial CoS Parameters Dynamically Obtained from RADIUS on page 394

Chapter 30

Class of Service Shaping-Rate Adjustments Overview

- Hierarchical CoS Shaping-Rate Adjustments Overview on page 413
- CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview on page 414
- Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 415

Hierarchical CoS Shaping-Rate Adjustments Overview

This overview describes how an MX-series router installed as an edge router in a subscriber access network can adjust hierarchical class-of-service (CoS) policy to prevent bandwidth contention at subscriber interfaces on Enhanced Queuing Dense Port Concentrator (EQ DPC) ports.

High-speed data service subscribers typically receive some combination of voice, data, and video services from an access network. Subscriber traffic is delivered from the access network, through a router, through a switched Ethernet network, to an Ethernet digital subscriber line access multiplexer (DSLAM). The DSLAM, in turn, forwards the subscriber's traffic to the residential gateway over a digital subscriber line (DSL). An MX-series router that is installed in a subscriber access network as an edge router can perform subscriber management functions that include subscriber identification and per-subscriber CoS.

To an MX-series router in a subscriber access network, a subscriber is an authenticated user—a user that has logged into the access network at a subscriber interface and then been verified by the configured authentication server and subsequently granted initial CoS services. Subscribers can be identified statically or dynamically. You can create a subscriber interface over a static VLAN interface, a static IP demux interface, a static interface set, or a dynamic IP demux interface that is created when a subscriber logs in using a Dynamic Host Configuration Protocol (DHCP) access method.

Per-subscriber CoS is supported only for subscriber interfaces on EQ DPC ports operating in hierarchical scheduler mode. For these types of subscriber interfaces, which can be static VLAN interfaces or static interface sets, you can configure hierarchical CoS. Hierarchical CoS enables you to apply traffic shaping parameters (which can include a delay-buffer bandwidth) and packet transmission scheduling parameters (which can include buffer management parameters) to an individual subscriber interface rather than to all interfaces configured on the port.

The characteristics of voice, data, and video applications vary widely in their requirements for traffic throughput, bandwidth management, delay and jitter tolerance, and buffer depth. To enhance the flexibility of the hierarchical CoS implementation in a subscriber access network, you can configure the MX-series router to perform real-time adjustments to the shaping rate configured for subscriber interfaces for residential gateways. Enabling a shaping-rate adjustment option on the router can prevent bandwidth contention at the interface from causing degradation of the subscriber's voice, data, or video services.

- Related Topics**
- CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview on page 414
 - Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 415
 - Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 417
 - Disabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 423
 - Example: Configuring Hierarchical CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 425

CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview

This overview describes how an MX-series router installed as an edge router can adjust hierarchical CoS policy for subscriber interfaces for subscriber local loops. You can configure the router to throttle the traffic sent to subscriber local loops so that the traffic does not exceed the current data transmission rate of those lines. This feature ensures that changes to subscriber local loop speeds do not cause bandwidth contention at the subscriber's residential gateway.

In a typical subscriber access network, traffic destined to a subscriber is delivered from the access network, through an edge router, to a DSLAM. The DSLAM multiplexes subscriber traffic through a DSL, also known as a *local loop*, to the subscriber's residential gateway. When line noise or cross talk in a subcarrier causes the error rate on a DSL to exceed a certain threshold, the DSLAM can adapt itself by lowering the data transmission rate to that carrier device. A lower data transmission rate is less susceptible to induced errors.

You can configure an MX-series router to adjust the configured shaping rates on scheduler nodes for subscriber interfaces that represent subscriber local loops. Whenever a DSLAM resynchronizes a subscriber local loop speed, the router adjusts the configured shaping rate for that line so that the aggregate egress traffic to those subscribers is shaped to the local loop speed before the traffic reaches the DSLAM. Unless the maximum amount of bandwidth allocated to the subscriber interface on the router is throttled to the local loop speed, bandwidth contention can occur at the subscriber's residential gateway, which can cause the DSLAM to drop packets. This type of shaping-rate adjustment requires the topology discovery and traffic-monitoring features of the Access Node Control Protocol (ANCP).

You can configure ANCP to communicate the subscriber local loop speed to the MX-series router, which in turn throttles traffic destined to the associated subscriber interface so that it matches the subscriber local loop speed. A JUNOS daemon, the Access Node Control Protocol daemon (**ancpd**), supports ANCP by acquiring subscriber

line rate information from DSLAMs and then communicating this data transmission rate to the JUNOS class-of-service daemon (`cosd`).

For more information about the ANCP protocol, see the “ANCP Topology Discovery and Traffic Monitoring Overview” on page 465.

- Related Topics**
- Hierarchical CoS Shaping-Rate Adjustments Overview on page 413
 - Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 415
 - Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 417
 - Disabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 423
 - Example: Configuring Hierarchical CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 425

Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops

These guidelines apply to configuring an MX-series router installed as an edge router to adjust the configured shaping rates on scheduler nodes for subscriber interfaces that represent subscriber local loops. This shaping-rate feature uses the topology discovery and traffic-monitoring features of the ANCP.

Keep the following points in mind when you enhance hierarchical CoS policy by configuring ANCP-driven shaping-rate adjustments:

- Shaping-rate adjustments are supported only for subscriber local loops that terminate at DSLAMs that you have configured as ANCP neighbors of the MX-series router.
- Shaping-rate adjustments are supported only for scheduler nodes for which you have configured an initial shaping rate by including the **shaping-rate** statement in a traffic-control profile applied to the scheduler node. Specify the initial shaping rate as a peak rate, in bits per second (bps), and not as a percentage. Other methods of configuring a shaping rate are not supported with this feature.
- Shaping-rate adjustments are supported only for scheduler nodes that are static logical interface sets that you have configured to operate at Level 3 of the scheduler hierarchy on the router. If an interface set is configured with a logical interface (such as unit 0) and queue, then the interface-set is an internal scheduler node (as opposed to a root node or a leaf node) at Level 2 of the hierarchy. However, if there are no traffic control profiles configured on logical interfaces in an interface set, then the interface set is an internal scheduler node at Level 3 of the hierarchy.
- Shaping-rate adjustments are supported only for subscriber interfaces over physical interfaces that you have configured to operate in hierarchical scheduler mode. Only ports on EQ DPCs in MX-series routers support hierarchical scheduler mode.
- After shaping-rate adjustments are enabled and the router has performed shaping-rate adjustments on a scheduler node, you can configure a new shaping rate by including the **shaping-rate** statement in a traffic-control profile and then

applying that profile to that scheduler node. However, this new shaping-rate value does not immediately result in shaping traffic at the new rate. The scheduler node continues to be shaped at rate set by ANCP. Only when the ANCP shaping-rate adjustment feature is disabled is the scheduler node shaped at the newly configured shaping-rate.

- The Layer 2 Tunneling Protocol (L2TP) is often used to carry traffic securely between an L2TP Network Server (LNS) and an L2TP Access Concentrator (LAC). The QoS adjustment feature supports the shaping overhead options that you can use to add a specified number of bytes to the actual packet length when determining shaped session packet length. ANCP shaping-rate adjustments are not supported for ingress traffic, only for egress traffic. To configure the number of bytes to add to the packet at the egress side of the tunnel, include the **egress-shaping-overhead** and **mode** statements at the **[edit chassis fpc slot-number pic *pic-number* traffic-manager]** hierarchy level. Use the shaping overhead options if you need to account for encapsulation overhead.

For more information about the ANCP protocol, see the “ANCP Topology Discovery and Traffic Monitoring Overview” on page 465.

Related Topics

- Hierarchical CoS Shaping-Rate Adjustments Overview on page 413
- CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview on page 414
- Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 417
- Disabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 423
- Example: Configuring Hierarchical CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 425

Chapter 31

Configuring Class of Service Shaping-Rate Adjustments

- Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 417
- Disabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 423

Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops

You can enhance a CoS implementation by enabling an MX-series router to adjust the hierarchical CoS policy shaping rate configured for static interface sets that consist of two or more VLANs and represent subscriber local loops. Whenever the digital subscriber line access multiplexer (DSLAM) resynchronizes its data transmission rate to a digital subscriber line (DSL), the router adjusts the shaping rate for the associated subscriber interface so that the maximum bandwidth allocation cannot exceed the current data rate for the associated subscriber local loop. This feature ensures that data transmission rate adjustments by the DSLAM do not cause bandwidth contention at the subscriber's residential gateway.

This topic includes the following tasks:

1. Configuring Static Logical Interface Sets to Serve as CoS Hierarchical Scheduler Nodes for Subscriber Loops on page 417
2. Configuring the Logical Interfaces That Compose the Static Logical Interface Sets on page 418
3. Configuring Hierarchical CoS on the Static Logical Interface Sets That Serve as Hierarchical Scheduler Nodes for Subscriber Local Loops on page 419
4. Configuring ANCP Functionality That Supports and Drives Shaping-Rate Adjustments for Subscriber Local Loops on page 421
5. Displaying Configuration Information About ANCP on page 422
6. Displaying Configuration Information About Shaping-Rate Adjustments for Subscriber Local Loops on page 422

Configuring Static Logical Interface Sets to Serve as CoS Hierarchical Scheduler Nodes for Subscriber Loops

To configure a logical interface set, begin by including the `interface-set` statement with the `interface-set-name` option at the `[edit interfaces]` hierarchy level.

An interface set is composed of two or more logical interfaces on the same physical interface. Each logical interface in an interface set corresponds to an individual subscriber service, such as voice, video, or data. To specify either a list of logical unit numbers or the single outer VLAN tag used to identify the logical interfaces that compose the interface set, include statements at the `[edit interfaces interface-set interface-set-name]` hierarchy level:

- For an interface set composed of a list of logical interfaces identified by an inner VLAN tag on Ethernet frames (called the customer VLAN, or C-VLAN, tag), you must specify each logical interface by including the `unit` statement with the `logical-unit-number` option.

```
[edit]
interfaces {
  interface-set interface-set-name {
    interface ethernet-interface-name { # EQ DPC port
      unit logical-unit-number;
      unit logical-unit-number;
      ...
    }
    ...
  }
}
```

- For an interface set composed of a set of VLANs grouped at the DSLAM and identified by the same service VLAN (S-VLAN) tag), you must specify the S-VLAN tag as the outer VLAN tag for each VLAN by including the `vlan-tags-outer` statement with the `vlan-tag` option.

```
[edit]
interfaces {
  interface-set interface-set-name {
    interface ethernet-interface-name { # EQ DPC port
      vlan-tags-outer vlan-tag; # Identify the DSLAM
    }
    ...
  }
}
```

For more information about configuring CoS hierarchical schedulers, see the *JUNOS Class of Service Configuration Guide*.

Configuring the Logical Interfaces That Compose the Static Logical Interface Sets

Each underlying physical interface must be configured to operate in hierarchical scheduler mode and to support stacked VLAN tagging on all logical interfaces. To configure, include the `hierarchical-scheduler` statement and the `stacked-vlan-tagging` statement at the `[edit interfaces ethernet-interface-name]` hierarchy level.

To associate the individual logical interfaces of an interface set with specific subscriber services provided by the subscriber local loop, bind an S-VLAN tag and a C-VLAN tag to each logical interface that belongs to a scheduler node that represents a subscriber local loop. Ethernet frames sent from the logical interfaces contain an outer VLAN tag that identifies a DSLAM and an inner VLAN tag that identifies a subscriber port on the DSLAM. To configure, include the `vlan-tags` statement at each logical interface:


```
[edit]
interfaces {
  ethernet-interface-name { # EQ DPC port underlying an interface set
    hierarchical-scheduler;
    stacked-vlan-tagging; # Support 802.1Q VLAN dual-tagged frames
    unit logical-unit-number { # Bind S-VLAN and C-VLAN tags to logical interface
      vlan-tags inner tpid.vlan-id outer tpid.vlan-id;
    }
    ...
  }
}
```

For more information about configuring 802.1Q VLANs, see the *JUNOS Network Interfaces Configuration Guide*.

Configuring Hierarchical CoS on the Static Logical Interface Sets That Serve as Hierarchical Scheduler Nodes for Subscriber Local Loops

To configure hierarchical CoS on the static logical interface set that serves as the hierarchical scheduler node for a subscriber local loop:

1. For each scheduler node that represents a subscriber local loop, configure an initial shaping rate.



NOTE: The CoS shaping-rate feature is supported only for scheduler nodes with a configured shaping rate. The initial shaping rate must be configured by applying a traffic-control profile that includes the **shaping-rate** statement. Specify the initial shaping rate as a peak rate, in bits per second (bps), and not as a percentage. Other methods of configuring a shaping rate are not supported with this feature.

- To enable traffic heading downstream (from the router to the DSLAM) to be gathered into an interface set, include the **interface-set** statement and define the logical interface set name as the *interface-set-name* option at the [edit class-of-service interfaces] hierarchy level.
- To apply output traffic scheduling and shaping parameters at the logical interface set level (rather than at the logical unit level), include the **output-traffic-control-profile** statement and specify the name of a traffic-control profile as the *profile-name* option at the [edit class-of-service interfaces interface-set *interface-set-name*] hierarchy level.

To configure, include the following statements:

```
class-of-service {
  interfaces { # Configure interface-specific CoS for incoming packets
    interface-set interface-set-name { # Configure a hierarchical scheduler
      output-traffic-control-profile tc-profile-name; # Level 3 scheduler node
    }
    ...
  }
  traffic-control-profiles { # Define traffic-control profiles
    tc-profile-name { # Specify a scheduler map and traffic-shaping parameters
```



```

        scheduler-map map-name;
        shaping-rate rate; # This is the "configured shaping rate"
        guaranteed-rate (percent percentage | rate);
        delay-buffer-rate (percent percentage | rate);
    }
    ...
}

```

You can include the statements at the following hierarchy levels:

- [edit class-of-service]
 - [edit dynamic-profiles *profile-name* class-of-service]
2. Configure the scheduler maps referenced in the traffic-control profiles applied to the interface sets, the schedulers referenced in those scheduler maps, and the drop profiles referenced in those schedulers.
 - A scheduler map establishes the traffic output queues (forwarding classes) for a scheduler node and associates each queue with a specific scheduler map.
 - A scheduler defines queue properties (transmit rate, buffer size, priority, and drop profile) that specify how traffic is treated in the output queue.
 - A drop profile specifies how aggressively the MX-series router drops packets that are managed by a particular scheduler by defining either a segmented or interpolated graph that maps output queue fullness to packet drop probability.

