



---

Junos<sup>®</sup> OS

# Subscriber Access Configuration Guide

Release  
11.2



---

Published: 2011-05-16

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

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, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks 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® OS Subscriber Access Configuration Guide*

Release 11.2

Copyright © 2011, Juniper Networks, Inc.

All rights reserved.

#### Revision History

May 2011—R1 Junos OS 11.2

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 OS 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)).



# Abbreviated Table of Contents

	About This Guide .....	li
Part 1	Managing Access Networks	
Chapter 1	Subscriber Access Overview .....	3
Part 2	AAA Service Framework for Subscriber Access	
Chapter 2	Configuring the AAA Service Framework for Subscriber Access .....	17
Chapter 3	Configuring Address-Assignment Pools for Subscriber Access .....	67
Chapter 4	Configuring Domain Maps for Subscriber Access .....	79
Chapter 5	AAA and Remote Subscriber Access Configuration Examples .....	91
Part 3	DHCP Local Server for Subscriber Access	
Chapter 6	DHCP Local Server Overview .....	97
Chapter 7	Configuring DHCP Local Server .....	107
Chapter 8	DHCP Local Server Examples .....	147
Part 4	DHCP Relay Agent for Subscriber Access	
Chapter 9	DHCP Relay Agent Overview .....	153
Chapter 10	Configuring DHCP Relay Agent .....	161
Chapter 11	Configuring Dynamic Access and Access-Internal Routes for DHCP Subscriber Management .....	205
Chapter 12	DHCP Relay Agent Examples .....	209
Part 5	PPP for Subscriber Access	
Chapter 13	Dynamic Profiles for PPP Overview .....	217
Chapter 14	Configuring PPP for Subscriber Access .....	219
Chapter 15	Configuring Subscriber Services for MLPPP Interfaces .....	225
Part 6	L2TP for Subscriber Access	
Chapter 16	L2TP for Subscriber Access Overview .....	231
Chapter 17	Configuring L2TP for Subscriber Access .....	241
Part 7	Diameter Base Protocol and Applications for Subscriber Access	
Chapter 18	Diameter Base Protocol Overview .....	255

Chapter 19	Configuring Diameter Base Protocol . . . . .	259
Chapter 20	JSRC and Juniper Networks Session Resource Control (SRC) Overview . . . . .	271
Chapter 21	Configuring JSRC for Subscriber Access . . . . .	279
Chapter 22	Subscribers on Static Interfaces . . . . .	283
Chapter 23	Configuring Subscribers over Static Interfaces . . . . .	287
Chapter 24	Static Subscribers for Subscriber Access Examples . . . . .	301
Chapter 25	PTSP and Juniper Networks Session and Resource Control (SRC) . . . . .	303
Chapter 26	Configuring the PTSP Application . . . . .	311
Chapter 27	Configuring Packet-Triggered Subscriber Services . . . . .	317
Chapter 28	Gx-Plus Overview . . . . .	329
Chapter 29	Configuring Gx-Plus . . . . .	339
<b>Part 8</b>	<b>Mobile IP Access</b>	
Chapter 30	Mobile IP Overview . . . . .	345
Chapter 31	Configuring Mobile IP . . . . .	357
<b>Part 9</b>	<b>Dynamic Profiles for Access and Services</b>	
Chapter 32	Dynamic Profiles Overview . . . . .	369
Chapter 33	Configuring Dynamic Profiles . . . . .	391
Chapter 34	Dynamic Profile Examples . . . . .	401
<b>Part 10</b>	<b>Dynamic VLANs</b>	
Chapter 35	Dynamic VLAN Overview . . . . .	407
Chapter 36	Configuring Dynamic VLANs . . . . .	409
Chapter 37	Dynamic VLAN Examples . . . . .	427
<b>Part 11</b>	<b>Subscriber Interfaces</b>	
Chapter 38	Subscriber Interface Overview . . . . .	433
Chapter 39	Configuring Subscriber Interfaces for Dynamic Profiles . . . . .	439
Chapter 40	Subscriber Interface Examples . . . . .	451
Chapter 41	Subscriber Interfaces over Aggregated Ethernet Overview . . . . .	471
Chapter 42	Configuring Subscriber Interfaces over Aggregated Ethernet . . . . .	479
Chapter 43	Subscriber Interfaces over Aggregated Ethernet Examples . . . . .	489
Chapter 44	Dynamic PPPoE Subscriber Interfaces Overview . . . . .	527
Chapter 45	Configuring Dynamic PPPoE Subscriber Interfaces . . . . .	535
Chapter 46	Dynamic PPPoE Subscriber Interfaces Examples . . . . .	547
<b>Part 12</b>	<b>Dynamic Firewall Filters, Service Sets and HTTP Redirect for Subscriber Access</b>	
Chapter 47	Dynamic Firewall Filters and Service Sets Overview . . . . .	555

Chapter 48	Configuring Filters for Dynamic Profiles .....	571
Chapter 49	Configuring Fast Update Filters .....	581
Chapter 50	Configuring Service Sets in Dynamic Profiles .....	595
Chapter 51	Firewall Filter Examples .....	597
Chapter 52	Redirecting HTTP Requests Overview .....	613
Chapter 53	Configuring HTTP Redirect .....	615
Chapter 54	HTTP Redirect Examples .....	619
<b>Part 13</b>	<b>Subscriber Secure Policy Traffic Mirroring</b>	
Chapter 55	Subscriber Secure Policy Overview .....	625
Chapter 56	Configuring RADIUS-Flow-Tap Service Support for Subscriber Secure Policy Mirroring .....	631
Chapter 57	Configuring RADIUS-Initiated Subscriber Secure Policy Traffic Mirroring .....	635
Chapter 58	Configuring DTCP-Initiated Subscriber Secure Policy Mirroring .....	641
Chapter 59	Subscriber Secure Policy Mirroring and SNMP Traps .....	645
Chapter 60	Subscriber Secure Policy Mirroring Examples .....	649
<b>Part 14</b>	<b>Class of Service for Subscriber Access</b>	
Chapter 61	Dynamic CoS for Subscriber Access Overview .....	659
Chapter 62	Configuration Summary of Dynamic CoS for Subscriber Access .....	669
Chapter 63	Configuring Dynamic Shaping and Scheduling for Subscriber Access ...	677
Chapter 64	RADIUS and Dynamic CoS Overview .....	689
Chapter 65	Configuring RADIUS for Dynamic CoS .....	697
Chapter 66	Interface Solutions for Dynamic CoS Overview .....	703
Chapter 67	Configuring Interface Solutions for Dynamic CoS .....	707
Chapter 68	Dynamic CoS for Subscriber Access Examples .....	713
Chapter 69	Bandwidth Management for Dynamic CoS Overview .....	747
Chapter 70	Configuring Bandwidth Management Parameters for Dynamic CoS ....	757
Chapter 71	Bandwidth Management for Dynamic CoS Examples .....	771
<b>Part 15</b>	<b>Protocols for Subscriber Access</b>	
Chapter 72	ANCP Overview .....	781
Chapter 73	Configuring ANCP .....	785
Chapter 74	Dynamic IGMP Configuration Overview .....	797
Chapter 75	Dynamic MLD Configuration Overview .....	799
Chapter 76	Dynamic Router Advertisement Overview .....	801
<b>Part 16</b>	<b>Subscriber Access Examples</b>	
Chapter 77	Service Profile Examples .....	805