To configure, include the statements at the static [edit class-of-service] hierarchy level:

```

[edit]
class-of-service {
  scheduler-maps { # Assign queuing characteristics to output queues
    map-name { # Map output queues to
      forwarding-class class-name scheduler scheduler-name;
      forwarding-class class-name scheduler scheduler-name;
      ...
    }
    ...
  }
  schedulers { # Define queuing characteristics
    scheduler-name { # Specify queuing and buffer management
      transmit-rate transmit-rate-option;
      buffer-size buffer-size-option;
      priority priority-level;
      drop-profile-map loss-priority loss-priority-option protocol any drop-profile
        drop-profile-name;
      ...
    }
  }
  drop-profiles { # Define random early detection (RED) for the delay buffer
    drop-profile-name { # Specify how to drop packets from an output queue
      drop-profile-name ( # Map a queue fullness to a drop probability

```



```

        fill-level percentage drop-probability percentage; # Option 1: segmented
        fill-level percentage drop-probability percentage;
        ...
    }
    interpolate { # Option 2: interpolated
        drop-probability [ values ];
        fill-level [ values ];
    }
    ...
}

```

For more information about configuring scheduler maps, schedulers, and drop profiles, see the *JUNOS Class of Service Configuration Guide*.

Configuring ANCP Functionality That Supports and Drives Shaping-Rate Adjustments for Subscriber Local Loops

To configure the Access Node Control Protocol (ANCP) functionality that supports and drives the shaping-rate adjustments for subscriber local loops:

- Enable the ANCP daemon (**ancpd**) to monitor subscriber local loop rates at the DSLAMs and communicate this information to **cosd**, the JUNOS class-of-service (CoS) daemon.
- Configure each DSLAM as an ANCP neighbor of the router so that TCP connections can be established between the router and each DSLAM.
- Identify the subscriber interface sets whose traffic is monitored and shaped by ANCP, and associate those interface sets with the corresponding identifiers configured on the access node (DSLAM) to uniquely identify the subscriber local loops within the access network.

The JUNOS ANCP daemon **ancpd** uses this information to build a mapping of subscribers to subscriber interfaces. When the **ancpd** receives port management messages from a DSLAM or other access node, it uses the access identifier contained in the message to determine which hierarchical scheduler node corresponds to the subscriber.

To configure, include statements at the **[edit protocols ancp]** hierarchy level:

```

[edit]
protocols {
  ancp {
    qos-adjust; # Enable ANCP to monitor and adjust CoS shaping rates
    neighbor ip-address; # Configure each DSLAM as an ANCP neighbor
    ...
    interfaces { # Identify subscribers for which ANCP can adjust shaping rates
      interface-set {
        interface-set-name {
          access-identifier identifier-string; # DSLAM ID for the local loop
        }
      }
    }
  }
}

```



```

    ...
  }
  ...
}
...
}

```

Displaying Configuration Information About ANCP

If the ANCP daemon (`ancpd`) is running, the following operational commands display or clear information about the ANCP configuration:

- To display ANCP neighbor information, issue the `show ancp neighbor` operational command.
- To clear ANCP neighbors, issue the `clear ancp neighbor` operational command.
- To display ANCP subscriber information, issue the `show ancp subscriber` operational command.
- To display ANCP class-of-service information, issue the `show ancp cos` operational command.

If the ANCP daemon is not yet running, the process starts when you commit a configuration that contains the `protocols ancp` stanza.

For more information about ANCP, see “ANCP Topology Discovery and Traffic Monitoring Overview” on page 465 and “Configuring ANCP” on page 467.

Displaying Configuration Information About Shaping-Rate Adjustments for Subscriber Local Loops

To display the configured shaping rate and the adjusted shaping rate for each logical interface set configured for hierarchical CoS, issue the `show class-of-service interface-set` operational command.



NOTE: After shaping-rate adjustments are enabled and the router has performed shaping-rate adjustments on a scheduler node, you can configure a new shaping rate by including the `shaping-rate` statement in a traffic-control profile and then applying that profile to that scheduler node. However, this new shaping-rate value does not immediately result in shaping traffic at the new rate. The scheduler node continues to be shaped at rate set by ANCP. Only when the ANCP shaping-rate adjustment feature is disabled is the scheduler node shaped at the newly configured shaping-rate.

-
- | | |
|-----------------------|--|
| Related Topics | <ul style="list-style-type: none"> ■ CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview on page 414 ■ Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 415 ■ Disabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 423 ■ Example: Configuring Hierarchical CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 425 |
|-----------------------|--|

Disabling CoS Shaping-Rate Adjustments for Subscriber Local Loops

To disable hierarchical CoS shaping-rate adjustments for subscriber local loops:

- Disable hierarchical CoS traffic-shaping adjustment by ANCP:

```
[edit]
protocols {
  ancp {
    delete qos-adjust;
  }
}
```

Traffic-shaping parameters for all subscriber local loops revert to their current configured values.

- Related Topics**
- CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview on page 414
 - Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 415
 - Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 417
 - Example: Configuring Hierarchical CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 425

Chapter 32

Class of Service Shaping-Rate Adjustments Examples

- Example: Configuring Hierarchical CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 425

Example: Configuring Hierarchical CoS Shaping-Rate Adjustments for Subscriber Local Loops

This example shows how you can enable shaping-rate adjustments for static logical interface sets that represent subscriber local loops:

1. Configure static logical interface sets to serve as CoS hierarchical scheduler nodes for subscriber local loops.

This example uses a single scheduler node that represents two subscriber local loops. The scheduler node is a static logical interface composed of two logical interfaces. The underlying physical interface is port 0 on a Gigabit Ethernet EQ DPC in slot 4, PIC 0:

```
[edit]
interfaces {
  interface-set ifset-of-logical-interfaces {
    interface ge-4/0/0 {
      unit 1;
      unit 2;
    }
  }
  ge-4/0/0 {
    description "access interface ge-4/0/0";
    hierarchical-scheduler;
    stacked-vlan-tagging;
    unit 1 {
      description "DSL type ADSL1 = 0x01";
      proxy-arp;
      vlan-tags outer 1 inner 1; # S-VLAN tag is '1' and C-VLAN tag is '1'
      family inet { # Specify a secondary loopback address
        unnumbered-address lo0.0 preferred-source-address 192.168.7.3;
      }
    }
    unit 2 {
      description "DSL type ADSL1 = 0x01";
      proxy-arp;
    }
  }
}
```



```

        vlan-tags outer 1 inner 2; # S-VLAN tag is '1' and C-VLAN tag is '2'
        family inet { # Specify a secondary loopback address
            unnumbered-address lo0.0 preferred-source-address 192.168.7.4;
        }
    }
}

```

2. Begin configuring hierarchical CoS on the static logical interface set that serves as the hierarchical scheduler node for the group of subscriber local loops.

```

[edit]
class-of-service {
    interfaces {
        interface-set ifset-of-logical-interfaces {
            output-traffic-control-profile tcp-premium-with-4-queues;
        }
    }
}

```

3. Configure the traffic-control profiles that can be applied to the scheduler node:

```

[edit]
class-of-service {
    traffic-control-profiles {
        tcp-basic-rate { # Specify a scheduler map and traffic controls
            shaping-rate 10m;
        }
        tcp-premium-with-4-queues { # Specify a scheduler map and traffic controls
            scheduler-map smap-premium-4q;
            shaping-rate 20m;
            guaranteed-rate 10m;
            delay-buffer-rate 5m;
        }
    }
}

```

In this example, the `tcp-premium-with-4-queues` traffic-control profile is applied to the interface set. The other profile provides a lower shaping rate and no guaranteed rate.

4. Configure the scheduler map `smap-premium-4q` that is referenced in the traffic-control profile for the scheduler node:

```

[edit]
class-of-service {
    scheduler-maps { # Define the queues that comprise each scheduler node
        smap-premium-4q { # Map each queue in the scheduler node to a scheduler
            forwarding-class be scheduler be_sch;
            forwarding-class af scheduler af_sch;
            forwarding-class ef scheduler ef_sch;
            forwarding-class nc scheduler nc_sch;
        }
    }
}

```


- Configure the four schedulers (referenced in the scheduler map) that define the four output queues for the scheduler node:

```
[edit]
class-of-service {
  schedulers { # Define scheduling characteristics of each queue
    be_sch { # Transmit rate and buffer management parameters
      transmit-rate percent 10;
      buffer-size remainder;
      priority low;
    }
    ef_sch { # Transmit rate and buffer management parameters
      ...
    }
    af_sch { # Transmit rate and buffer management parameters
      ...
    }
    nc_sch { # Transmit rate and buffer management parameters
      ...
    }
  }
}
```

- Enable ANCP to communicate with the DSLAM to adjust the CoS shaping rate for the scheduler node.

You must enable the ANCP feature for performing CoS traffic shaping adjustments, configure the DSLAM as an ANCP neighbor, and specify the DSLAM-assigned identifier for the subscriber local loop represented by the scheduler node:

```
[edit]
protocols {
  ancp {
    qos-adjust; # Enable ANCP to adjust CoS shaping rates
    neighbor 10.2.3.4; # Configure the DSLAM as an ANCP neighbor
    interfaces { # Identify subscribers for which ANCP can adjust shaping rates
      interface-set {
        ifset-of-logical-interfaces {
          access-identifier "dslam port 2/3"; # DSLAM ID for the local loop
        }
      }
    }
  }
}
```



NOTE: If the ANCP daemon is not yet running, the process starts when you commit a configuration that contains the `protocols ancp` stanza.

- You can display the configured shaping rate and the adjusted shaping rate for each logical interface set configured for hierarchical CoS, issue the `show class-of-service interface-set` operational command.

- Related Topics**
- Hierarchical CoS Shaping-Rate Adjustments Overview on page 413
 - CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview on page 414
 - Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 415
 - Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 417

Chapter 33

Summary of Class of Service for Subscriber Access Statements

buffer-size

Syntax	buffer-size (percent <i>percentage</i> remainder temporal <i>microseconds</i> \$junos-cos-scheduler-bs);
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>]
Release Information	Statement introduced before JUNOS Release 7.4. The [edit dynamic-profiles <i>profile-name</i>] hierarchy added in JUNOS Release 9.3. The \$junos-cos-scheduler-bs internal variable added in JUNOS Release 9.4.
Description	Specify buffer size.
Default	If you do not include this statement, the default scheduler transmission rate and buffer size percentages for queues 0 through 7 are 95, 0, 0, 5, 0, 0, 0, and 0 percent.
Options	<p>percent <i>percentage</i>—Buffer size as a percentage of total buffer.</p> <p>remainder—Remaining buffer available.</p> <p>temporal <i>microseconds</i>—Buffer size as a temporal value. The queuing algorithm starts dropping packets when it queues more than a computed number of bytes. This maximum is computed by multiplying the logical interface speed by the configured temporal value.</p> <p>Range: The ranges vary by platform as follows:</p> <ul style="list-style-type: none"> ■ For other M-series platforms: 1 through 200,000 microseconds. ■ For IQ PICs on T-series and M320 platforms: 1 through 50,000 microseconds. ■ For IQ PICs on other M-series platforms: 1 through 100,000 microseconds. <p>\$junos-scheduler-bx—JUNOS internal variable that is replaced with the buffer size obtained from the RADIUS server when a subscriber authenticates over the subscriber interface to which the subscriber access dynamic profile is attached.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Dynamic Variables Overview on page 276 ■ Configuring Schedulers in a Dynamic Profile on page 393 ■ scheduler

class-of-service

Syntax	class-of-service { ... }
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i>]
Release Information	Statement introduced before JUNOS Release 7.4. The [edit dynamic-profiles <i>profile-name</i>] hierarchy added in JUNOS Release 9.2.
Description	Configure JUNOS CoS features in a dynamic profile.
Default	If you do not configure any CoS features, all packets are transmitted from output transmission queue 0.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring Static Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 389

delay-buffer-rate

Syntax	delay-buffer-rate (percent <i>percentage</i> <i>rate</i> \$junos-cos-delay-buffer-rate);
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>]
Release Information	Statement introduced in JUNOS 7.6. The [edit dynamic-profiles <i>profile-name</i>] hierarchy added in JUNOS Release 9.2. The \$junos-cos-delay-buffer-rate variable added in JUNOS Release 9.4.
Description	For EQ DPC interfaces, base the delay-buffer calculation on a delay-buffer rate.
Default	If you do not include this statement, the delay-buffer calculation is based on the guaranteed rate if one is configured, or the shaping rate if no guaranteed rate is configured.
Options	<p>rate—For EQ DPC interfaces, delay-buffer rate, in bits per second (bps). You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).</p> <p>Range: 1000 through 160,000,000,000 bps</p> <p>\$junos-cos-delay-buffer-rate—JUNOS internal variable that is replaced with the delay-buffer rate obtained from the RADIUS server when a subscriber authenticates over the subscriber interface to which the subscriber access dynamic profile is attached.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Dynamic Variables Overview on page 276 ■ Configuring Traffic Shaping and Scheduling in a Dynamic Profile on page 392 ■ output-traffic-control-profile

drop-profile

Syntax	<code>drop-profile (<i>profile-name</i> <i>variable</i>);</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i> drop-profile-map loss-priority (any low medium-low medium-high high) protocol (any non-tcp tcp)]
Release Information	Statement introduced before JUNOS Release 7.4. The [edit dynamic-profiles <i>profile-name</i>] hierarchy added in JUNOS Release 9.3. The \$junos-cos-scheduler-dropfile-low, \$junos-cos-scheduler-dropfile-medium-low, \$junos-cos-scheduler-dropfile-medium-high, \$junos-cos-scheduler-dropfile-high, and \$junos-cos-scheduler-dropfile-any internal variable added in JUNOS Release 9.4.
Description	<p>Within the drop-profile map, specify the name of the drop profile to use for random early detection (RED) for a specific packet-loss priority (PLP) level and protocol type. A drop profile maps a fill level (fullness of a queue) to a drop probability (probability that a packet will be dropped). When a packet arrives, RED checks the queue fill level. If the fill level corresponds to a nonzero drop probability, the RED algorithm determines whether to drop the arriving packet.</p> <p>You enable RED by applying a drop profile to a scheduler.</p> <p>You configure drop profiles statically (at the [edit class-of-service drop-profiles] hierarchy level).</p>
Options	<p><i>profile-name</i>—Name of the drop profile.</p> <p><i>variable</i>—One of the following JUNOS internal variable that is replaced with a value obtained from the RADIUS server when a subscriber authenticates over the subscriber interface to which the subscriber access dynamic profile is attached:</p> <ul style="list-style-type: none"> ■ \$junos-cos-scheduler-dropfile-low—Name of the drop profile for PLP level low and protocol any, specified for a scheduler configured in a dynamic profile for subscriber access. ■ \$junos-cos-scheduler-dropfile-medium-low—Name of the drop profile for PLP level medium-low and protocol any, specified for a scheduler configured in a dynamic profile for subscriber access. ■ \$junos-cos-scheduler-dropfile-medium-high—Name of the drop profile for PLP level medium-high and protocol any, specified for a scheduler configured in a dynamic profile for subscriber access. ■ \$junos-cos-scheduler-dropfile-high—Name of the drop profile for PLP level high and protocol any, specified for a scheduler configured in a dynamic profile for subscriber access. ■ \$junos-cos-scheduler-dropfile-lny—Name of the drop profile for PLP level any and protocol any, specified for a scheduler configured in a dynamic profile for subscriber access.
Required Privilege Level	interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

- Related Topics**
- For more information about configuring drop profiles and drop-profile maps, see the *JUNOS Class of Service Configuration Guide* .
 - Dynamic Variables Overview on page 276
 - Configuring Schedulers in a Dynamic Profile on page 393
 - scheduler

drop-profile-map

Syntax drop-profile-map loss-priority (any | low | medium-low | medium-high | high) protocol (any | non-tcp | tcp) drop-profile (*profile-name* | *variable*);

Hierarchy Level [edit dynamic-profiles *profile-name* class-of-service schedulers *scheduler-name*]

Release Information Statement introduced before JUNOS Release 7.4.
The [edit dynamic-profiles *profile-name*] hierarchy added in JUNOS Release 9.3.
The \$junos-cos-scheduler-dropfile-low, \$junos-cos-scheduler-dropfile-medium-low, \$junos-cos-scheduler-dropfile-medium-high, \$junos-cos-scheduler-dropfile-high, and \$junos-cos-scheduler-dropfile-any internal variable added in JUNOS Release 9.4.