Part 17	Complete Configuration Statement Hierarchy and Summary of Statements for Subscriber Access	
Chapter 78	Subscriber Access Statement Hierarchy .....	811
Chapter 79	Subscriber Access Configuration Statements .....	835
Part 18	Index	
	Index .....	1289
	Index of Statements and Commands .....	1319

# Table of Contents

	<b>About This Guide</b> .....	li
	JUNOS Documentation and Release Notes .....	li
	Objectives .....	lii
	Audience .....	lii
	Supported Routing Platforms .....	liii
	Using the Indexes .....	liii
	Using the Examples in This Manual .....	liii
	Merging a Full Example .....	liii
	Merging a Snippet .....	liv
	Documentation Conventions .....	liv
	Documentation Feedback .....	lvi
	Requesting Technical Support .....	lvi
	Self-Help Online Tools and Resources .....	lvii
	Opening a Case with JTAC .....	lvii
<b>Part 1</b>	<b>Managing Access Networks</b>	
<b>Chapter 1</b>	<b>Subscriber Access Overview</b> .....	<b>3</b>
	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 Considerations .....	5
	Platform Support .....	5
	Interface Support .....	6
	DPC Support .....	6
	Subscriber Access Licensing Overview .....	6
	Subscriber Management Unified ISSU Support .....	6
	Verifying and Monitoring Subscriber Management Unified ISSU State .....	7
	Subscriber Access Operation Flow Using DHCP Relay .....	7
	Subscriber Activation and Service Management in an Access Network .....	8
	Components of a Dynamic Profile .....	9
	Router Predefined Variables Used by Dynamic Profiles .....	9
	Configuring Subscriber Access .....	9
	Collecting Subscriber Access Logs Before Contacting Juniper Technical Support .....	12

## Part 2

### Chapter 2

## AAA Service Framework for Subscriber Access

<b>Configuring the AAA Service Framework for Subscriber Access</b> . . . . .	17
AAA Service Framework Overview . . . . .	18
Configuring Router or Switch Interaction with RADIUS Servers . . . . .	20
Configuring Authentication and Accounting Parameters for Subscriber Access . . . . .	21
Specifying the Authentication and Accounting Methods for Subscriber Access . . . . .	21
RADIUS Acct-On and Acct-Off Messages . . . . .	22
RADIUS Accounting Statistics for Subscriber Access Overview . . . . .	23
Configuring Per-Subscriber Session Accounting . . . . .	24
Configuring Per-Service Session Accounting . . . . .	25
Configuring RADIUS Server Parameters for Subscriber Access . . . . .	26
Specifying RADIUS Authentication and Accounting Servers for Subscriber Access . . . . .	27
RADIUS Server Options for Subscriber Access . . . . .	28
Configuring RADIUS Server Options for Subscriber Access . . . . .	29
Configuring How RADIUS Attributes Are Used for Subscriber Access . . . . .	31
Using RADIUS Dynamic Requests for Subscriber Access Management . . . . .	34
Dynamic Service Activation During Login Overview . . . . .	35
RADIUS-Initiated Change of Authorization (CoA) Overview . . . . .	35
CoA Messages . . . . .	36
Qualifications for Change of Authorization . . . . .	36
Message Exchange . . . . .	36
RADIUS-Initiated Disconnect Overview . . . . .	37
Disconnect Messages . . . . .	37
Qualifications for Disconnect . . . . .	37
Message Exchange . . . . .	37
Configuring RADIUS-Initiated Dynamic Request Support . . . . .	38
Verifying and Managing the RADIUS Dynamic-Request Feature . . . . .	38
RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework . . . . .	39
RADIUS IETF Attributes Supported by the AAA Service Framework . . . . .	39
Juniper Networks VSAs Supported by the AAA Service Framework . . . . .	45
DSL Forum Vendor-Specific Attributes . . . . .	50
Error-Cause Codes (RADIUS Attribute 101) for Dynamic Requests . . . . .	52
Configuring an Access Profile for Subscriber Management . . . . .	53
Attaching Access Profiles . . . . .	53
Understanding Session Options for Subscriber Access . . . . .	54
Configuring Subscriber Session Options . . . . .	55
AAA Configuration Testing and Troubleshooting . . . . .	56
Testing a Subscriber AAA Configuration . . . . .	56
Tracing Subscriber Management Database Operations for Subscriber Access . . . . .	58
Configuring the Subscriber Management Database Trace Log Filename . . . . .	59
Configuring the Number and Size of Subscriber Management Database Log Files . . . . .	59
Configuring Access to the Subscriber Management Database Log File . . . . .	59



	Configuring a Regular Expression for Subscriber Management Database to Be Logged . . . . .	60
	Configuring the Subscriber Management Database Tracing Flags . . . . .	60
	Tracing Subscriber Management Session Database Replication Operations for Subscriber Access . . . . .	61
	Configuring the Number and Size of Subscriber Management Session Database Replication Log Files . . . . .	62
	Configuring a Regular Expression for Subscriber Management Session Database Replication to Be Logged . . . . .	63
	Configuring Access to the Subscriber Management Session Database Replication Log File . . . . .	63
	Configuring the Subscriber Management Session Database Replication Trace Log Filename . . . . .	64
	Configuring the Subscriber Management Session Database Replication Tracing Flags . . . . .	64
	Verifying and Managing Subscriber AAA Information . . . . .	65
<b>Chapter 3</b>	<b>Configuring Address-Assignment Pools for Subscriber Access . . . . .</b>	<b>67</b>
	Address-Assignment Pools Overview . . . . .	67
	Configuring Address-Assignment Pools . . . . .	68
	Configuring an Address-Assignment Pool Name and Addresses . . . . .	69
	Configuring a Named Address Range for Dynamic Address Assignment . . . . .	69
	Configuring Address-Assignment Pool Linking . . . . .	70
	Configuring Static Address Assignment . . . . .	71
	Configuring Address-Assignment Pool Usage Threshold Traps . . . . .	71
	Configuring DHCP Client-Specific Attributes . . . . .	72
	DHCP Attributes for Address-Assignment Pools . . . . .	73
	Address-Assignment Pools Licensing Requirements . . . . .	74
	Tracing General Authentication Service Processes . . . . .	74
	Configuring the General Authentication Service Processes Trace Log Filename . . . . .	75
	Configuring the Number and Size of General Authentication Service Processes Log Files . . . . .	75
	Configuring Access to the Log File . . . . .	76
	Configuring a Regular Expression for Lines to Be Logged . . . . .	76
	Configuring the Trace Operation . . . . .	76
<b>Chapter 4</b>	<b>Configuring Domain Maps for Subscriber Access . . . . .</b>	<b>79</b>
	Domain Mapping Overview . . . . .	80
	Default Domain Map . . . . .	80
	Configuring Domain Maps . . . . .	81
	Specifying an Access Profile in a Domain Map . . . . .	82
	Specifying a Dynamic Profile in a Domain Map . . . . .	83
	Specifying an Address Pool in a Domain Map . . . . .	83
	Specifying an AAA Logical System/Routing Instance in a Domain Map . . . . .	84
	Specifying a Target Logical System/Routing Instance in a Domain Map . . . . .	85
	Configuring Domain Name Usage for Domain Maps . . . . .	86
	Specifying Domain Name Delimiters . . . . .	87
	Specifying the Parsing Direction for Domain Names . . . . .	87
	Enabling Domain Name Stripping . . . . .	88

	Specifying a Tunnel Profile in a Domain Map . . . . .	88
	Configuring PADN Parameters for a Domain Map . . . . .	89
	Verifying and Managing Domain Map Configuration . . . . .	89
<b>Chapter 5</b>	<b>AAA and Remote Subscriber Access Configuration Examples . . . . .</b>	<b>91</b>
	Example: Configuring RADIUS-Based Subscriber Authentication and Accounting . . . . .	91
	Example: Configuring an Address-Assignment Pool . . . . .	93
<b>Part 3</b>	<b>DHCP Local Server for Subscriber Access</b>	
<b>Chapter 6</b>	<b>DHCP Local Server Overview . . . . .</b>	<b>97</b>
	Extended DHCP Local Server Overview . . . . .	98
	Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools . . . . .	99
	Providing DHCP Client Configuration Information . . . . .	99
	Minimal Configuration for Clients . . . . .	100
	DHCP Local Server and Address-Assignment Pools . . . . .	100
	DHCPv6 Local Server Overview . . . . .	102
	Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview . . . . .	104
	Multiple DHCP Subscribers Sharing the Same VLAN Logical Interface . . . . .	104
	Primary Dynamic Profile . . . . .	105
<b>Chapter 7</b>	<b>Configuring DHCP Local Server . . . . .</b>	<b>107</b>
	DHCP Duplicate Client Differentiation Using Client Subinterface Overview . . . . .	108
	Guidelines for Configuring Support for DHCP Duplicate Clients . . . . .	109
	Configuring DHCP Duplicate Client Support . . . . .	109
	Using External AAA Authentication Services with DHCP . . . . .	110
	Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use . . . . .	111
	Grouping Interfaces with Common DHCP Configurations . . . . .	112
	Guidelines for Configuring Interface Ranges . . . . .	113
	Group-Specific DHCP Local Server Options . . . . .	115
	Overriding Default DHCP Local Server Configuration Settings . . . . .	115
	Specifying the Maximum Number of DHCP Clients Per Interface . . . . .	116
	Disabling ARP Table Population . . . . .	117
	Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server . . . . .	119
	DHCP Auto Logout Overview . . . . .	120
	Auto Logout Overview . . . . .	120
	How DHCP Identifies and Releases Clients . . . . .	120
	Option 60 and Option 82 Requirements . . . . .	121
	Automatically Logging Out DHCP Clients . . . . .	121
	Deleting DHCP Local Server and DHCP Relay Override Settings . . . . .	122
	Use of DHCP Option 50 and DHCPv6 IA_NA Option to Request a Specific IP Address . . . . .	123
	Subscriber Binding Retention During Interface Delete Events . . . . .	123

	Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events . . . . .	124
	Verifying and Managing the DHCP Maintain Subscribers Feature . . . . .	125
	Attaching Dynamic Profiles to DHCP Subscriber Interfaces . . . . .	125
	Attaching a Dynamic Profile to All DHCP Subscriber Interfaces . . . . .	126
	Attaching a Dynamic Profile to a Group of DHCP Subscriber Interfaces . . . . .	126
	Configuring Passwords for Usernames . . . . .	127
	Creating Unique Usernames for DHCP Clients . . . . .	128
	Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients . . . . .	130
	Default Client/Server Interaction . . . . .	130
	Dynamic Client/Server Interaction for DHCPv4 . . . . .	131
	Dynamic Client/Server Interaction for DHCPv6 . . . . .	131
	Dynamic Configuration Options . . . . .	132
	Configuring Extended DHCP Local Server Dynamic Client Reconfiguration . . . . .	133
	Configuring Dynamic Reconfiguration Attempts for DHCP Clients . . . . .	134
	Configuring Deletion of the Client When Dynamic Reconfiguration Fails . . . . .	135
	Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect . . . . .	136
	Configuring a Token for DHCP Local Server Authentication . . . . .	136
	Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings . . . . .	137
	Verifying and Managing DHCP Local Server Configuration . . . . .	138
	Verifying and Managing DHCPv6 Local Server Configuration . . . . .	138
	Graceful Routing Engine Switchover . . . . .	139
	Tracing Extended DHCP Operations . . . . .	139
	Configuring the Extended DHCP Log Filename . . . . .	140
	Configuring the Number and Size of Extended DHCP Log Files . . . . .	141
	Configuring Access to the Extended DHCP Log File . . . . .	141
	Configuring a Regular Expression for Extended DHCP Lines to Be Logged . . . . .	142
	Configuring the Extended DHCP Tracing Flags . . . . .	142
	Tracing Extended DHCP Operations for Specific Interfaces . . . . .	144
<b>Chapter 8</b>	<b>DHCP Local Server Examples . . . . .</b>	<b>147</b>
	Example: Minimum Extended DHCP Local Server Configuration . . . . .	147
	Example: Extended DHCP Local Server Configuration with Optional Pool Matching . . . . .	147
	Example: Extended DHCPv6 Local Server Configuration . . . . .	148
<b>Part 4</b>	<b>DHCP Relay Agent for Subscriber Access</b>	
<b>Chapter 9</b>	<b>DHCP Relay Agent Overview . . . . .</b>	<b>153</b>
	Extended DHCP Relay Agent Overview . . . . .	154
	Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers . . . . .	154
	DHCP Relay Proxy Overview . . . . .	156
	Interaction Among DHCP Relay Proxy, DHCP Client, and DHCP Servers . . . . .	156
	Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview . . . . .	158
	Multiple DHCP Subscribers Sharing the Same VLAN Logical Interface . . . . .	158
	Primary Dynamic Profile . . . . .	159

<b>Chapter 10</b>	<b>Configuring DHCP Relay Agent</b>	<b>161</b>
	DHCP Duplicate Client Differentiation Using Client Subinterface Overview	162
	Guidelines for Configuring Support for DHCP Duplicate Clients	163
	Configuring DHCP Duplicate Client Support	163
	Using External AAA Authentication Services with DHCP	164
	Grouping Interfaces with Common DHCP Configurations	165
	Guidelines for Configuring Interface Ranges	166
	Group-Specific DHCP Relay Options	167
	Overriding the Default DHCP Relay Configuration Settings	168
	Overwriting giaddr Information	170
	Replacing the DHCP Relay Request and Release Packet Source Address	170
	Overriding Option 82 Information	170
	Using Layer 2 Unicast Transmission for DHCP Packets	171
	Trusting Option 82 Information	172
	Disabling ARP Table Population	172
	Specifying the Maximum Number of DHCP Clients Per Interface	173
	DHCP Snooping Support	174
	Configuring DHCP Snooping for DHCP Relay Agent	175
	Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent	176
	Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent	178
	DHCP Auto Logout Overview	180
	Auto Logout Overview	181
	How DHCP Identifies and Releases Clients	181
	Option 60 and Option 82 Requirements	182
	DHCP Relay Agent Option 82 Value for Auto Logout	182
	Automatically Logging Out DHCP Clients	183
	Sending Release Messages When Clients Are Deleted	184
	Subscriber Binding Retention During Interface Delete Events	185
	Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events	185
	Verifying and Managing the DHCP Maintain Subscribers Feature	186
	Disabling DHCP Relay	187
	Disabling Automatic Binding of Stray DHCP Requests	187
	Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers	189
	Using Matching Option 60 Strings to Process DHCP Client Traffic	189
	Using Nonmatching Option 60 Strings to Process DHCP Client Traffic	192
	Displaying a Count of Discarded DHCP Packets with Option 60 Information	192
	Enabling and Disabling Insertion of Option 82 Information	192
	Configuring Agent Circuit ID Information	193
	Configuring an Option 82 Prefix	193
	Using a Textual Description in Option 82	195
	Configuring Server Groups	195
	Configuring Active Server Groups	196