Description Define loss priority value for drop profile.

The statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

- Related Topics**
- Dynamic Variables Overview on page 276
 - Configuring Schedulers in a Dynamic Profile on page 393
 - scheduler

forwarding-class

Syntax	<code>forwarding-class <i>class-name</i>;</code>
Hierarchy Level	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service scheduler-maps <i>map-name</i>]</code>
Release Information	Statement introduced before JUNOS Release 7.4. The <code>[edit dynamic-profiles <i>profile-name</i>]</code> hierarchy added in JUNOS Release 9.3.
Description	Associate a scheduler with a scheduler map.
Options	<i>scheduler-name</i> —Name of the scheduler configuration block.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring Schedulers in a Dynamic Profile on page 393

guaranteed-rate

Syntax	<code>guaranteed-rate (percent <i>percentage</i> <i>rate</i> \$junos-cos-guaranteed-rate);</code>
Hierarchy Level	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>]</code>
Release Information	Statement introduced in JUNOS 7.6. The <code>[edit dynamic-profiles <i>profile-name</i>]</code> hierarchy added in JUNOS Release 9.2 The <code>\$junos-cos-guaranteed-rate</code> variable added in JUNOS Release 9.4.
Description	For EQ DPC interfaces only, configure a guaranteed minimum rate for a logical interface.
Default	If you do not include this statement and you do not include the <code>delay-buffer-rate</code> statement, the logical interface receives a minimal delay-buffer rate and minimal bandwidth equal to 2 MTU-sized packets.
Options	<p>rate—For EQ DPC interfaces, guaranteed rate, in bits per second (bps). You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).</p> <p>Range: 1000 through 160,000,000,000 bps</p> <p>\$junos-cos-guaranteed-rate—JUNOS internal variable that is replaced with the guaranteed rate obtained from the RADIUS server when a subscriber authenticates over the subscriber interface to which the subscriber access dynamic profile is attached.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Dynamic Variables Overview on page 276 ■ Configuring Traffic Shaping and Scheduling in a Dynamic Profile on page 392 ■ output-traffic-control-profile

interfaces

Syntax `interfaces {
 interface-name {
 }
 unit logical-unit-number {
 output-traffic-control-profile profile-name;
 }
 }`

Hierarchy Level [edit dynamic-profiles *profile-name* class-of-service]

Release Information Statement introduced before JUNOS Release 7.4.
 The [edit dynamic-profiles *profile-name*] hierarchy added in JUNOS Release 9.2.

Description Configure interface-specific CoS properties for incoming packets.

Options *interface-name*—Either the specific name of the interface you want to assign to the dynamic-profile or the interface variable (\$junos-interface-ifd-name). The interface variable is dynamically replaced with the interface the DHCP client accesses when connecting to the router.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Topics ■ Applying CoS to an Interface in a Dynamic Profile on page 400

loss-priority

Syntax	loss-priority (any low medium-low medium-high high);
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i> drop-profile-map]
Release Information	Statement introduced before JUNOS Release 7.4. The [edit dynamic-profiles <i>profile-name</i>] hierarchy added in JUNOS Release 9.3.
Description	Specify a loss priority to which to apply a drop profile in a dynamic profile. The drop profile map sets the drop profile for a specific PLP and protocol type. The inputs for the map are the PLP designation and the protocol type. The output is the drop profile.
Options	any—The drop profile applies to packets with any PLP. high—The drop profile applies to packets with high PLP. medium—The drop profile applies to packets with medium PLP. low—The drop profile applies to packets with low PLP.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring Schedulers in a Dynamic Profile on page 393

output-traffic-control-profile

Syntax	output-traffic-control-profile <i>profile-name</i> ;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> class-of-service interfaces <i>interface-name</i> <i>logical-unit-number</i>]
Release Information	Statement introduced in JUNOS Release 7.6. The [edit dynamic-profiles <i>profile-name</i>] hierarchy added in JUNOS Release 9.2.
Description	For EQ DPCs on MX-series routers, apply an output traffic scheduling and shaping profile to the logical interface.
Options	<i>profile-name</i> —Name of the traffic-control profile to be applied to this interface
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Applying CoS to an Interface in a Dynamic Profile on page 400 ■ traffic-control-profiles

priority

Syntax	<code>priority (<i>priority-level</i> \$junos-cos-scheduler-priority);</code>
Hierarchy Level	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>]</code>
Release Information	Statement introduced before JUNOS Release 7.4. The <code>[edit dynamic-profiles <i>profile-name</i>]</code> hierarchy added in JUNOS Release 9.3. The <code>\$junos-cos-scheduler-bs</code> internal variable added in JUNOS Release 9.4.
Description	Specify packet-scheduling priority value in a dynamic profile.
Options	<p><i>priority-level</i>—one of the following packet-scheduling priority values:</p> <ul style="list-style-type: none"> ■ <code>low</code>—Scheduler has low priority. ■ <code>medium-low</code>—Scheduler has medium-low priority. ■ <code>medium-high</code>—Scheduler has medium-high priority. ■ <code>high</code>—Scheduler has high priority. Assigning high priority to a queue prevents the queue from being underserved. ■ <code>strict-high</code>—Scheduler has strictly high priority. Configure a <code>high</code> priority queue with unlimited transmission bandwidth available to it. As long as it has traffic to send, the <code>strict-high</code> priority queue receives precedence over <code>low</code>, <code>medium-low</code>, and <code>medium-high</code> priority queues, but not <code>high</code> priority queues. You can configure <code>strict-high</code> priority on only one queue per interface. <p><code>\$junos-cos-scheduler-pri</code>—JUNOS internal variable that is replaced with the packet-scheduling priority value obtained from the RADIUS server when a subscriber authenticates over the subscriber interface to which the subscriber access dynamic profile is attached.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Dynamic Variables Overview on page 276 ■ Configuring Schedulers in a Dynamic Profile on page 393 ■ scheduler

protocol

Syntax	<code>protocol (any non-tcp tcp);</code>
Hierarchy Level	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i> drop-profile-map]</code>
Release Information	Statement introduced before JUNOS Release 7.4. The <code>[edit dynamic-profiles <i>profile-name</i>]</code> hierarchy added in JUNOS Release 9.3.
Description	Specify the protocol type for the specified scheduler in a dynamic profile.
Options	<p><code>any</code>—Accept any protocol type.</p> <p><code>non-tcp</code>—Accept any protocol type other than TCP/IP.</p> <p><code>tcp</code>—Accept only TCP/IP protocol.</p>



NOTE: Protocol types `non-tcp` and `tcp` are not supported on MX-series routers.

Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Configuring Schedulers in a Dynamic Profile on page 393

scheduler

Syntax	<code>scheduler <i>scheduler-name</i>;</code>
Hierarchy Level	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service scheduler-maps <i>map-name</i>]</code>
Release Information	Statement introduced before JUNOS Release 7.4. The <code>[edit dynamic-profiles <i>profile-name</i>]</code> hierarchy added in JUNOS Release 9.2.
Description	Associate a scheduler with a scheduler map in a dynamic profile.
Options	<code><i>scheduler-name</i></code> —Name of the scheduler configuration block.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	<ul style="list-style-type: none"> ■ Configuring Schedulers in a Dynamic Profile on page 393

scheduler-map

Syntax	<code>scheduler-map (<i>map-name</i> \$junos-cos-scheduler-map);</code>
Hierarchy Level	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>]</code>
Release Information	Statement introduced before JUNOS Release 7.4. The <code>[edit dynamic-profiles <i>profile-name</i>]</code> hierarchy added in JUNOS Release 9.3. The <code>\$junos-cos-scheduler-map</code> variable added in JUNOS Release 9.4.
Description	For EQ DPC interfaces only, associate a scheduler map name with a traffic-control profile in a dynamic profile. The scheduler map can be defined dynamically (at the <code>[edit dynamic-profiles <i>profile-name</i> class-of-service scheduler-maps]</code> hierarchy level) or statically (at the <code>[edit class-of-service scheduler-maps]</code> hierarchy level).
Options	<i>map-name</i> —Name of the scheduler map. \$junos-cos-scheduler-map—JUNOS internal variable that is replaced with the scheduler-map name obtained from the RADIUS server when a subscriber authenticates over the subscriber interface to which the subscriber access dynamic profile is attached.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Dynamic Variables Overview on page 276 ■ Configuring Traffic Shaping and Scheduling in a Dynamic Profile on page 392 ■ output-traffic-control-profile

scheduler-maps

Syntax scheduler-maps {
 map-name {
 forwarding-class *class-name* scheduler *scheduler-name*;
 }
 }

Hierarchy Level [edit dynamic-profiles *profile-name* class-of-service]

Release Information Statement introduced before JUNOS Release 7.4.
 The [edit dynamic-profiles *profile-name*] hierarchy added in JUNOS Release 9.3.

Description Specify a scheduler map name in a dynamic profile and associate it with the scheduler configuration and forwarding class.

Options *map-name*—Name of the scheduler map.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Topics ■ [Configuring Schedulers in a Dynamic Profile on page 393](#)

schedulers

Syntax schedulers {
 (*scheduler-name* | \$junos-cos-scheduler) {
 buffer-size (*seconds* | percent *percentage* | remainder | temporal *microseconds*);
 drop-profile-map loss-priority (any | low | medium-low | medium-high | high) protocol
 (any | non-tcp | tcp) drop-profile *profile-name*;
 priority *priority-level*;
 transmit-rate (percent *percentage* | *rate* | remainder) <exact | rate-limit>;
 }
 }

Hierarchy Level [edit dynamic-profiles *profile-name* class-of-service]

Release Information Statement introduced before JUNOS Release 7.4.
 The [edit dynamic-profiles *profile-name*] hierarchy added in JUNOS Release 9.3.
 The \$junos-cos-scheduler internal variable added in JUNOS Release 9.4.

Description Specify scheduler name and parameter values in a dynamic profile.

Options *scheduler-name*—Name of the scheduler to be configured.

\$junos-cos-scheduler—JUNOS internal variable that is replaced with the scheduler name obtained from the RADIUS server when a subscriber authenticates over the subscriber interface to which the subscriber access dynamic profile is attached.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Topics

- Dynamic Variables Overview on page 276
- Configuring Schedulers in a Dynamic Profile on page 393
- scheduler

shaping-rate

Syntax	shaping-rate (percent <i>percentage</i> <i>rate</i> \$junos-cos-shaping-rate);
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>] [edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>]
Release Information	Statement introduced in JUNOS Release 7.6. The [edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>] hierarchy added in JUNOS Release 9.2. The \$junos-cos-shaping-rate variable added in JUNOS Release 9.4.
Description	For EQ DPC interfaces only, configure a shaping rate for a logical interface. The sum of the shaping rates for all logical interfaces on the physical interface can exceed the physical interface bandwidth. This practice is known as oversubscription of the peak information rate (PIR).
Default	The default behavior depends on various factors.
Options	<p>rate—For EQ DPC interfaces, peak rate, in bits per second (bps). You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000).</p> <p>Range: 1000 through 160,000,000,000 bps</p> <p>\$junos-cos-shaping-rate—JUNOS internal variable that is replaced with the shaping rate obtained from the RADIUS server when a subscriber authenticates over the subscriber interface to which the subscriber access dynamic profile is attached.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Dynamic Variables Overview on page 276 ■ Configuring Traffic Shaping and Scheduling in a Dynamic Profile on page 392 ■ output-traffic-control-profile

traffic-control-profiles

Syntax traffic-control-profiles *profile-name* {
 delay-buffer-rate (percent *percentage* | *rate*);
 guaranteed-rate (percent *percentage* | *rate*);
 scheduler-map *map-name*;
 shaping-rate (percent *percentage* | *rate*);
 }

Hierarchy Level [edit dynamic-profiles *profile-name* class-of-service]

Release Information Statement introduced in JUNOS Release 7.6.
 The [edit dynamic-profiles *profile-name*] hierarchy added in JUNOS Release 9.2.

Description For EQ DPC interfaces only, configure traffic shaping and scheduling profiles.

Options *profile-name*—Name of the traffic-control profile.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Topics

- Configuring Traffic Shaping and Scheduling in a Dynamic Profile on page 392
- output-traffic-control-profile

transmit-rate

Syntax	transmit-rate (<i>rate</i> percent <i>percentage</i> remainder \$junos-cos-scheduler-tx) <exact rate-limit>;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>]
Release Information	Statement introduced before JUNOS Release 7.4. rate-limit option introduced in JUNOS Release 8.3. The [edit dynamic-profiles <i>profile-name</i>] hierarchy added in JUNOS Release 9.3. The \$junos-cos-scheduler-tx internal variable added in JUNOS Release 9.4.
Description	Specify the transmit rate or percentage for a scheduler in a dynamic profile.
Default	If you do not include this statement, the default scheduler transmission rate and buffer size percentages for queues 0 through 7 are 95, 0, 0, 5, 0, 0, 0, and 0 percent.
Options	<p><i>rate</i>—Transmission rate, in bps. You can specify a value in bits per second either as a complete decimal number or as a decimal number followed by the abbreviation k (1000), m (1,000,000), or g (1,000,000,000). Range: 3200 through 160,000,000,000 bps</p> <p>percent <i>percentage</i>—Percentage of transmission capacity. A percentage of zero drops all packets in the queue. Range: 0 through 100 percent</p> <p>remainder—Use remaining rate available.</p> <p>\$junos-cos-scheduler-tx—JUNOS internal variable that is replaced with the transmission rate obtained from the RADIUS server when a subscriber authenticates over the subscriber interface to which the subscriber access dynamic profile is attached</p> <p>exact—(Optional) Enforce the exact transmission rate. Under sustained congestion, a rate-controlled queue that goes into negative credit fills up and eventually drops packets. Make sure this value never exceeds the rate-controlled amount.</p> <p>rate-limit—(Optional) Limit the transmission rate to the rate-controlled amount during congestion. In contrast to the exact option, when there is no congestion, the scheduler with the rate-limit option shares unused bandwidth above the rate-controlled amount.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Dynamic Variables Overview on page 276 ■ Configuring Schedulers in a Dynamic Profile on page 393 ■ scheduler

unit

Syntax unit *logical-unit-number* {
 output-traffic-control-profile *profile-name* ;
 }

Hierarchy Level [edit dynamic-profiles *profile-name* class-of-service interfaces *interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.
 The [edit dynamic-profiles *profile-name*] hierarchy added in JUNOS Release 9.2.

Description Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

Options *logical-unit-number*—Either the specific unit number of the interface you want to assign to the dynamic-profile or the static unit number variable (\$junos-underlying-interface-unit). The static unit number variable is dynamically replaced with the client unit number when the client session begins. The client unit number is specified by the DHCP client when it accesses the subscriber network.

Range: 0 through 16,384

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Topics ■ Applying CoS to an Interface in a Dynamic Profile on page 400

Part 8

Dynamic Protocols for Subscriber Access

- Dynamic Protocol Configuration Overview on page 451
- Summary of IGMP Dynamic Profile Statements on page 453
- ANCP Overview on page 465
- Configuring ANCP on page 467
- Summary of ANCP Statements on page 475

Chapter 34

Dynamic Protocol Configuration Overview

- Dynamic IGMP Configuration Overview on page 451

Dynamic IGMP Configuration Overview

The Internet Group Management Protocol (IGMP) is a host to router signaling protocol for IPv4 used to support IP multicasting. This protocol manages the membership of hosts and routers in multicast groups. IP hosts use IGMP to report their multicast group memberships to any immediately neighboring multicast routers. Multicast routers use IGMP to learn, for each of their attached physical networks, which groups have members.

Subscriber access supports the configuration of IGMP within the **dynamic profiles** hierarchy. By specifying IGMP statements within a dynamic profile, you can dynamically apply IGMP configuration when a subscriber connects to an interface using a particular access technology (DHCP), enabling the subscriber to access a carrier (multicast) network.

- Related Topics**
- Dynamic Profiles Overview on page 275
 - Configuring a Dynamic Profile for Client Access on page 287
 - For general information about configuring IGMP, see the *JUNOS Multicast Protocols Configuration Guide*

Chapter 35

Summary of IGMP Dynamic Profile Statements

accounting

Syntax	accounting;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in JUNOS Release 8.5. The [edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>] hierarchy added in JUNOS Release 9.2.
Description	Enable the collection of IGMP join and leave event statistics on a per-interface basis.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none">■ Configuring a Dynamic Profile for Client Access on page 287■ For information about recording IGMP join and leave events, see “Recording IGMP Join and Leave Events” in the <i>JUNOS Multicast Protocols Configuration Guide</i>

disable

Syntax "disable:\$junos-igmp-enable";

Hierarchy Level [edit dynamic-profiles *profile-name* protocols igmp interface *interface-name*],
[edit logical-systems *logical-system-name* protocols igmp interface *interface-name*],
[edit protocols igmp interface *interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.
The [edit dynamic-profiles *profile-name* protocols igmp interface *interface-name*] hierarchy added in JUNOS Release 9.2.

Description Disable IGMP on the interface.



NOTE: Though the purpose of this statement is to disable IGMP on interfaces, under the **dynamic-profiles** hierarchy you can use this statement and an enable variable (**disable:\$junos-igmp-enable**) to ensure that IGMP is not disabled by a AAA-based authentication and management method (RADIUS).

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics

- Configuring a Dynamic Profile for Client Access on page 287
- For information about disabling IGMP, see “Disabling IGMP” in the *JUNOS Multicast Protocols Configuration Guide*

group

Syntax For group configuration with a source, use the following syntax:

```
group ip-address {
    source ip-address;
}
```

For group configuration without a source, use the following syntax:

```
group group;
```

Hierarchy Level [edit dynamic-profiles *profile-name* protocols igmp interface *interface-name* static],
[edit logical-systems *logical-system-name* protocols igmp interface *interface-name* static],
[edit protocols igmp interface *interface-name* static]

Release Information Statement introduced before JUNOS Release 7.4.
The [edit dynamic-profiles *profile-name* protocols igmp interface *interface-name* static] hierarchy added in JUNOS Release 9.2.

Description When configuring with a source address, configure the IGMP multicast group address that receives data on an interface and a source address for certain packets. For configuration without a source address, configure only the IGMP multicast group address that receives data on an interface.

Options *ip-address*—Group IP address.

group—Name of group.



NOTE: You must specify a unique address for each group.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics

- Configuring a Dynamic Profile for Client Access on page 287
- For information about configuring static group membership, see “Enabling IGMP Static Group Membership” in the *JUNOS Multicast Protocols Configuration Guide*

group-policy

Syntax	<code>group-policy <i>policy-name</i>;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmpinterface <i>interface-name</i>]
Release Information	Statement introduced in JUNOS Release 9.1. The [edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>] hierarchy added in JUNOS Release 9.2.
Description	<p>When this statement is enabled on a router running IGMP version 2 (IGMPv2), after the router receives an IGMP report, compare the group against the specified group policy and performs the action configured in that policy (for example, rejects the report).</p> <p>When this statement is enabled on a router running IGMP version 3 (IGMPv3), after the router receives an IGMP report, compare the group against the specified group policy and performs the action configured in that policy (for example, rejects the report).</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring a Dynamic Profile for Client Access on page 287 ■ For information about rejecting unwanted reports for an IGMP interface, see “Filtering Unwanted IGMP Reports at the IGMP Interface Level” in the <i>JUNOS Multicast Protocols Configuration Guide</i>

igmp

Syntax	<pre> igmp { interface <i>interface-name</i> { accounting; disable; group-policy; immediate-leave; no-accounting; promiscuous-mode; ssm-map <i>ssm-map-name</i>; static { group <i>group</i> { source <i>source</i>; } } version <i>version</i>; } } </pre>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols], [edit logical-systems <i>logical-system-name</i> protocols], [edit protocols]
Release Information	Statement introduced before JUNOS Release 7.4. The [edit dynamic-profiles <i>profile-name</i> protocols] hierarchy added in JUNOS Release 9.2.
Description	Enable IGMP on the router. IGMP must be enabled for the router to receive multicast packets.
Default	IGMP is disabled on the router. IGMP is automatically enabled on all broadcast interfaces when you configure Protocol Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP).
Options	The statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring a Dynamic Profile for Client Access on page 287 ■ For general information about configuring IGMP, see the <i>JUNOS Multicast Protocols Configuration Guide</i> ■ For information about enabling IGMP, see “Enabling IGMP” in the <i>JUNOS Multicast Protocols Configuration Guide</i>

immediate-leave

Syntax	<code>immediate-leave;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in JUNOS Release 8.3. The [edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>] hierarchy added in JUNOS Release 9.2.
Description	Immediately remove the group membership from the interface and suppresses the sending of any group-specific queries for the multicast group when this statement is enabled on a router running IGMP version 2 (IGMPv2), after the router receives a leave group membership message from a host associated with the interface. Suppress the sending of group-and-source queries but rely on the JUNOS-supported host tracking mechanism to determine whether or not it should remove a particular source group membership from the interface when this statement is enabled on a router running IGMP version 3 (IGMPv3), after the router receives a report with the type BLOCK_OLD_SOURCES.



NOTE: When issuing this command on IGMPv2 interfaces, ensure that the IGMP interface has only one IGMP host connected. If more than one IGMPv2 host is connected to a LAN through the same interface, and one host sends a done message, the router removes all hosts on the interface from the multicast group. The router loses contact with the hosts that are supposed to remain in the multicast group until they send join requests in response to the next general multicast listener query from the router.

Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring a Dynamic Profile for Client Access on page 287 ■ For information about configuring IGMP immediate leave, see “Specifying Immediate-Leave Host Removal” in the <i>JUNOS Multicast Protocols Configuration Guide</i>

interface

Syntax	<pre> interface <i>interface-name</i> { accounting; disable; group-policy; immediate-leave no-accounting; promiscuous-mode; ssm-map <i>ssm-map-name</i>; static { group <i>group</i> { source <i>source</i>; } } version <i>version</i>; } </pre>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp], [edit logical-systems <i>logical-system-name</i> protocols igmp], [edit protocols igmp]
Release Information	Statement introduced before JUNOS Release 7.4. The [edit dynamic-profiles <i>profile-name</i> protocols igmp] hierarchy added in JUNOS Release 9.2.
Description	Enable IGMP on an interface and configure interface-specific properties.
Options	<p><i>interface-name</i>—Variable for the interface. Specify the interface variable (\$junos-underlying-interface) to indicate that the dynamic profile chooses an interface for the accessing DHCP client.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring a Dynamic Profile for Client Access on page 287 ■ For information about configuring IGMP interfaces, see “Enabling IGMP” in the <i>JUNOS Multicast Protocols Configuration Guide</i>

no-accounting

Syntax	no-accounting;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in JUNOS Release 8.5. The [edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>] hierarchy added in JUNOS Release 9.2.
Description	Disable the collection of IGMP join and leave event statistics on a per-interface basis.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring a Dynamic Profile for Client Access on page 287 ■ For information about disabling IGMP accounting on an interface, see “Enabling or Disabling IGMP Accounting on Individual Interfaces” in the <i>JUNOS Multicast Protocols Configuration Guide</i>

promiscuous-mode

Syntax	promiscuous-mode;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in JUNOS Release 8.3. The [edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>] hierarchy added in JUNOS Release 9.2.
Description	Specify that the interface accepts IGMP reports from hosts on any subnetwork.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring a Dynamic Profile for Client Access on page 287 ■ For information about how to use IGMP promiscuous mode, see “Accepting IGMP Messages from Remote Subnetworks” in the <i>JUNOS Multicast Protocols Configuration Guide</i>

protocols

Syntax

```
protocols {
  igmp {
    interface interface-name {
      accounting;
      disable;
      group-policy;
      immediate-leave;
      no-accounting;
      promiscuous-mode;
      ssm-map ssm-map-name;
      static {
        group group {
          source source;
        }
      }
      version version;
    }
  }
}
```

Hierarchy Level [edit dynamic-profiles protocols],
[edit logical-systems *logical-system-name* protocols],
[edit protocols]

Release Information Statement introduced before JUNOS Release 7.4.
Statement supported in the [edit dynamic-profiles] hierarchy in JUNOS Release 9.2.

Description Enable IGMP on the router. IGMP must be enabled for the router to receive multicast packets.

Default IGMP is disabled on the router. IGMP is automatically enabled on all broadcast interfaces when you configure Protocol Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP).

Options The statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Topics ■ For general information about configuring IGMP, see the *JUNOS Multicast Protocols Configuration Guide*, Part 3, “IGMP”

source

Syntax	<code>source <i>source</i>;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i> static], [edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i> static], [edit protocols igmp interface <i>interface-name</i> static]
Release Information	Statement introduced before JUNOS Release 7.4. The [edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i> static] hierarchy added in JUNOS Release 9.2.
Description	Specify the IP version 4 (IPv4) unicast address to send data on an interface.
Options	<i>source</i> —IPv4 unicast address.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring a Dynamic Profile for Client Access on page 287 ■ For information about defining an IGMP source, see “Enabling IGMP Static Group Membership” in the <i>JUNOS Multicast Protocols Configuration Guide</i>

ssm-map

Syntax	<code>ssm-map <i>ssm-map-name</i>;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced in JUNOS Release 7.4. The [edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>] hierarchy added in JUNOS Release 9.2.
Description	Apply an SSM map to an IGMP interface.
Options	<i>ssm-map-name</i> —Name of SSM map.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring a Dynamic Profile for Client Access on page 287 ■ For information about configuring SSM maps, see “Source-Specific Multicast Groups Overview” in the <i>JUNOS Multicast Protocols Configuration Guide</i>

static

Syntax static {
 group *group*;
 group *group* {
 source *source*;
 }
 }

Hierarchy Level [edit dynamic-profiles *profile-name* protocols igmp interface *interface-name*],
 [edit logical-systems *logical-system-name* protocols igmp interface *interface-name*],
 [edit protocols igmp interface *interface-name*]

Release Information Statement introduced before JUNOS Release 7.4.
 The [edit dynamic-profiles *profile-name* protocols igmp interface *interface-name*] hierarchy added in JUNOS Release 9.2.

Description Test multicast forwarding on an interface without a receiver host.

Options The remaining statements are explained separately.

Required Privilege Level routing and trace—To view this statement in the configuration.
 routing-control and trace-control—To add this statement to the configuration.

Related Topics ■ Configuring a Dynamic Profile for Client Access on page 287
 ■ For information about testing multicast forwarding without a receiver host, see “Enabling IGMP Static Group Membership” in the *JUNOS Multicast Protocols Configuration Guide*

version

Syntax	<code>version <i>version</i>;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols igmpinterface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> protocols igmp interface <i>interface-name</i>], [edit protocols igmp interface <i>interface-name</i>]
Release Information	Statement introduced before JUNOS Release 7.4. The [edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>] hierarchy added in JUNOS Release 9.2.
Description	Specify the version of IGMP.
Options	<i>version</i> —IGMP version number. Range: 1, 2, or 3 Default: IGMP version 2



NOTE: Routers running different versions of IGMP negotiate the lowest common version of IGMP that is supported by hosts on their subnet and operate in that version.