	Enabling DHCP Relay Proxy Mode . . . . .	196
	Attaching Dynamic Profiles to DHCP Subscriber Interfaces . . . . .	197
	Attaching a Dynamic Profile to All DHCP Subscriber Interfaces . . . . .	197
	Attaching a Dynamic Profile to a Group of DHCP Subscriber Interfaces . . . . .	198
	Verifying and Managing DHCP Relay Configuration . . . . .	198
	Tracing Extended DHCP Operations . . . . .	199
	Configuring the Extended DHCP Log Filename . . . . .	200
	Configuring the Number and Size of Extended DHCP Log Files . . . . .	200
	Configuring Access to the Extended DHCP Log File . . . . .	201
	Configuring a Regular Expression for Extended DHCP Lines to Be Logged . . . . .	201
	Configuring the Extended DHCP Tracing Flags . . . . .	201
	Tracing Extended DHCP Operations for Specific Interfaces . . . . .	203
<b>Chapter 11</b>	<b>Configuring Dynamic Access and Access-Internal Routes for DHCP Subscriber Management . . . . .</b>	<b>205</b>
	Access and Access-Internal Routes for Subscriber Management . . . . .	205
	Configuring Dynamic Access Routes for Subscriber Management . . . . .	206
	Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management . . . . .	207
	Verifying the Configuration of Access and Access-Internal Routes for Subscriber Management . . . . .	208
<b>Chapter 12</b>	<b>DHCP Relay Agent Examples . . . . .</b>	<b>209</b>
	Example: Minimum DHCP Relay Agent Configuration . . . . .	209
	Example: DHCP Relay Agent Configuration with Multiple Clients and Servers . . . . .	209
	Example: Configuring DHCP Snooping Support for DHCP Relay Agent . . . . .	211
	Example: Using Option 60 Strings to Forward DHCP Client Traffic . . . . .	213
	Example: Using Option 60 Strings to Drop DHCP Client Traffic . . . . .	214
<b>Part 5</b>	<b>PPP for Subscriber Access</b>	
<b>Chapter 13</b>	<b>Dynamic Profiles for PPP Overview . . . . .</b>	<b>217</b>
	Dynamic Profiles for PPP Subscriber Interfaces Overview . . . . .	217
<b>Chapter 14</b>	<b>Configuring PPP for Subscriber Access . . . . .</b>	<b>219</b>
	Configuring Dynamic Authentication for PPP Subscribers . . . . .	219
	Access and Access-Internal Routes for Subscriber Management . . . . .	220
	Configuring Dynamic Access Routes for Subscriber Management . . . . .	221
	Configuring Dynamic Access-Internal Routes for PPP Subscriber Management . . . . .	222
	Attaching Dynamic Profiles to Static PPP Subscriber Interfaces . . . . .	223
	Verifying and Managing PPP Configuration for Subscriber Management . . . . .	223
	Verifying the Configuration of Access and Access-Internal Routes for Subscriber Management . . . . .	223

<b>Chapter 15</b>	<b>Configuring Subscriber Services for MLPPP Interfaces . . . . .</b>	<b>225</b>
	Dynamic PPP Subscriber Services for Static MLPPP Interfaces . . . . .	225
	Hardware Requirements for PPP Subscriber Services on Non-Ethernet Interfaces . . . . .	226
	Configuring PPP Subscriber Services for MLPPP Bundles . . . . .	226
	Enabling PPP Subscriber Services for Static Non-Ethernet Interfaces . . . . .	226
	Attaching Dynamic Profiles to MLPPP Bundles . . . . .	227
 <b>Part 6</b>	 <b>L2TP for Subscriber Access</b>	
<b>Chapter 16</b>	<b>L2TP for Subscriber Access Overview . . . . .</b>	<b>231</b>
	L2TP for Subscriber Access Overview . . . . .	231
	L2TP Terminology . . . . .	233
	L2TP Implementation . . . . .	233
	Sequence of Events on the LAC . . . . .	234
	Sequence of Events on the LNS . . . . .	235
	LAC Tunnel Selection Overview . . . . .	235
	Tunnel Selection Failover Between Preference Levels . . . . .	236
	Tunnel Selection Failover Within a Preference Level . . . . .	237
	Tunnel Selection and Maximum Sessions per Tunnel . . . . .	237
	Tunnel Selection with Weighted Load Balancing . . . . .	238
	L2TP Failover and Peer Resynchronization . . . . .	238
	L2TP LAC and Graceful Routing Engine Switchover . . . . .	239
 <b>Chapter 17</b>	 <b>Configuring L2TP for Subscriber Access . . . . .</b>	 <b>241</b>
	Configuring an L2TP LAC . . . . .	241
	Configuring a Tunnel Profile for Subscriber Access . . . . .	242
	Configuring the L2TP LAC Tunnel Selection Parameters . . . . .	244
	Configuring LAC Tunnel Selection Failover Within a Preference Level . . . . .	244
	Configuring Weighted Load Balancing for LAC Tunnel Sessions . . . . .	245
	Preventing the LAC from Sending Calling Number AVP 22 to the LNS . . . . .	246
	Preventing the LAC From Negotiating L2TP Failover Protocol . . . . .	246
	Tracing L2TP Operations for Subscriber Access . . . . .	247
	Configuring the L2TP Trace Log Filename . . . . .	247
	Configuring the Number and Size of L2TP Log Files . . . . .	248
	Configuring Access to the L2TP Log File . . . . .	248
	Configuring a Regular Expression for L2TP LAC to Be Logged . . . . .	249
	Configuring the L2TP Tracing Flags . . . . .	249
	Verifying and Managing L2TP for Subscriber Access . . . . .	250
 <b>Part 7</b>	 <b>Diameter Base Protocol and Applications for Subscriber Access</b>	
<b>Chapter 18</b>	<b>Diameter Base Protocol Overview . . . . .</b>	<b>255</b>
	Diameter Base Protocol Overview . . . . .	255
 <b>Chapter 19</b>	 <b>Configuring Diameter Base Protocol . . . . .</b>	 <b>259</b>
	Configuring Diameter . . . . .	259
	Configuring the Origin Attributes of the Diameter Instance . . . . .	260
	Configuring Diameter Peers . . . . .	260
	Configuring Diameter Network Elements . . . . .	261