If you have already configured the router to use IGMP version 1 and then configure it to use IGMP version 2, the router continues to use IGMP version 1 for up to 6 minutes and then uses IGMP version 2.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

- Related Topics**
- Configuring a Dynamic Profile for Client Access on page 287
 - For information about specifying a different IGMP version, see “Changing the IGMP Version” in the *JUNOS Multicast Protocols Configuration Guide*

Chapter 36

ANCP Overview

- ANCP Topology Discovery and Traffic Monitoring Overview on page 465

ANCP Topology Discovery and Traffic Monitoring Overview

This topic describes ANCP as a means to monitor and modify subscriber traffic in the access network.

Access Node Control Protocol (ANCP) acts as a control plane between a service-oriented Layer 3 edge device and a Layer 2 access node. Queuing and scheduling mechanisms for subscriber traffic must avoid congestion within the access network while contending with multiple flows and distinct CoS requirements. These mechanisms require the edge device—a network access server (NAS)—to provide information about the access network and subscriber traffic.

The NAS uses topology discovery to get this information from the access node, typically a DSL access multiplexer (DSLAM). The information includes:

- Topology of the access network
- DSL line state
- Actual upstream and downstream net data rates of a synchronized DSL link
- Maximum attainable upstream and downstream net data rates
- Interleaving delay

The NAS receives the service profile for the subscribers from a RADIUS server. Most of the services are enforced by the NAS itself. The NAS shapes the aggregate egress traffic to subscribers based on the local loop throughput reported by the DSLAM. This traffic shaping optimizes traffic flow while avoiding traffic drops in the access node.

Some service attributes, such as interleaving delay and multicast channel information, are enforced at the access node. ANCP provides the line configuration mechanism that the edge device can use to pass the line configuration on to the access nodes. Typically multiple profiles are provisioned on the access node. The NAS instructs the access node which profile to use for a given subscriber.

Subscribers typically receive some combination of voice, data, and video services. Each service can be provisioned on a VLAN. The group of VLANs carrying services to a subscriber is the *interface set*. Subscribers are identified based on the unique

access identifier that is configured on the access node through which they receive traffic. You must configure this access identifier to associate it with an interface set. When ANCP receives a port management message from an access node, it uses the access identifier contained in the message to determine which interface set corresponds to the subscriber. You can configure the interface-sets by including the **interface-set** statement at the **[edit protocols ancp interfaces]** hierarchy level. Associate the access-identifier with the interface set by including the **access-identifier** statement at the **[edit protocols ancp interfaces interface-sets *interface-set-name*]** hierarchy level.

ANCP communicates to CoS the shaping rate that CoS must apply to a particular set of VLANs to avoid traffic drops in the access node. ANCP can affect only the shaping rate. When ANCP removes a shaping rate it previously applied, then the traffic shaping rate reverts to that configured in the CLI.

ANCP sends a keepalive message to CoS at specific intervals. If CoS does not receive a keepalive in the expected time, it reverts the shaping rate changes it made in response to ANCP. You can adjust how long CoS waits for a keepalive message by including the **maximum-helper-restart-time** statement at the **[edit protocols ancp]** hierarchy level. The interval between keepalive messages is automatically set to one-third the value of the maximum helper restart time. For example, if you set the maximum helper restart time to 120 seconds, then ANCP sends keepalive messages every 40 seconds. In this example, if CoS does not receive a keepalive message within 120 seconds, then it reverts the ANCP-derived policy changes.

ANCP can monitor and shape traffic only for access nodes that are configured as ANCP neighbors. Neighbors can establish TCP connections with the NAS. You can configure an access node as an ANCP neighbor by including the **neighbor** statement at the **[edit protocols ancp]** hierarchy level.

ANCP exchanges adjacency messages with neighbors. If an adjacency message is not received from a neighbor within the expected period, then the neighbor is considered to be down and is disconnected. You can adjust how long ANCP waits for an adjacency message by including the **adjacency-timer** statement at the **[edit protocols ancp]** hierarchy level. The interval between adjacency messages is automatically set to one-third the value of the adjacency timer.

- Related Topics**
- Configuring ANCP on page 467
 - [edit-protocols ancp] Hierarchy Level on page 496

Chapter 37

Configuring ANCP

- Configuring ANCP on page 467
- Configuring ANCP Neighbors on page 468
- Tracing ANCP Operations on page 468
- Associating an Access Node with Subscribers for ANCP Operations on page 471
- Specifying the Interval Between ANCP Adjacency Messages on page 472
- Specifying How Long Processes Wait for ANCP Restart to Complete on page 472
- Configuring ANCP for Backwards Compatibility on page 473
- Configuring ANCP to Adjust CoS Traffic Shaping on page 473

Configuring ANCP

You can configure ANCP to enable a service-oriented Layer 3 edge device to discover information about the topology of a connected access network. ANCP can also provide details about subscriber traffic and enable the adjustment of QoS traffic shaping for subscribers.

To configure ANCP:

1. Configure trace options for troubleshooting the configuration.

See “Tracing ANCP Operations” on page 468.
2. Specify each ANCP neighboring access node to be monitored.

See “Configuring ANCP Neighbors” on page 468.
3. Specify the subscribers reached by multiple VLANs through a particular access node.

See “Associating an Access Node with Subscribers for ANCP Operations” on page 471.
4. Configure the adjacency timer.

See “Specifying the Interval Between ANCP Adjacency Messages” on page 472.
5. Configure the graceful restart timer.

See “Specifying How Long Processes Wait for ANCP Restart to Complete” on page 472.

6. Configure ANCP to work with an early IETF draft.

See “Configuring ANCP for Backwards Compatibility” on page 473.

7. Configure ANCP to adjust QoS subscriber traffic shaping.

See “Configuring ANCP to Adjust CoS Traffic Shaping” on page 473.

Configuring ANCP Neighbors

You must configure each neighboring access node that you want ANCP to monitor and potentially shape traffic for.

To configure an ANCP neighbor:

- Specify the IP address of the neighbor.

```
[edit protocols ancp]
user@host# set neighbor 10.2.3.4
```

- Related Topics**
- Configuring ANCP on page 467
 - neighbor

Tracing ANCP Operations

ANCP supports tracing operations. ANCP tracing operations track ANCP operations and record them in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

1. Important events are logged in a file called **ancpd** located in the **/var/log** directory. You cannot change the directory (**/var/log**) in which trace files are located.
2. When the file **ancpd** reaches 128 kilobytes (KB), it is renamed **ancpd.0**, then **ancpd.1**, and so on, until there are three trace files. Then the oldest trace file (**ancpd.2**) is overwritten.

You can optionally configure the maximum file size to be from 10 KB through 1 gigabyte (GB). You can also specify the number of trace files to be from 2 through 1000. (For more information about how log files are created, see the *JUNOS System Log Messages Reference*.)

Log files can be accessed only by the user who configures the tracing operation.

To configure ANCP tracing operations:

1. Specify that you want to configure tracing options.


```
[edit protocols ancp]
user@host# edit traceoptions
```

2. (Optional) Configure the name for the file used for the trace output.

See “Configuring the ANCP Trace Log Filename” on page 469.

3. (Optional) Configure the number and size of the log files.

See “Configuring the Number and Size of ANCP Log Files” on page 469.

4. (Optional) Configure access to the log file.

See “Configuring Access to the ANCP Log File” on page 470.

5. (Optional) Configure a regular expression to filter logging events.

See “Configuring a Regular Expression for ANCP Lines to Be Logged” on page 470.

6. (Optional) Configure flags to filter the operations to be logged.

See “Configuring the ANCP Tracing Flags” on page 471.

The ANCP traceoptions operations are described in the following sections:

- Configuring the ANCP Trace Log Filename on page 469
- Configuring the Number and Size of ANCP Log Files on page 469
- Configuring Access to the ANCP Log File on page 470
- Configuring a Regular Expression for ANCP Lines to Be Logged on page 470
- Configuring the ANCP Tracing Flags on page 471

Configuring the ANCP Trace Log Filename

By default, the name of the file that records trace output for ANCP is `ancpd`. You can specify a different name with the `file` option.

To configure the filename for ANCP tracing operations:

- Specify the name of the file used for the trace output.

```
[edit protocols ancp traceoptions]
user@host# set file ancp_1
```

Configuring the Number and Size of ANCP Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed `filename.0`, then `filename.1`, and so on, until there are three trace files. Then the oldest trace file (`filename.2`) is overwritten.

You can optionally configure the maximum file size to be from 10 KB through 1 gigabyte (GB). You can also specify the number of trace files to be from 2 through 1000.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (*filename*) reaches 2 MB, *filename* is renamed *filename.0*, and a new file called *filename* is created. When the new *filename* reaches 2 MB, *filename.0* is renamed *filename.1* and *filename* is renamed *filename.0*. This process repeats until there are 20 trace files. Then the oldest file (*filename.19*) is overwritten by the newest file (*filename.0*).

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output. (DHCP local server and DHCP relay agent both support the **files** and **size** options for the **traceoptions** statement.)

```
[edit protocols ancp traceoptions]
user@host# set file ancp_1_logfile_1 files 20 size 2097152
```

Configuring Access to the ANCP Log File

By default, log files can be accessed only by the user who configures the tracing operation. You can enable all users to read the log file and you can explicitly set the default behavior of the log file.

To specify that all users can read the log file:

- Configure the log file to be world-readable.

```
[edit protocols ancp traceoptions]
user@host# set file ancp_1_logfile_1 world-readable
```

To explicitly set the default behavior, in which the log file can only be read by the user who configured tracing:

- Configure the log file to be no-world-readable.

```
[edit protocols ancp traceoptions]
user@host# set file ancp_1_logfile_1 no-world-readable
```

Configuring a Regular Expression for ANCP Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events.

You can refine the output by including regular expressions that will be matched.

To configure regular expressions to be matched:

- Configure the regular expression.

```
[edit protocols ancp traceoptions]
user@host# set file ancp_1_logfile_1 match regex
```


Configuring the ANCP Tracing Flags

By default, only important events are logged. You can specify which trace operations are logged by including specific tracing flags. The following table describes the flags that you can include.

Flag	Description
all	Trace all operations
config	Trace configuration events
cos	Trace class-of-service events
general	Trace general flow.
packet	Trace ANCP packet transmit and receive events
process	Trace process internal events
protocol	Trace protocol operations
restart	Trace process restart flow
routing-socket	Trace routing socket events
session	Trace connection events and sessions
startup	Trace ANCP startup events and flow
subscriber	Trace subscriber events
timer	Trace timer processing

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit protocols ancp traceoptions]
user@host# set flag restart
```

Associating an Access Node with Subscribers for ANCP Operations

Subscribers are identified by a system-wide unique access loop identifier that is associated with a named set of VLANs through which traffic is sent to the subscribers.

To configure the set of VLANs for subscribers and associate an access node with the subscribers:

- Specify the set name and the unique access-loop identifier for the access node.

```
[edit protocols ancp interfaces]
user@host# set interface-set vlan5 access-identifier "dslam port 2/3"
```


- Related Topics**
- Configuring ANCP on page 467
 - access-identifier
 - interface-set

Specifying the Interval Between ANCP Adjacency Messages

You can specify the interval between adjacency messages that are sent to ANCP adjacency peers.

To configure the interval between ANCP adjacency messages:

- Specify the time in seconds.
- ```
[edit protocols ancp]
user@host# set adjacency-timer 20
```

- Related Topics**
- Configuring ANCP on page 467
  - adjacency-timer

## Specifying How Long Processes Wait for ANCP Restart to Complete

---

You can specify how long other processes wait for ANCP to restart. If ANCP goes down and does not restore its sessions with the peer DSLAMs within the specified interval, the CoS updates implemented as a result of ANCP are reverted to the configured values. Consequently, traffic to the subscribers is not effectively shaped, resulting in traffic drops in the DSLAMs. When ANCP subsequently comes back and restores its sessions, updates are sent to shape subscriber traffic.

If instead the connection to a peer DSLAMs is lost and not restored within the specified interval while ANCP is still running, the CoS updates implemented as a result of ANCP are maintained. The shaping rate changes only if the connection comes back up and ANCP subsequently sends updates to shape subscriber traffic on the peer.

To configure the interval between ANCP adjacency messages:

- Specify the time in seconds.
- ```
[edit protocols ancp]
user@host# set maximum-helper-restart-time 150
```

- Related Topics**
- Configuring ANCP on page 467
 - maximum-helper-restart-time

Configuring ANCP for Backwards Compatibility

You can configure ANCP to operate in a mode compatible with the protocol as it was initially proposed to operate. This pre-ietf mode is compatible with *draft-wadhwa-gsmp-l2control-configuration-00.txt*, *GSMP extensions for layer2 control (L2C)*. Setting this backwards-compatible mode enables interoperation with devices that are not compatible with the current IETF ANCP draft, *draft-ietf-ancp-protocol-02.txt*, *Protocol for Access Node Control Mechanism in Broadband Networks*.

To configure ANCP to operate in a backwards-compatible mode:

- Specify the pre-ietf mode.

```
[edit protocols ancpl]
user@host# set pre-ietf mode
```

- Related Topics**
- Configuring ANCP on page 467
 - pre-ietf-mode

Configuring ANCP to Adjust CoS Traffic Shaping

You can specify that CoS policy for interface sets (subscriber VLANs) are adjusted based on information received from the access network in ANCP messages. Adding or removing this statement updates CoS shaping rate adjustments accordingly for all the subscribers in the network.

To configure CoS adjustment for subscriber traffic based on ANCP messages:

- Specify CoS adjustment.

```
[edit protocols ancpl]
user@host# set qos-adjust
```

- Related Topics**
- Configuring ANCP on page 467
 - CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview on page 414
 - Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 415
 - Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 417
 - Disabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 423
 - qos-adjust

Chapter 38

Summary of ANCP Statements

ancp

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

Hierarchy Level [edit services]

Release Information Statement introduced in JUNOS Release 9.4.

Description Configure JUNOS ANCP features.

The remaining statements are described separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Topics ■ Configuring ANCP on page 467

access-identifier

Syntax	access-identifier <i>identifier-string</i> ;
Hierarchy Level	[edit protocols ancp interfaces interface-set]
Release Information	Statement introduced in JUNOS Release 9.4.
Description	Associate the specified access node with the set of VLANs that carry traffic to the subscriber using that access node; identify a particular subscriber.
Options	<i>identifier-string</i> —Unique identifier string for the access node; also configured on the access node.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Associating an Access Node with Subscribers for ANCP Operations on page 471

adjacency-timer

Syntax	adjacency-timer <i>seconds</i> ;
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in JUNOS Release 9.4.
Description	Specify the interval between adjacency messages sent to ANCP adjacency peer (access node).
Options	<i>seconds</i> —Number of seconds between adjacency messages. Range: 1 through 25 seconds Default: 10 seconds
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Specifying the Interval Between ANCP Adjacency Messages on page 472

interfaces

Syntax	<pre> interfaces { interface-set <i>interface-set-name</i> { access-identifier <i>identifier-string</i>; } }</pre>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in JUNOS Release 9.4.
Description	<p>Identify the subscribers whose traffic is monitored and shaped by ANCP.</p> <p>The remaining statements are described separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	■ Associating an Access Node with Subscribers for ANCP Operations on page 471

interface-set

Syntax	<pre> interface-set <i>interface-set-name</i> { access-identifier <i>identifier-string</i>; } </pre>
Hierarchy Level	[edit protocols ancp interfaces]
Release Information	Statement introduced in JUNOS Release 9.4.
Description	Identify a group of VLANs on which traffic is sent to a subscriber identified by the access identifier.
Options	<p><i>interface-set-name</i>—Name of a group of VLANs that carry traffic to the subscriber identified by the access node identifier.</p> <p>The remaining statement is described separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Topics	■ Associating an Access Node with Subscribers for ANCP Operations on page 471

maximum-helper-restart-time

Syntax	maximum-helper-restart-time <i>seconds</i>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in JUNOS Release 9.4.
Description	Specify how long other router processes wait for ANCP to restart before considering it to be down.
Options	<i>seconds</i> —Number of seconds other processes wait for ANCP to restart. Range: 45 through 600 seconds Default: 45 seconds
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Specifying How Long Processes Wait for ANCP Restart to Complete on page 472

neighbor

Syntax	neighbor <i>ip-address</i> ;
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in JUNOS Release 9.4.
Description	Specify an ANCP neighbor to be monitored.
Options	<i>ip-address</i> —IP address of the ANCP neighbor.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	<ul style="list-style-type: none"> ■ Configuring ANCP on page 467

pre-ietf-mode

Syntax	pre-ietf-mode
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in JUNOS Release 9.4.
Description	Configure ANCP to run in a mode that is backwards compatible with the draft RFC, <i>Protocol for Access Node Control Mechanism in Broadband Networks</i> , <i>draft-ietf-ancp-protocol-00.txt</i> .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring ANCP for Backwards Compatibility on page 473

qos-adjust

Syntax	qos-adjust;
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in JUNOS Release 9.4.
Description	Specify that CoS policy for interfaces and interface sets is adjusted according to ANCP protocol messages. Updates QoS adjustments for all subscribers.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Topics	■ Configuring ANCP to Adjust CoS Traffic Shaping on page 473

traceoptions

Syntax traceoptions {
 file <filename> <files number> <size maximum-file-size> <world-readable |
 no-world-readable> <match regular-expression >;
 flag flag <disable>;
 level (all | error | info | notice | verbose | warning);
 no-remote-trace;
 }

Hierarchy Level [edit protocols ancp]

Release Information Statement introduced in JUNOS Release 9.4.

Description Define tracing operations for ANCP processes.

Options file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory */var/log*.

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- all—Trace all operations.
- config—Trace configuration events.
- general—Trace general flow.
- packet—Trace ANCP packet transmit and receive operations.
- process—Trace process internals.
- protocol—Trace protocol events.
- restart—Trace process restart flow
- routing-socket—Trace routing socket events.
- session—Trace connection events and flow.
- startup—Trace ANCP startup events and flow.
- subscriber—Trace subscriber events.
- timer—Trace timer processing.

level—Level of tracing to perform. You can specify any of the following levels:

- all—Match all levels.
- error—Match error conditions.
- info—Match informational messages.
- notice—Match notice messages about conditions requiring special handling.
- verbose—Match verbose messages.
- warning—Match verbose messages.

`disable`—Disable this trace flag.

`no-remote-trace`—Disable remote tracing.

Required Privilege Level `interface`—To view this statement in the configuration.
 `interface-control`—To add this statement to the configuration.

Related Topics ■ Tracing ANCP Operations on page 468

Part 9

Subscriber Access Examples

- Service Profile Examples on page 485

Chapter 39

Service Profile Examples

- Example: Configuring a Tiered Service Profile for Subscriber Access on page 485

Example: Configuring a Tiered Service Profile for Subscriber Access

This example shows how to configure a tiered service profile for subscribers.

The profile contains three services:

- Gold—Subscribers that pay for this service are allocated 10M bandwidth for data, voice, and video services.
- Silver—Subscribers that pay for this service are allocated 5M bandwidth for data, voice, and video services.
- Bronze—Subscribers that pay for this service are allocated 1M bandwidth for the data service only.

Each subscriber is allocated a VLAN that is created statically. Subscribers log in using DHCP and authenticate using RADIUS. The subscribers can migrate from one service to another when they change subscriptions.

To configure a profile for a tiered service:

1. Configure the VLAN interfaces associated with each subscriber. Enable hierarchical scheduling for the interface.

```
interfaces {
  ge-2/0/0 {
    description subscribers;
    hierarchical-scheduler;
    stacked-vlan-tagging;
    unit 1 {
      vlan-tags outer 100 inner 100;
      family inet {
        unnumbered-address lo0.0 preferred-source-address 100.0.0.1;
      }
    }
    unit 2 {
      family inet {
        vlan-tags outer 101 inner 101;
        unnumbered-address lo0.0 preferred-source-address 100.0.0.1;
      }
    }
  }
}
```



```

    unit 3 {
      vlan-tags outer 102 inner 102;
      family inet {
        unnumbered-address lo0.0 preferred-source-address 100.0.0.1;
      }
    }
  }
}

```

2. Configure the static CoS parameters.

In this example, each offering (video, voice, and data) is assigned a queue, and each service (Gold, Silver, and Bronze) is assigned a scheduler.

```

class-of-service {
  forwarding-classes {
    queue 0 data;
    queue 1 voice;
    queue 3 video;
  }
  scheduler-maps {
    bronze_service_smap {
      forwarding-class data scheduler data_sch;
    }
    silver_service_smap {
      forwarding-class data scheduler data_sch;
      forwarding-class voice scheduler silver_voice_sch;
      forwarding-class video scheduler silver_video_sch;
    }
    gold_service_smap {
      forwarding-class data scheduler data_sch;
      forwarding-class voice scheduler gold_voice_sch;
      forwarding-class video scheduler gold_video_sch;
    }
  }
  schedulers {
    data_sch {
      transmit-rate percent 20;
      buffer-size remainder;
      priority low;
    }
    silver_voice_sch {
      transmit-rate percent 30;
      buffer-size remainder;
      priority high;
    }
    silver_video_sch {
      transmit-rate percent 30;
      buffer-size remainder;
      priority medium;
    }
    gold_voice_sch {
      transmit-rate percent 40;
      buffer-size remainder;
      priority high;
    }
  }
}

```



```

    gold_video_sch {
        transmit-rate percent 40;
        buffer-size remainder;
        priority medium;
    }
}

```

3. Configure the dynamic profile for the service.

The scheduler maps configured for each service are referenced in the dynamic profile.

```

dynamic-profiles {
    subscriber_profile {
        interfaces {
            "$junos-interface-ifd-name" {
                unit "$junos-underlying-interface-unit" {
                    family inet;
                }
            }
        }
        class-of-service {
            traffic-control-profiles {
                subscriber_tcp {
                    scheduler-map $smap;
                    shaping-rate $shaping-rate;
                    guaranteed-rate $guaranteed-rate;
                    delay-buffer-rate $delay-buffer-rate;
                }
            }
            interfaces {
                "$junos-interface-ifd-name" {
                    unit "$junos-underlying-interface-unit" {
                        output-traffic-control-profile subscriber_tcp;
                    }
                }
            }
        }
    }
}

```

4. Configure access for the subscribers.

The DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server. You use DHCP relay to obtain configuration parameters, including an IP address, for subscribers. In this example, one DHCP server, address 100.20.42.1, can be used by subscribers.

The DHCP relay configuration is attached to an active server group named `service_provider_group`.

The subscribers are grouped together within the `subscriber_group`, and identifies characteristics such as authentication, username info, and the associated interfaces for the group members. In this example, it also identifies the active server group and the dynamic interface that is used by the subscribers in the group.


```
forwarding-options {  
  dhcp-relay {  
    server-group {  
      service_provider_group {  
        100.20.42.1;  
      }  
    }  
    group subscriber_group {  
      active-server-group service_provider_group;  
      dynamic-profile subscriber_profile;  
      interface ge-2/0/0.1;  
      interface ge-2/0/0.2;  
      interface ge-2/0/0.3;  
    }  
  }  
}
```

Related Topics ■ For more information about configuring CoS for subscriber access, see CoS for Subscriber Access Overview on page 377

Part 10

Complete Configuration Statement Hierarchy for Subscriber Access

- Subscriber Access Statement Hierarchy on page 491

Chapter 40

Subscriber Access Statement Hierarchy

- [edit access address-assignment] Hierarchy Level on page 491
- [edit access profile] Hierarchy Level on page 491
- [edit dynamic-profiles] Hierarchy Level on page 493
- [edit forwarding-options dhcp-relay] Hierarchy Level on page 494
- [edit-protocols ancp] Hierarchy Level on page 496
- [edit services mobile-ip] Hierarchy Level on page 496
- [edit services radius-flow-tap] Hierarchy Level on page 497
- [edit system services dhcp-local-server] Hierarchy Level on page 497

[edit access address-assignment] Hierarchy Level

```
address-assignment {  
  pool pool-name family inet {  
    network address-or-prefix</subnet-mask>;  
    range range-name {  
      low lower-limit high upper-limit;  
    }  
    host hostname {  
      hardware-address mac-address;  
      ip-address ip-address;  
    }  
    dhcp-attributes {  
      [protocol-specific attributes]  
    }  
  }  
}
```

[edit access profile] Hierarchy Level

```
profile profile-name {  
  authentication-order [ authentication-methods ];  
  accounting {  
    accounting-stop-on-access-deny;  
    accounting-stop-on-failure;  
    order [ accounting-method ];  
    statistics (time | volume-time);  
    update-interval minutes;  
  }  
}
```



```

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

```



```

    }
    radius-server server-address {
        accounting-port port-number;
        port port-number;
        retry attempts;
        routing-instance routing-instance-name;
        secret password;
        timeout source-address;
        timeout seconds;
    }
}

```

[edit dynamic-profiles] Hierarchy Level

```

dynamic-profiles {
    profile-name {
        class-of-service {
            interfaces{
                interface-name {
                }
                unit logical-unit-number {
                    output-traffic-control-profile profile-name;
                }
            }
            traffic-control-profiles profile-name {
                delay-buffer-rate (percent percentage | rate);
                guaranteed-rate (percent percentage | rate);
                scheduler-map map-name;
                shaping-rate (percent percentage | rate);
            }
        }
        interfaces {
            interface-name {
                unit logical-unit-number {
                    family family {
                        address address;
                        filter {
                            input filter-name;
                            output filter-name;
                        }
                        unnumbered-addressinterface-name {
                            preferred-source-address address;
                        }
                    }
                    vlan-id;
                }
                vlan-tagging;
            }
            demux0 {
                unit logical-unit-number {
                    demux-options {
                        underlying-interface interface-name
                    }
                    demux-source {
                        source-prefix;
                    }
                }
            }
        }
    }
}

```



```

        family family {
            address address;
            filter {
                input filter-name;
                output filter-name;
            }
            mac-validate (loose | strict):
            unnumbered-address interface-name {
                preferred-source-address address;
            }
        }
    }
}
protocols {
igmp {
    interface interface-name {
        accounting;
        disable;
        group-policy;
        immediate-leave;
        no-accounting;
        promiscuous-mode;
        ssm-map ssm-map-name;
        static {
            group group {
                source source;
            }
        }
        version version;
    }
}
}
}

```

[edit forwarding-options dhcp-relay] Hierarchy Level

```

dhcp-relay {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            mac-address;
            option-60;
            option-82 [circuit-id] [remote-id];
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    dynamic-profile profile-name (aggregate-clients | use-primary primary-profile-name);
    overrides {
        always-write-giaddr;
        always-write-option-82;
    }
}

```



```

    client-discover-match;
    interface-client-limit number;
    layer2-unicast-replies;
    no-arp;
    trust-option-82;
    disable-relay;
}
relay-option-60 {
    vendor-option {
        (equals | starts-with) (ascii match-string | hexadecimal match-hex) {
            (default-relay-server-group server-group-name |
             default-local-server-group local-server-group-name |
             drop);
        }
        (default-relay-server-group server-group-name |
         default-local-server-group local-server-group-name |
         drop);
    }
}
relay-option-82 {
    circuit-id {
        prefix host-name logical-system-name routing-instance-name;
    }
}
server-group {
    server-group-name {
        server-ip-address;
    }
}
active-server-group server-group-name;
group group-name {
    active-server-group server-group-name;
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            mac-address;
            option-60;
            option-82 [circuit-id] [remote-id];
            overrides {
                always-write-giaddr;
                always-write-option-82;
                client-discover-match;
                interface-client-limit number;
                layer2-unicast-replies;
                no-arp;
                trust-option-82;
                disable-relay;
            }
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
}

```



```

dynamic-profile profile-name (aggregate-clients | use-primary primary-profile-name);
relay-option-60 {
  vendor-option {
    (equals | starts-with) (ascii match-string | hexadecimal match-hex) {
      (default-relay-server-group server-group-name |
      default-local-server-group local-server-group-name |
      drop);
    }
    (default-relay-server-group server-group-name |
    default-local-server-group local-server-group-name |
    drop);
  }
}
relay-option-82 {
  circuit-id {
    prefix host-name logical-system-name routing-instance-name;
  }
}
interface interface-name [upto upto-interface-name] [exclude];
}
traceoptions {
  file filename <files number> <size size> <world-readable | no-world-readable>
    <match regex>;
  flag flag;
}
}

```

[edit-protocols ancp] Hierarchy Level

```

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

```

[edit services mobile-ip] Hierarchy Level

```

authenticate {
  order (aaa | local);
}
dynamic-home-assignment {

```



```

home-agent {
  nai (name@domain.com | @domain.com) {
    home-agent ip-address;
  }
}
home-agent {
  enable-service {
    [list-of-interfaces];
  }
  virtual-network {
    home-agent-address ip-address {
      registration-lifetime value;
      timestamp-tolerance value;
      revocation-required;
    }
  }
}
peer {
  (ip-address address | nai user@domain) {
    spi hexval {
      algorithm (hmac-md5 | md5);
      entity-type (host | mobility-agent);
      key (hex | ascii) string;
      replay-method (timestamp tolerance seconds | none);
    }
  }
}
traceoptions
  file filename <files number> <match regular-expression > <size maximum-file-size>
  <world-readable | no-world-readable>;
  flag flag;
  level <all | error | info | notice | verbose | warning>;
  no-remote-trace;
}

```

[edit services radius-flow-tap] Hierarchy Level