	Configuring the Diameter Transport . . . . .	262
	Tracing Diameter Base Protocol Processes for Subscriber Access . . . . .	262
	Configuring the Diameter Base Protocol Trace Log Filename . . . . .	263
	Configuring the Number and Size of Diameter Base Protocol Log Files . . . . .	264
	Configuring Access to the Diameter Base Protocol Log File . . . . .	264
	Configuring a Regular Expression for Diameter Base Protocol Lines to Be Logged . . . . .	265
	Configuring the Diameter Base Protocol Tracing Flags . . . . .	265
	Verifying Diameter Node, Instance, and Route Information . . . . .	266
	Verifying and Managing Diameter Function Information . . . . .	267
	Verifying and Managing Diameter Peer Information . . . . .	268
	Verifying Diameter Network Element Information . . . . .	269
	Troubleshooting Diameter Network Configuration . . . . .	269
	Troubleshooting Diameter Network Connectivity . . . . .	270
<b>Chapter 20</b>	<b>JSRC and Juniper Networks Session Resource Control (SRC)</b>	
	<b>Overview . . . . .</b>	<b>271</b>
	Juniper Networks Session and Resource Control (SRC) and JSRC Overview . . . .	271
	Hardware Requirements for JSRC for Subscriber Access . . . . .	272
	Diameter Messages Exchanged by JSRC and the SAE . . . . .	272
	Understanding Diameter AVPs for JSRC . . . . .	273
	Understanding JSRC-SAE Interactions . . . . .	276
	Subscriber Login . . . . .	276
	Subscriber Service Activation and Deactivation . . . . .	277
	Subscriber Resynchronization . . . . .	277
	Subscriber Session Terminated by the SAE . . . . .	278
	Subscriber Logout . . . . .	278
<b>Chapter 21</b>	<b>Configuring JSRC for Subscriber Access . . . . .</b>	<b>279</b>
	Configuring JSRC . . . . .	279
	Configuring the JSRC Partition . . . . .	280
	Assigning a Partition to JSRC . . . . .	281
	Authorizing Subscribers with JSRC . . . . .	281
	Provisioning Subscribers with JSRC . . . . .	282
<b>Chapter 22</b>	<b>Subscribers on Static Interfaces . . . . .</b>	<b>283</b>
	Subscribers on Static Interfaces Overview . . . . .	283
<b>Chapter 23</b>	<b>Configuring Subscribers over Static Interfaces . . . . .</b>	<b>287</b>
	Configuring Subscribers over Static Interfaces . . . . .	288
	Specifying the Static Subscriber Global Access Profile . . . . .	289
	Specifying the Static Subscriber Global Dynamic Profile . . . . .	289
	Enabling Multiple Subscribers on a VLAN Logical Interface for All Static Subscribers . . . . .	290
	Configuring the Static Subscriber Global Authentication Password . . . . .	290
	Configuring the Static Subscriber Global Username . . . . .	291
	Creating a Static Subscriber Group . . . . .	292
	Specifying the Static Subscriber Group Access Profile . . . . .	293
	Specifying the Static Subscriber Group Dynamic Profile . . . . .	293
	Enabling Multiple Subscribers on a VLAN Logical Interface for a Static Subscriber Group . . . . .	294

	Configuring the Static Subscriber Group Authentication Password . . . . .	294
	Configuring the Static Subscriber Group Username . . . . .	295
	Forcing a Static Subscriber to Be Logged Out . . . . .	296
	Resetting the State of an Interface for Static Subscriber Login . . . . .	296
	Forcing a Group of Static Subscribers to Be Logged Out . . . . .	296
	Resetting the State of an Interface Group for Static Subscriber Login . . . . .	296
	Tracing Static Subscriber Operations . . . . .	297
	Configuring the Static Subscribers Trace Log Filename . . . . .	298
	Configuring the Number and Size of Static Subscribers Log Files . . . . .	298
	Configuring Access to the Static Subscribers Log File . . . . .	298
	Configuring a Regular Expression for Static Subscriber Lines to Be Logged . . . .	299
	Configuring the Static Subscribers Tracing Flags . . . . .	299
<b>Chapter 24</b>	<b>Static Subscribers for Subscriber Access Examples . . . . .</b>	<b>301</b>
	Example: Configuring Static Subscribers for Subscriber Access . . . . .	301
<b>Chapter 25</b>	<b>PTSP and Juniper Networks Session and Resource Control (SRC) . . . .</b>	<b>303</b>
	PTSP Overview . . . . .	303
	Hardware Requirements for PTSP for Subscriber Access . . . . .	304
	Juniper Networks Session and Resource Control (SRC) and PTSP Overview . .	304
	Diameter Messages Exchanged by PTSP and the SAE . . . . .	304
	Understanding Diameter AVPs for PTSP . . . . .	305
	Understanding PTSP-SAE Interactions . . . . .	308
	Packet-Triggered Subscribers Services Overview . . . . .	309
<b>Chapter 26</b>	<b>Configuring the PTSP Application . . . . .</b>	<b>311</b>
	Configuring the PTSP Application . . . . .	311
	Configuring the PTSP Partition . . . . .	312
	Assigning the PTSP Partition . . . . .	312
	Tracing Packet-Triggered Subscriber Operations . . . . .	313
	Configuring the Packet-Triggered Subscribers Trace Log Filename . . . . .	313
	Configuring the Size of Packet-Triggered Subscribers Log Files . . . . .	314
	Configuring the Packet-Triggered Subscribers Tracing Flags . . . . .	314
<b>Chapter 27</b>	<b>Configuring Packet-Triggered Subscriber Services . . . . .</b>	<b>317</b>
	Configuring PTSP . . . . .	317
	Configuring the Multiservices DPC for PTSP . . . . .	318
	Enabling the PTSP Service Package on the Multiservices DPC . . . . .	318
	Configuring Services Interface for PTSP . . . . .	318
	Configuring PTSP Service Rules . . . . .	319
	Configuring Static PTSP Rules . . . . .	319
	Configuring PTSP Rule Sets . . . . .	321
	Configuring PTSP Service Sets . . . . .	322
	Configuring the PTSP Forwarding Instance . . . . .	322
	Configuring a Statistics Profile for PTSP . . . . .	324
	Configuring the File Properties for Statistics Data Output . . . . .	325
	Configuring the Profile Properties for Statistics Data Output . . . . .	325
	Configuring the Record Type for Statistics Data . . . . .	326
	Tracing PTSP Operations . . . . .	326
	Verifying and Managing PTSP Configuration . . . . .	327



<b>Chapter 28</b>	<b>Gx-Plus Overview . . . . .</b>	<b>329</b>
	Gx-Plus for Provisioning Subscribers Overview . . . . .	329
	Diameter Messages Exchanged by Gx-Plus and the PCRF . . . . .	330
	Understanding Diameter AVPs for Gx-Plus . . . . .	332
	Understanding Gx-Plus–PCRF Interactions . . . . .	335
	Subscriber Login . . . . .	336
	Fault Tolerance and Event Notification . . . . .	336
	PCRF-Generated Discovery . . . . .	337
	Subscriber Audit . . . . .	338
	Subscriber Logout . . . . .	338
<b>Chapter 29</b>	<b>Configuring Gx-Plus . . . . .</b>	<b>339</b>
	Configuring Gx-Plus . . . . .	339
	Configuring the Gx-Plus Partition . . . . .	340
	Configuring the Gx-Plus Global Attribute . . . . .	341
	Provisioning Subscribers with Gx-Plus . . . . .	341
<b>Part 8</b>	<b>Mobile IP Access</b>	
<b>Chapter 30</b>	<b>Mobile IP Overview . . . . .</b>	<b>345</b>
	Mobile IP Home Agent Elements and Behavior . . . . .	345
	Mobile IP Registration . . . . .	348
	Home Address Assignment . . . . .	348
	Authentication . . . . .	348
	Reauthentication . . . . .	349
	AAA Authentication . . . . .	349
	Local Authentication . . . . .	350
	Accounting . . . . .	351
	Mobile IP Routing and Forwarding . . . . .	352
	Mobile IP in the WiMAX Environment . . . . .	353
<b>Chapter 31</b>	<b>Configuring Mobile IP . . . . .</b>	<b>357</b>
	Configuring Mobile IP . . . . .	357
	Configuring the Mobile IP Authentication Method . . . . .	358
	Configuring the Mobile IP Home Agent . . . . .	358
	Configuring the Local Authentication Attributes for the Mobile Node . . . . .	359
	Configuring Accounting for Mobile IP Subscribers . . . . .	360
	Configuring Dynamic Home Assignment for the Mobile Node . . . . .	360
	Configuring the Access Type for Mobile IP . . . . .	361
	Tracing Mobile IP Operations for Subscriber Access . . . . .	361
	Configuring the Mobile IP Trace Log Filename . . . . .	363
	Configuring the Number and Size of Mobile IP Log Files . . . . .	363
	Configuring Access to the Mobile IP Log File . . . . .	364
	Configuring a Regular Expression for Mobile IP Lines to Be Logged . . . . .	364
	Configuring the Mobile IP Tracing Flags . . . . .	365