```

radius-flow-tap {
  forwarding-class class-name;
  interfaces interface-name;
  source-ipv4-address ipv4-address;
}

```

[edit system services dhcp-local-server] Hierarchy Level

```

dhcp-local-server {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
    }
  }
}

```



```

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

```


Part 11

Index

- Index on page 501
- Index of Statements and Commands on page 509

Index

Symbols

#, comments in configuration statements.....	xxxiii
\$junos-cos-delay-buffer-rate internal variable.....	432
\$junos-cos-guaranteed-rate internal variable.....	436
\$junos-cos-scheduler internal variable.....	443
\$junos-cos-scheduler-bs internal variable.....	430
\$junos-cos-scheduler-dropfile-any internal variable.....	433
\$junos-cos-scheduler-dropfile-high internal variable.....	433
\$junos-cos-scheduler-dropfile-low internal variable.....	433
\$junos-cos-scheduler-dropfile-medium-high internal variable.....	433
\$junos-cos-scheduler-dropfile-medium-low internal variable.....	433
\$junos-cos-scheduler-map internal variable.....	441
\$junos-cos-scheduler-pri internal variable.....	439
\$junos-cos-scheduler-tx internal variable.....	446
\$junos-cos-shaping-rate internal variable.....	444
(), in syntax descriptions.....	xxxiii
802.1Q VLANs	
VLAN tagging.....	360
< >, in syntax descriptions.....	xxxiii
[], in configuration statements.....	xxxiii
{ }, in configuration statements.....	xxxiii
(pipe), in syntax descriptions.....	xxxiii

A

AAA	
and Mobile IP home agent.....	243
AAA directed logout	
DHCP authentication services.....	53, 76
AAA Service Framework.....	17
dynamic service activation	
during login.....	25
access profiles	
attaching.....	37
access-identifier statement	
ANCP.....	476
accounting	
configuring RADIUS.....	19
Mobile IP time-based.....	243

accounting methods.....	19
accounting statement	
access profile.....	123
IGMP (interface).....	453
accounting statistics.....	20
accounting-port statement.....	124
accounting-server statement.....	125
accounting-session-id-format statement.....	125
accounting-stop-on-access-deny statement.....	126
accounting-stop-on-failure statement.....	126
active server groups	
DHCP relay.....	95
active-server-group statement.....	127
address statement.....	343
address-assignment pools	
client attributes.....	41
DHCP.....	42
DHCP local server.....	51
license requirements.....	43
name.....	40
named range.....	41
network address.....	40
static address.....	41
tracing operations.....	43
address-assignment statement.....	39, 128
adjacency-timer statement	
ANCP.....	476
agent-circuit-id suboption	
DHCP relay.....	92
aggregated Ethernet logical interfaces <i>See</i> subscriber interfaces, IP demux over aggregated Ethernet <i>See</i> subscriber interfaces, VLAN over aggregated Ethernet	
algorithm statement	
Mobile IP.....	257
always-write-giaddr statement.....	129
always-write-option-82 statement.....	130
ANCP	
adjusting subscriber traffic with.....	465
CoS shaping rate adjustment for subscriber local loops.....	465
monitoring subscriber traffic with.....	465
overview.....	465
shaping-rate adjustments for subscriber local loops.....	414
tracing operations.....	468

ancp statement	
ANCP.....	475
attribute statement	
dynamic profile variables.....	297
attributes statement.....	131
authenticate statement	
Mobile IP.....	257
authentication	
configuring RADIUS.....	19
Mobile IP home agent.....	243
authentication methods.....	19
authentication services	
with DHCP.....	53, 76
authentication statement	
DHCP local server.....	132
DHCP relay agent.....	133
authentication-order statement.....	134
authentication-server statement.....	134
auto logout	
DHCP.....	59, 84
DHCP relay agent option 82.....	85

B

boot-file statement.....	135
boot-server statement.....	135
braces, in configuration statements.....	xxxiii
brackets	
angle, in syntax descriptions.....	xxxiii
square, in configuration statements.....	xxxiii
buffer-size statement	
dynamic-profiles.....	430

C

change of authorization <i>See</i> CoA	
circuit-id statement	
address-assignment pools.....	136
DHCP relay agent.....	137
circuit-type statement	
DHCP local server.....	138
DHCP relay agent.....	139
class of service <i>See</i> CoS	
class-of-service statement.....	431
client attributes	
address-assignment pools.....	41
client configuration information	
DHCP.....	49
client usernames	
DHCP	
unique.....	64
client-discover-match statement	
DHCP local server.....	140
DHCP relay agent.....	141

CoA	
messages.....	26
RADIUS.....	26
comments, in configuration statements.....	xxxiii
conventions	
text and syntax.....	xxxii
CoS	
IP demux	
configuring.....	400
overview.....	378
RADIUS-provided parameters	
configuring a client dynamic profile.....	394
example.....	410
overview.....	378
shaping-rate adjustments for subscriber local loops	
configuration guidelines.....	415
disabling.....	423
enabling.....	417
example.....	425
overview.....	414
subscriber access	
changing services.....	385
configuration guidelines.....	388
configuration overview.....	389
configuring variables.....	397
dynamic configuration overview.....	391
interfaces.....	400
overview.....	377
static scheduling and queuing example.....	403
traffic parameters.....	392
curly braces, in configuration statements.....	xxxiii
customer support.....	xli
contacting JTAC.....	xli

D

default-local-server-group statement.....	142
default-relay-server-group statement.....	143
default-value statement	
dynamic profile variables.....	297
delay-buffer-rate statement.....	432
delimiter statement	
DHCP local server.....	144
DHCP relay agent.....	145
demux interfaces	
unit statement.....	357
demux-options statement	
dynamic demux interface.....	345
demux-source statement	
dynamic demux interfaces.....	346
demux0 statement	
dynamic demux interface.....	344

- DHCP
 - ARP table population
 - overriding.....58, 81
 - authentication services.....53, 76
 - AAA directed logout.....53, 76
 - auto logout.....59, 84
 - client configuration information.....49
 - grouping interfaces.....55, 77
 - maximum clients per interface
 - overriding.....57, 83
 - unique client usernames.....64
 - user passwords.....63
- DHCP local server
 - address-assignment pool selection.....54
 - address-assignment pools.....51
 - ARP table population
 - overriding.....58, 81
 - client auto logout.....61, 86
 - dynamic profile attachment
 - multiple subscribers.....62, 95
 - overview.....52, 75
 - use primary profile.....62, 95
 - grouping interfaces
 - options.....56
 - interaction
 - address-assignment pools.....49
 - DHCP clients.....49
 - maximum clients per interface
 - overriding.....57, 83
 - minimal configuration
 - default settings.....50
 - overriding default configuration.....56
 - overview.....48
 - tracing operations.....66, 97
 - verifying configuration.....66
- DHCP relay
 - access and access-internal routes.....73
 - active server groups.....95
 - agent-circuit-id suboption.....92
 - ARP table population
 - overriding.....58, 81
 - client auto logout.....61, 86
 - configuration examples
 - minimum configuration.....118
 - multiple clients and servers
 - configuration.....119
 - option 60 drop configuration.....121
 - option 60 forward configuration.....120
 - disabling.....83
 - discarded packets
 - counting.....91
 - dynamic profile attachment
 - multiple subscribers.....62, 95
 - overview.....52, 75
 - use primary profile.....62, 95
 - graceful Routing Engine switchover.....74
 - grouping interfaces
 - options.....78
 - Layer 2 unicast transmission.....81
 - matching option 60 strings.....88
 - maximum clients per interface
 - overriding.....57, 83
 - nonmatching option 60 strings.....91
 - option 60 information.....87
 - option 82 information.....91
 - option 82 prefix.....93
 - overriding broadcast bit.....81
 - overriding default configuration.....79
 - overriding option 82.....80
 - overwrite giaddr.....80
 - server groups.....94
 - state persistence.....74
 - tracing operations.....66, 97
 - trusting option 82.....81
- DHCP relay agent
 - how components interact.....72
 - Option 82
 - auto logout.....85
 - overview.....72
 - verifying configuration.....97
- DHCP subscriber
 - auto logout.....61, 86
- dhcp-attributes statement.....146
- dhcp-local-server statement.....147
- dhcp-relay statement.....149
- directed logout
 - AAA.....53, 76
- disable statement
 - IGMP.....454
- disable-relay statement.....152
- documentation set
 - comments on.....xl
- domain-name statement
 - address-assignment pools.....152
 - DHCP local server.....153
 - DHCP relay agent.....154
- drop statement.....155
- drop-profile statement
 - dynamic profiles.....433
 - RED.....433
- drop-profile-map statement
 - dynamic profiles.....434
- dynamic firewall filters
 - attaching statically created.....367
 - attaching with RADIUS.....368
 - basic syntax.....365
 - components.....364
 - configuration guidelines.....365
 - examples.....371
 - ordering.....369
 - overview.....363

- processing order.....364
 - types of.....363
 - Dynamic Host Control Protocol *See* DHCP
 - dynamic profiles
 - components.....8
 - configuring basic.....283
 - configuring for client access.....287
 - configuring services levels.....288
 - DHCP attachment.....62, 95
 - overview.....52, 75
 - examples.....293, 294
 - interface support.....275
 - overview.....52, 75
 - modifying.....289
 - overview.....275
 - router internal variables.....8
 - tiered service example.....485
 - dynamic protocols
 - overview.....451
 - dynamic requests
 - RADIUS.....25, 28
 - dynamic service activation
 - during login.....25
 - dynamic variables
 - configuring.....284, 285
 - overview.....276
 - dynamic-home-assignment statement
 - Mobile IP.....258
 - dynamic-profile statement
 - DHCP local server.....157
 - DHCP relay agent.....158
 - dynamic-profiles
 - interfaces statement.....350
 - dynamic demux.....351
 - dynamic-profiles statement.....298
- E**
- enable-service statement
 - Mobile IP.....258
 - entity-type statement
 - Mobile IP.....259
 - Ethernet interfaces
 - unnumbered
 - preferred source address.....354
 - VLAN tagging.....360
 - ethernet-port-type-virtual statement.....159
 - exclude statement.....160
- F**
- family statement.....347
 - dynamic demux interfaces.....348
 - Fast Ethernet interfaces
 - VLAN tagging.....360
 - filter statement.....349
 - firewall filters *See* dynamic firewall filters
 - flow-tap service *See* subscriber secure policy
 - font conventions.....xxxii
 - forwarding-class statement
 - dynamic profiles.....435
 - subscriber secure policy.....162
- G**
- Gigabit Ethernet interfaces
 - VLAN tagging.....360
 - grace-period statement.....163
 - graceful Routing Engine switchover
 - DHCP relay agent.....74
 - group statement
 - DHCP local server.....164
 - DHCP relay agent.....165
 - IGMP (with source).....455
 - IGMP (without source).....455
 - group-policy statement
 - IGMP.....456
 - guaranteed-rate statement.....436
- H**
- hardware-address statement.....167
 - home agent, Mobile IP *See* Mobile IP home agent
 - home-agent statement
 - Mobile IP
 - dynamic home assignment rule.....260
 - networks.....259
 - home-agent-address statement
 - Mobile IP.....260
 - host statement.....167
- I**
- icons defined, notice.....xxxii
 - IGMP
 - enabling.....457, 461
 - version.....464
 - igmp statement.....457
 - ignore statement.....168
 - immediate-leave statement
 - IGMP.....458
 - immediate-update statement.....168
 - interface groups
 - DHCP local server
 - options.....56
 - DHCP relay
 - options.....78
 - interface statement
 - DHCP local server.....169
 - DHCP relay agent.....170
 - IGMP.....459, 461

interface-client-limit statement	
DHCP local server.....	171
DHCP relay agent.....	172
interface-description-format statement.....	173
interface-set statement	
ANCP.....	477
interfaces	
unit statement.....	356
interfaces statement.....	173
ANCP.....	477
CoS.....	437
dynamic profiles.....	350
dynamic demux	351
internal variables <i>See</i> variables, JUNOS internal	
Internet Group Management Protocol <i>See</i> IGMP	
ip-address statement.....	174
ip-address-first statement.....	175

J

Juniper Networks VSAs.....	29
supported.....	32

K

key statement	
Mobile IP.....	261

L

layer2-unicast-replies statement.....	176
license requirements	
address-assignment pools.....	43
local-server-group statement.....	177
logical-system-name statement	
DHCP local server.....	179
DHCP relay agent.....	178
loss-priority statement	
dynamic profiles.....	438

M

MAC address validation	
dynamic subscriber interfaces	
configuring.....	317
overview.....	309
static subscriber interfaces	
configuring.....	316
mac-address statement	
DHCP local server.....	180
DHCP relay agent.....	181
mac-validate statement.....	352
mandatory statement	
dynamic profile variables.....	300
manuals	
comments on.....	xl

maximum-helper-restart-time statement	
ANCP.....	478
maximum-lease-time statement.....	181
Mobile IP	
tracing operations.....	250
Mobile IP home agent	
AAA.....	243
accounting.....	243
agent discovery.....	243
authentication.....	243
home address assignment.....	243
overview.....	243
registration.....	243
mobile-ip statement.....	262

N

nai statement	
Mobile IP.....	263
name-server statement.....	182
nas-identifier statement.....	182
nas-port-extended-format statement.....	183
neighbor statement	
ANCP.....	478
netbios-node-type statement.....	184
network statement.....	184
no-accounting statement	
IGMP (interface).....	460
no-arp statement	
DHCP local server.....	185
DHCP relay agent.....	186
notice icons defined.....	xxxii

O

option 60 information	
DHCP relay.....	87
option 60 strings	
DHCP relay.....	88, 91
Option 82	
DHCP relay agent	
auto logout.....	85
option 82 information	
DHCP relay.....	91
option 82 prefix	
DHCP relay.....	93
option statement.....	187
option-60 statement	
DHCP local server.....	188
DHCP relay agent.....	189
option-82 statement	
address-assignment pools.....	190
DHCP local server.....	191
address-assignment pools.....	192
DHCP relay agent.....	193
option-match statement.....	194

options statement.....	195
order statement	
accounting.....	196
Mobile IP.....	264
output-traffic-control-profile statement.....	438
override-nas-information statement.....	196
overrides statement	
DHCP local server.....	197
DHCP relay agent.....	198

P

parentheses, in syntax descriptions.....	xxxiii
password statement	
DHCP local server.....	199
DHCP relay agent.....	200
passwords	
DHCP users.....	63
peer statement	
Mobile IP.....	265
physical interfaces	
VLAN tagging.....	360
pool statement.....	200
pool-match-order statement.....	201