<b>Part 9</b>	<b>Dynamic Profiles for Access and Services</b>	
<b>Chapter 32</b>	<b>Dynamic Profiles Overview</b>	<b>369</b>
	Dynamic Profiles Overview	369
	Dynamic Profile Interface Support	370
	What Dynamic Profiles Do	370
	How Dynamic Profiles Work	370
	Dynamic Profile Semantic Checking	370
	Dynamic Variables Overview	371
	How Dynamic Variables Work	371
	Default Values for Predefined Variables	371
	Junos OS Predefined Variables	372
	Junos OS Predefined Variables That Correspond to RADIUS Attributes and VSAs	385
	User-Defined Variables	389
<b>Chapter 33</b>	<b>Configuring Dynamic Profiles</b>	<b>391</b>
	Configuring a Basic Dynamic Profile	391
	Configuring Predefined Dynamic Variables in Dynamic Profiles	392
	Configuring Default Values for Predefined Variables in a Dynamic Profile	393
	Configuring User-Defined Dynamic Variables in Dynamic Profiles	394
	Configuring a Dynamic Profile for Client Access	395
	Configuring a Dynamic Profile for Various Levels of Services	397
	Modifying Dynamic Profiles	398
<b>Chapter 34</b>	<b>Dynamic Profile Examples</b>	<b>401</b>
	Example: IGMP Dynamic Profile	401
	Example: Firewall Dynamic Profile	402
	Example: Minimum MLPPP Dynamic Profile	402
	Example: Minimum PPPoE Dynamic Profile	403
	Example: Subscriber Secure Policy Dynamic Profile	403
<b>Part 10</b>	<b>Dynamic VLANs</b>	
<b>Chapter 35</b>	<b>Dynamic VLAN Overview</b>	<b>407</b>
	Dynamic 802.1Q VLAN Overview	407
	Static VLAN Configuration	407
	Dynamic VLAN Configuration	407
<b>Chapter 36</b>	<b>Configuring Dynamic VLANs</b>	<b>409</b>
	Configuring VLAN Dynamic Profiles	409
	Configuring a VLAN Dynamic Profile for Creating Single-Tag VLANs Using Standard TPID Values	410
	Configuring a VLAN Dynamic Profile for Creating Single-Tag VLANs Using Any TPID Values	411
	Configuring a Stacked VLAN Dynamic Profile	413
	Configuring a VLAN Dynamic Profile That Associates VLAN Interfaces with Separate Routing Instances	414
	Configuring VLAN Interfaces to Use Dynamic Profiles	416
	Associating a Single-Tag VLAN Dynamic Profile with an Interface	416
	Associating a Stacked VLAN Dynamic Profile with an Interface	416

	Configuring Which VLAN Ethernet Packet Types Dynamic Profiles Can Accept . . . . .	417
	Configuring the VLAN Ethernet Packet Type for Single-Tag VLAN Dynamic Profiles . . . . .	417
	Configuring the VLAN Ethernet Packet Type for Stacked VLAN Dynamic Profiles . . . . .	418
	Configuring an Authentication Password for VLAN or Stacked VLAN Ranges . . . . .	418
	Configuring VLAN Ranges for Use with Dynamic Profiles . . . . .	419
	Configuring Single-Level VLAN Ranges for Use with VLAN Dynamic Profiles . . . . .	419
	Configuring Stacked VLAN Ranges for Use with Stacked VLAN Dynamic Profiles . . . . .	420
	Configuring Dynamic Mixed VLAN Ranges . . . . .	422
	Configuring VLAN Dynamic Profile Override . . . . .	423
	Configuring Dynamic Authentication for VLAN Interfaces . . . . .	424
	Configuring VLAN Interface Username Information for AAA Authentication . . . . .	425
	Verifying and Managing Dynamic VLAN Configuration . . . . .	426
<b>Chapter 37</b>	<b>Dynamic VLAN Examples . . . . .</b>	<b>427</b>
	Example: Configuring a VLAN Dynamic Profile for VLANs with a TPID of 0x8100 . . . . .	427
	Example: Configuring a VLAN Dynamic Profile for VLANs with Any TPID Value and Enabling Demux Interfaces over the VLAN Interface . . . . .	427
	Example: Configuring a Stacked VLAN Dynamic Profile . . . . .	428
	Example: Dynamic VLAN Interface Configuration . . . . .	428
	Example: Dynamic Stacked VLAN Interface Configuration . . . . .	428
	Example: Dynamic Flexible VLAN Interface Configuration . . . . .	429
	Example: Configuring a Flexible VLAN Interface for Use with a Nonstandard Ethertype . . . . .	429
<b>Part 11</b>	<b>Subscriber Interfaces</b>	
<b>Chapter 38</b>	<b>Subscriber Interface Overview . . . . .</b>	<b>433</b>
	Subscriber Interface Overview . . . . .	433
	Statically Identifying Subscribers . . . . .	433
	Dynamically Identifying Subscribers . . . . .	434
	Static Subscriber Interfaces and VLAN Overview . . . . .	434
	Subscriber Interfaces and Demultiplexing Overview . . . . .	435
	Interface Sets of Static Demux Interfaces . . . . .	435
	Dynamic Demultiplexing Interfaces . . . . .	435
	Guidelines for Configuring Demux Interfaces for Subscriber Access . . . . .	436
	MAC Address Validation for Subscriber Interfaces Overview . . . . .	437
	Supported Types of Subscriber Interfaces . . . . .	437
	Trusted Addresses . . . . .	437
	Types of MAC Address Validation . . . . .	437
<b>Chapter 39</b>	<b>Configuring Subscriber Interfaces for Dynamic Profiles . . . . .</b>	<b>439</b>
	Configuring Static Subscriber Interfaces in Dynamic Profiles . . . . .	439
	Configuring a Subscriber Interface with a Static VLAN Interface . . . . .	440
	Configuring Static Subscriber Interfaces Using IP Demux Interfaces . . . . .	440