port statement	201
pre-ietf-mode statement	
ANCP.....	479
precedence statement.....	353
preferred-source-address statement.....	354
prefix statement.....	202
priority statement	
dynamic profiles.....	439
profile statement.....	205
promiscuous-mode statement	
IGMP (interface).....	460
protocol statement	
dynamic profiles.....	440
protocols statement.....	461

Q

qos-adjust statement	
ANCP.....	479

R

RADIUS	
CoA.....	26
CoS parameters for initial services	
configuring a client dynamic profile.....	394
example.....	410
overview.....	378
dynamic requests.....	25, 28
RADIUS attributes.....	29
ignoring and excluding.....	23
supported.....	29

RADIUS servers <i>See</i> subscriber secure policy	
configuring interaction with.....	18
configuring parameters.....	21
options.....	21
specifying.....	21
radius statement.....	208
dynamic profile variables.....	300
radius-flow-tap statement.....	209
RADIUS-initiated disconnect.....	27
messages.....	27
radius-server statement	210
range statement.....	211
registration-lifetime statement	
Mobile IP.....	266
relay-option-60 statement.....	212
relay-option-82 statement.....	213
relay-server-group statement.....	214
remote-id statement.....	215
replay-method statement	
Mobile IP.....	267
retry statement.....	215
revert-interval statement.....	216
revocation-required statement	
Mobile IP.....	266
router statement.....	216
routing-instance statement.....	217
routing-instance-name statement	
DHCP local server.....	218
DHCP relay agent.....	219

S

scheduler statement	
dynamic profiles.....	440
scheduler-map statement	
dynamic profiles.....	441
scheduler-maps statement	
dynamic profiles.....	442
schedulers statement	
dynamic profiles.....	443
secret statement	
access.....	219
server groups	
DHCP relay.....	94
server-group statement.....	220
shaping-rate adjustments.....	413
for subscriber local loops.....	465
configuration guidelines.....	415
disabling.....	423
enabling.....	417
example.....	425
overview.....	414
shaping-rate statement	
dynamic profiles.....	444
source statement	
IGMP (interface).....	462

source-address statement.....221
 source-ipv4-address statement.....221
 spi statement
 Mobile IP.....268
 ssm-map statement
 IGMP (interface).....462
 state persistence, DHCP.....74
 static statement
 IGMP (interface).....463
 statistics statement.....222, 269
 subscriber access
 configuration overview.....8
 configuring.....15
 environment.....4
 licensing.....6
 managing access and services.....7
 operation flow.....6
 overview.....3
 support.....5
 subscriber access management
 overview.....15
 subscriber information
 verifying.....37
 subscriber interfaces
 configuring in dynamic profiles.....311
 example
 gigabit Ethernet VLAN.....319
 gigabit Ethernet VLAN with multiple logical
 units.....319
 gigabit Ethernet VLAN with no
 autonegotiation.....320
 IP demux over aggregated Ethernet.....340
 loopback.....320
 VLAN over aggregated Ethernet.....337
 IP demux
 configuring.....313
 guidelines.....308
 overview.....307
 IP demux over aggregated Ethernet
 configuring.....331
 example.....340
 overview.....325
 overview.....5, 305
 VLAN
 configuring.....312
 overview.....306
 VLAN over aggregated Ethernet
 configuring.....329
 example.....337
 overview.....323
 subscriber local loops
 CoS shaping-rate adjustments
 configuration guidelines.....415
 disabling.....423
 enabling.....417

 example.....425
 overview.....414
 CoS shaping-rate adjustments with ANCP.....465
 subscriber secure policy
 architecture.....105
 configuration guidelines.....111
 configuring.....110
 considerations.....109
 flow-tap service configuration.....112
 overview.....104
 RADIUS server configuration.....113
 RADIUS-initiated.....107
 system resources.....111
 terminating.....114
 support, technical *See* technical support
 syntax conventions.....xxxii

T

tag statement
 dynamic profile variables.....301
 technical support
 contacting JTAC.....xli
 tftp-server statement.....223
 timeout statement.....223
 timestamp-tolerance statement
 Mobile IP.....270
 traceoptions statement
 address-assignment pools.....224
 ANCP.....480
 DHCP local server.....227
 DHCP relay agent.....230
 Mobile IP.....271
 tracing operations
 address-assignment pools.....43
 ANCP.....468
 DHCP local server.....66, 97
 DHCP relay.....66, 97
 Mobile IP.....250
 traffic mirroring *See* subscriber secure policy
 traffic-control-profiles statement.....445
 transmit-rate statement
 dynamic profiles.....446
 trust-option-82 statement.....232

U

underlying-interface statement
 dynamic profiles.....355
 unit statement
 CoS.....447
 demux interfaces.....357
 interfaces.....356
 unnumbered interfaces
 Ethernet
 preferred source address.....354

unnumbered-address statement.....	358
update-interval statement.....	233
user-defined variables <i>See</i> variables, user-defined	
user-prefix statement	
DHCP local server.....	236
DHCP relay agent.....	237
username-include statement	
DHCP local server.....	234
DHCP relay agent.....	235

V

variables	
overview.....	276
variables statement	
dynamic profile variables.....	301
variables, JUNOS internal.....	277
dynamic CoS (schedulers)	
\$junos-cos-scheduler.....	443
\$junos-cos-scheduler-bs.....	430
\$junos-cos-scheduler-dropfile-any.....	433
\$junos-cos-scheduler-dropfile-high.....	433
\$junos-cos-scheduler-dropfile-low.....	433
\$junos-cos-scheduler-dropfile-medium-high.....	433
\$junos-cos-scheduler-dropfile-medium-low.....	433
\$junos-cos-scheduler-pri.....	439
\$junos-cos-scheduler-tx.....	446
configuring a client dynamic profile.....	394
example.....	410
overview.....	378
dynamic CoS (traffic-control-profiles)	
\$junos-cos-delay-buffer-rate.....	432
\$junos-cos-guaranteed-rate.....	436
\$junos-cos-scheduler-map.....	441
\$junos-cos-shaping-rate.....	444
configuring a client dynamic profile.....	394
example.....	410
overview.....	378
variables, user-defined.....	281
vendor-id statement	
dynamic profile variables.....	302
vendor-option statement.....	238
vendor-specific attributes	
supported.....	32
version statement	
IGMP (interface).....	464
virtual-network statement	
Mobile IP.....	272
VLAN tagging.....	360
vlan-id statement.....	359
vlan-nas-port-stacked-format statement.....	239
vlan-tagging statement.....	360
VSAs	
supported.....	32

W

wins-server statement.....	239
wireless roaming	
Mobile IP.....	243

Index of Statements and Commands

A

access-identifier statement	
ANCP.....	476
accounting statement	
access profile.....	123
IGMP (interface).....	453
accounting-port statement.....	124
accounting-server statement.....	125
accounting-session-id-format statement.....	125
accounting-stop-on-access-deny statement.....	126
accounting-stop-on-failure statement.....	126
active-server-group statement.....	127
address statement.....	343
address-assignment statement.....	39, 128
adjacency-timer statement	
ANCP.....	476
algorithm statement	
Mobile IP.....	257
always-write-giaddr statement.....	129
always-write-option-82 statement.....	130
ancp statement	
ANCP.....	475
attribute statement	
dynamic profile variables.....	297
attributes statement.....	131
authenticate statement	
Mobile IP.....	257
authentication statement	
DHCP local server.....	132
DHCP relay agent.....	133
authentication-order statement.....	134
authentication-server statement.....	134

B

boot-file statement.....	135
boot-server statement.....	135
buffer-size statement	
dynamic-profiles.....	430

C

circuit-id statement	
address-assignment pools.....	136
DHCP relay agent.....	137
circuit-type statement	
DHCP local server.....	138
DHCP relay agent.....	139
class-of-service statement.....	431
client-discover-match statement	
DHCP local server.....	140
DHCP relay agent.....	141

D

default-local-server-group statement.....	142
default-relay-server-group statement.....	143
default-value statement	
dynamic profile variables.....	297
delay-buffer-rate statement.....	432
delimiter statement	
DHCP local server.....	144
DHCP relay agent.....	145
demux interfaces	
unit statement.....	357
demux-options statement	
dynamic demux interface.....	345
demux-source statement	
dynamic demux interfaces.....	346
demux0 statement	
dynamic demux interface.....	344
dhcp-attributes statement.....	146
dhcp-local-server statement.....	147
dhcp-relay statement.....	149
disable statement	
IGMP.....	454
disable-relay statement.....	152
domain-name statement	
address-assignment pools.....	152
DHCP local server.....	153
DHCP relay agent.....	154
drop statement.....	155
drop-profile statement	
dynamic profiles.....	433

drop-profile-map statement	
dynamic profiles.....	434
dynamic-home-assignment statement	
Mobile IP.....	258
dynamic-profile statement	
DHCP local server.....	157
DHCP relay agent.....	158
dynamic-profiles statement.....	298

E

enable-service statement	
Mobile IP.....	258
entity-type statement	
Mobile IP.....	259
ethernet-port-type-virtual statement.....	159
exclude statement.....	160

F

family statement.....	347
dynamic demux interfaces.....	348
filter statement.....	349
forwarding-class statement	
dynamic profiles.....	435
subscriber secure policy.....	162

G

grace-period statement.....	163
group statement	
DHCP local server.....	164
DHCP relay agent.....	165
IGMP (with source).....	455
IGMP (without source).....	455
group-policy statement	
IGMP.....	456
guaranteed-rate statement.....	436

H

hardware-address statement.....	167
home-agent statement	
Mobile IP	
dynamic home assignment rule.....	260
networks.....	259
home-agent-address statement	
Mobile IP.....	260
host statement.....	167

I

igmp statement.....	457
ignore statement.....	168
immediate-leave statement	
IGMP.....	458

immediate-update statement.....	168
interface statement	
DHCP local server.....	169
DHCP relay agent.....	170
IGMP.....	459, 461
interface-client-limit statement	
DHCP local server.....	171
DHCP relay agent.....	172
interface-description-format statement.....	173
interface-set statement	
ANCP.....	477
interfaces statement.....	173
ANCP.....	477
CoS.....	437
dynamic profiles.....	350
dynamic demux	351
ip-address statement.....	174
ip-address-first statement.....	175

K

key statement	
Mobile IP.....	261

L

layer2-unicast-replies statement.....	176
local-server-group statement.....	177
logical-system-name statement	
DHCP local server.....	179
DHCP relay agent.....	178
loss-priority statement	
dynamic profiles.....	438

M

mac-address statement	
DHCP local server.....	180
DHCP relay agent.....	181
mac-validate statement.....	352
mandatory statement	
dynamic profile variables.....	300
maximum-helper-restart-time statement	
ANCP.....	478
maximum-lease-time statement.....	181
mobile-ip statement.....	262

N

nai statement	
Mobile IP.....	263
name-server statement.....	182
nas-identifier statement.....	182
nas-port-extended-format statement.....	183
neighbor statement	
ANCP.....	478

netbios-node-type statement.....	184
network statement.....	184
no-accounting statement	
IGMP (interface).....	460
no-arp statement	
DHCP local server.....	185
DHCP relay agent.....	186

O

option statement.....	187
option-60 statement	
DHCP local server.....	188
DHCP relay agent.....	189
option-82 statement	
address-assignment pools.....	190
DHCP local server.....	191
address-assignment pools.....	192
DHCP relay agent.....	193
option-match statement.....	194
options statement.....	195
order statement	
accounting.....	196
Mobile IP.....	264
output-traffic-control-profile statement.....	438
override-nas-information statement.....	196
overrides statement	
DHCP local server.....	197
DHCP relay agent.....	198

P

password statement	
DHCP local server.....	199
DHCP relay agent.....	200
peer statement	
Mobile IP.....	265
pool statement.....	200
pool-match-order statement.....	201
port statement	201
pre-ietf-mode statement	
ANCP.....	479
precedence statement.....	353
preferred-source-address statement.....	354
prefix statement.....	202
priority statement	
dynamic profiles.....	439
profile statement.....	205
promiscuous-mode statement	
IGMP (interface).....	460
protocol statement	
dynamic profiles.....	440
protocols statement.....	461

Q

qos-adjust statement	
ANCP.....	479

R

radius statement.....	208
dynamic profile variables.....	300
radius-flow-tap statement.....	209
radius-server statement	210
range statement.....	211
registration-lifetime statement	
Mobile IP.....	266
relay-option-60 statement.....	212
relay-option-82 statement.....	213
relay-server-group statement.....	214
remote-id statement.....	215
reply-method statement	
Mobile IP.....	267
retry statement.....	215
revert-interval statement.....	216
revocation-required statement	
Mobile IP.....	266
router statement.....	216
routing-instance statement.....	217
routing-instance-name statement	
DHCP local server.....	218
DHCP relay agent.....	219

S

scheduler statement	
dynamic profiles.....	440
scheduler-map statement	
dynamic profiles.....	441
scheduler-maps statement	
dynamic profiles.....	442
schedulers statement	
dynamic profiles.....	443
secret statement	
access.....	219
server-group statement.....	220
shaping-rate statement	
dynamic profiles.....	444
source statement	
IGMP (interface).....	462
source-address statement.....	221
source-ipv4-address statement.....	221
spi statement	
Mobile IP.....	268
ssm-map statement	
IGMP (interface).....	462
static statement	
IGMP (interface).....	463
statistics statement.....	222, 269

T

tag statement	
dynamic profile variables.....	301
tftp-server statement.....	223
timeout statement.....	223
timestamp-tolerance statement	
Mobile IP.....	270
traceoptions statement	
address-assignment pools.....	224
ANCP.....	480
DHCP local server.....	227
DHCP relay agent.....	230
Mobile IP.....	271
traffic-control-profiles statement.....	445
transmit-rate statement	
dynamic profiles.....	446
trust-option-82 statement.....	232

U

underlying-interface statement	
dynamic profiles.....	355
unit statement	
CoS.....	447
demux interfaces.....	357
interfaces.....	356
unnumbered-address statement.....	358
update-interval statement.....	233
user-prefix statement	
DHCP local server.....	236
DHCP relay agent.....	237
username-include statement	
DHCP local server.....	234
DHCP relay agent.....	235

V

variables statement	
dynamic profile variables.....	301
vendor-id statement	
dynamic profile variables.....	302
vendor-option statement.....	238
version statement	
IGMP (interface).....	464
virtual-network statement	
Mobile IP.....	272
vlan-id statement.....	359
vlan-nas-port-stacked-format statement.....	239
vlan-tagging statement.....	360

W

wins-server statement.....	239
----------------------------	-----