	Configuring Static Subscriber Interfaces Using VLAN Demux Interfaces . . .	441
	Associating Dynamic Profiles with Statically Created Interfaces . . . . .	441
	Configuring a Subscriber Interface Using a Set of Static IP Demux Interfaces . .	443
	Configuring a Subscriber Interface Using a Set of Static VLAN Demux Interfaces . . . . .	444
	Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles . . . . .	445
	Configuring Dynamic Subscriber Interfaces Using VLAN Demux Interfaces in Dynamic Profiles . . . . .	446
	Configuring MAC Address Validation for Subscriber Interfaces . . . . .	447
	Configuring MAC Address Validation for Static Subscriber Interfaces . . . .	448
	Configuring MAC Address Validation for Dynamic Subscriber Interfaces . .	448
<b>Chapter 40</b>	<b>Subscriber Interface Examples . . . . .</b>	<b>451</b>
	Example: Configuring a Static Subscriber Interface on a Gigabit Ethernet VLAN Interface (Multiple Logical Units) . . . . .	451
	Example: Configuring a Static Subscriber Interface on a Gigabit Ethernet VLAN Interface . . . . .	452
	Example: Configuring a Static Subscriber Interface on a Gigabit Ethernet VLAN Interface (No Autonegotiation) . . . . .	452
	Example: Configuring a Static Subscriber Interface with a Loopback . . . . .	452
	Example: Configuring Dynamic Subscriber Interfaces on IP Demux Interfaces . .	453
	Example: Configuring IPv6 Addressing for a Dynamic IP Demux Interface over Static VLANs . . . . .	455
	Example: Configuring IPv6 Addressing for a Dynamic IP Demux Interface over Dynamic VLANs . . . . .	456
	Example: Configuring a Dynamic IP Demux Interface with Dual Stacking . . . .	459
	Example: Configuring IPv4 Static VLAN Demux Interfaces over a Gigabit Ethernet Underlying Interface with DHCP Local Server . . . . .	462
	Example: Configuring IPv4 Dynamic VLAN Demux Interfaces over a Gigabit Ethernet Underlying Interface with DHCP Local Server . . . . .	464
	Example: Configuring CoS on Static LSQ MLPPP Bundle Interfaces . . . . .	467
<b>Chapter 41</b>	<b>Subscriber Interfaces over Aggregated Ethernet Overview . . . . .</b>	<b>471</b>
	Static and Dynamic VLAN Subscriber Interfaces over Aggregated Ethernet Overview . . . . .	471
	Guidelines for Configuring an Aggregated Ethernet Logical Interface to Support a Static or Dynamic VLAN Subscriber Interface . . . . .	471
	Static or Dynamic Demux Subscriber Interfaces over Aggregated Ethernet Overview . . . . .	472
	Options for Aggregated Ethernet Logical Interfaces That Support Demux Subscriber Interfaces . . . . .	472
	Hardware Requirements with Static or Dynamic Demux Subscriber Interfaces over Aggregated Ethernet . . . . .	473
	Features Supported with Static or Dynamic Demux Subscriber Interfaces over Aggregated Ethernet . . . . .	473
	Distribution of Demux Subscribers in an Aggregated Ethernet Interface . . . .	474
	Distribution Models . . . . .	474
	Sample Targeted Distribution Topology . . . . .	475
	Redundancy and Redistribution Mechanisms . . . . .	475

	Considerations and Best Practices . . . . .	476
<b>Chapter 42</b>	<b>Configuring Subscriber Interfaces over Aggregated Ethernet . . . . .</b>	<b>479</b>
	Configuring a Static or Dynamic VLAN Subscriber Interface over Aggregated Ethernet . . . . .	479
	Configuring a Static or Dynamic IP Demux Subscriber Interface over Aggregated Ethernet . . . . .	481
	Configuring a Static or Dynamic VLAN Demux Subscriber Interface over Aggregated Ethernet . . . . .	482
	Configuring the Distribution Type for Demux Subscribers on Aggregated Ethernet Interfaces . . . . .	484
	Configuring Link and Module Redundancy for Demux Subscribers in an Aggregated Ethernet Interface . . . . .	484
	Configuring Rebalancing of Demux Subscribers in an Aggregated Ethernet Interface . . . . .	485
	Configuring Periodic Rebalancing of Subscribers in an Aggregated Ethernet Interface . . . . .	485
	Configuring Manual Rebalancing of Subscribers on an Aggregated Ethernet Interface . . . . .	485
	Verifying the Distribution of Demux Subscribers in an Aggregated Ethernet Interface . . . . .	486
	Configuring the PPPoE Family for an Underlying Interface . . . . .	486
<b>Chapter 43</b>	<b>Subscriber Interfaces over Aggregated Ethernet Examples . . . . .</b>	<b>489</b>
	Example: Configuring a Static Subscriber Interface on a VLAN Interface over Aggregated Ethernet . . . . .	489
	Example: Configuring a Static Subscriber Interface on an IP Demux Interface over Aggregated Ethernet . . . . .	492
	Example: Configuring a Static Subscriber Interface on a VLAN Interface over Aggregated Ethernet . . . . .	494
	Example: Configuring IPv4 Static VLAN Demux Interfaces over an Aggregated Ethernet Underlying Interface with DHCP Local Server . . . . .	497
	Example: Configuring IPv4 Dynamic VLAN Demux Interfaces over an Aggregated Ethernet Underlying Interface with DHCP Local Server . . . . .	500
	Example: Configuring IPv6 Dynamic VLAN Demux Interfaces over an Aggregated Ethernet Underlying Interface with DHCP Local Server . . . . .	503
	Example: Configuring IPv4 Dynamic Stacked VLAN Demux Interfaces over an Aggregated Ethernet Underlying Interface with DHCP Local Server . . . . .	506
	Example: Configuring a Static PPPoE Subscriber Interface on a Static Underlying VLAN Demux Interface over Aggregated Ethernet . . . . .	509
	Example: Configuring a Dynamic PPPoE Subscriber Interface on a Static Underlying VLAN Demux Interface over Aggregated Ethernet . . . . .	514
	Example: Configuring a Dynamic PPPoE Subscriber Interface on a Dynamic Underlying VLAN Demux Interface over Aggregated Ethernet . . . . .	519
<b>Chapter 44</b>	<b>Dynamic PPPoE Subscriber Interfaces Overview . . . . .</b>	<b>527</b>
	Subscriber Interfaces and PPPoE Overview . . . . .	527
	Benefits of Using Dynamic PPPoE Subscriber Interfaces . . . . .	528
	Supported Platforms for Dynamic PPPoE Subscriber Interfaces . . . . .	529

	Sequence of Operations for PPPoE Subscriber Access . . . . .	529
	Sequence When a PPPoE Subscriber Logs In . . . . .	529
	Sequence When a PPPoE Subscriber Logs Out . . . . .	530
	Dynamic PPPoE Subscriber Interfaces over Static Underlying Interfaces	
	Overview . . . . .	531
	PPPoE Dynamic Profile Configuration . . . . .	531
	PPPoE Underlying Interface Configuration . . . . .	532
	Address Assignment for Dynamic PPPoE Subscriber Interfaces . . . . .	532
	Guidelines for Configuring Dynamic PPPoE Subscriber Interfaces . . . . .	533
<b>Chapter 45</b>	<b>Configuring Dynamic PPPoE Subscriber Interfaces . . . . .</b>	<b>535</b>
	Configuring Dynamic PPPoE Subscriber Interfaces Using Dynamic Profiles . . . .	535
	Configuring a Basic PPPoE Dynamic Profile . . . . .	536
	Configuring a PPPoE Dynamic Profile with Additional Options . . . . .	539
	Configuring an Underlying Interface for Dynamic PPPoE Subscriber	
	Interfaces . . . . .	541
	Assigning a Dynamic Profile and Routing Instance to a Service Name or ACI/ARI	
	Pair for Dynamic PPPoE Interface Creation . . . . .	543
	Verifying and Managing Dynamic PPPoE Configuration . . . . .	544
<b>Chapter 46</b>	<b>Dynamic PPPoE Subscriber Interfaces Examples . . . . .</b>	<b>547</b>
	Example: Configuring a Dynamic PPPoE Subscriber Interface on a Static Gigabit	
	Ethernet VLAN Interface . . . . .	547
	Example: Configuring a PPPoE Service Name Table for Dynamic Subscriber	
	Interface Creation . . . . .	549
	Evaluation Order for Matching Client Information in PPPoE Service Name	
	Tables . . . . .	552
<b>Part 12</b>	<b>Dynamic Firewall Filters, Service Sets and HTTP Redirect for</b>	
	<b>Subscriber Access</b>	
<b>Chapter 47</b>	<b>Dynamic Firewall Filters and Service Sets Overview . . . . .</b>	<b>555</b>
	Dynamic Firewall Filters Overview . . . . .	555
	Classic Filters Overview . . . . .	556
	Classic Filter Types . . . . .	556
	Classic Filter Components . . . . .	557
	Classic Filter Processing . . . . .	557
	Guidelines for Creating and Applying Classic Filters for Subscriber	
	Interfaces . . . . .	558
	Basic Classic Filter Syntax . . . . .	558
	Ascend-Data-Filter Policies for Subscriber Management Overview . . . . .	559
	Filter Naming Conventions . . . . .	560
	Using Multiple Sessions with Ascend-Data-Filters on an Interface . . . . .	560
	Ascend-Data-Filter Attribute Fields . . . . .	561
	Fast Update Filters Overview . . . . .	564
	Fast Update Filter Components . . . . .	565
	Fast Update Filter Processing . . . . .	565
	Fast Update Filter Names . . . . .	566
	Guidelines for Creating and Applying Fast Update Filters . . . . .	566
	Basic Fast Update Filter Syntax . . . . .	567

	Match Conditions and Actions in Fast Update Filters . . . . .	568
	Match Conditions . . . . .	568
	Actions . . . . .	569
	Adding Terms Only Once . . . . .	569
	Dynamic Service Sets Overview . . . . .	569
<b>Chapter 48</b>	<b>Configuring Filters for Dynamic Profiles . . . . .</b>	<b>571</b>
	Dynamically Attaching Statically Created Filters for a Specific Interface Family Type . . . . .	571
	Dynamically Attaching Statically Created Filters for Any Interface Type . . . . .	572
	Dynamically Attaching Filters Using RADIUS Variables . . . . .	573
	Defining Dynamic Filter Processing Order . . . . .	574
	Configuring Firewall Filter Bypass . . . . .	575
	Configuring Service Packet Counting . . . . .	576
	Dynamically Applying Ascend-Data-Filter Policies to Subscriber Sessions . . . . .	577
	Verifying and Managing Dynamic Ascend-Data-Filter Policy Configuration . . . . .	578
<b>Chapter 49</b>	<b>Configuring Fast Update Filters . . . . .</b>	<b>581</b>
	Configuring Fast Update Filters . . . . .	581
	Configuring the Match Order for Fast Update Filters . . . . .	582
	Configuring Terms for Fast Update Filters . . . . .	583
	Fast Update Filter Match Conditions . . . . .	584
	Fast Update Filter Actions and Action Modifiers . . . . .	585
	Configuring Filters to Permit Expected Traffic . . . . .	585
	Avoiding Conflicts When Terms Match . . . . .	586
	How the Router Evaluates Terms in a Filter . . . . .	587
	Using Implied Wildcards . . . . .	588
	Conflict Caused by Overlapping Ranges . . . . .	589
	Associating Fast Update Filters with Interfaces in a Dynamic Profile . . . . .	591
	Verifying and Managing Firewall Filter Configuration . . . . .	592
<b>Chapter 50</b>	<b>Configuring Service Sets in Dynamic Profiles . . . . .</b>	<b>595</b>
	Associating Service Sets with Interfaces in a Dynamic Profile . . . . .	595
	Verifying and Managing Service Sets Information . . . . .	596
<b>Chapter 51</b>	<b>Firewall Filter Examples . . . . .</b>	<b>597</b>
	Examples: Configuring Static Filters . . . . .	597
	Example: Configuring Dynamic Ascend-Data-Filter Support for Subscriber Access . . . . .	600
	Example: Configuring Static Ascend-Data-Filter Support for Subscriber Access . . . . .	603
	Example: Configuring Fast Update Filters for Subscriber Access . . . . .	607
	Example: Bypassing Firewall Filters . . . . .	608
<b>Chapter 52</b>	<b>Redirecting HTTP Requests Overview . . . . .</b>	<b>613</b>
	Redirecting HTTP Requests . . . . .	613
<b>Chapter 53</b>	<b>Configuring HTTP Redirect . . . . .</b>	<b>615</b>
	Configuring HTTP Redirect Services . . . . .	615
	Verifying HTTP Redirect Requests . . . . .	618

<b>Chapter 54</b>	<b>HTTP Redirect Examples . . . . .</b>	<b>619</b>
	Example: Walled Garden as a Service Filter . . . . .	619
	Example: Walled Garden as an HTTP Service Rule . . . . .	620
	Example: HTTP Service Within a Service Set . . . . .	620
	Example: HTTP Service Attached to a Static Interface . . . . .	621
	Example: HTTP Service Attached to a Dynamic Interface . . . . .	621
<b>Part 13</b>	<b>Subscriber Secure Policy Traffic Mirroring</b>	
<b>Chapter 55</b>	<b>Subscriber Secure Policy Overview . . . . .</b>	<b>625</b>
	Subscriber Secure Policy Overview . . . . .	625
	Subscriber Secure Policy Terms . . . . .	626
	Subscriber Secure Policy and L2TP LAC Subscribers . . . . .	627
	Subscriber Secure Policy Licensing Requirements . . . . .	628
	Subscriber Secure Policy Traffic Mirroring Architecture . . . . .	628
	RADIUS-Initiated Traffic Mirroring Process . . . . .	629
	DTCP-Initiated Traffic Mirroring Process . . . . .	630
<b>Chapter 56</b>	<b>Configuring RADIUS-Flow-Tap Service Support for Subscriber Secure Policy Mirroring . . . . .</b>	<b>631</b>
	Guidelines for Configuring Subscriber Secure Policy Mirroring on the RADIUS-Flow-Tap Service . . . . .	631
	Configuring RADIUS-Flow-Tap Service Support for Subscriber Secure Policy Mirroring . . . . .	632
<b>Chapter 57</b>	<b>Configuring RADIUS-Initiated Subscriber Secure Policy Traffic Mirroring . . . . .</b>	<b>635</b>
	Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview . . . . .	635
	RADIUS Attributes Used for Subscriber Secure Policy . . . . .	636
	RADIUS Attributes Used as Traffic Mirroring Triggers . . . . .	637
	RADIUS-Based Mirroring Attributes . . . . .	637
	Considerations When Using RADIUS Attributes for Subscriber Secure Policy . . . . .	638
	Configuring RADIUS Server Support for Subscriber Secure Policy Mirroring . . . . .	639
	Subscriber Secure Policy Mirroring Session Termination . . . . .	639
<b>Chapter 58</b>	<b>Configuring DTCP-Initiated Subscriber Secure Policy Mirroring . . . . .</b>	<b>641</b>
	Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview . . . . .	641
	Configuring DTCP Support for Subscriber Secure Policy Mirroring . . . . .	642
	DTCP Attributes Used for Subscriber Secure Policy . . . . .	644
	DTCP Traffic Mirroring Attributes . . . . .	644
<b>Chapter 59</b>	<b>Subscriber Secure Policy Mirroring and SNMP Traps . . . . .</b>	<b>645</b>
	Subscriber Secure Policy Mirroring and SNMP Traps . . . . .	645
	SNMP Traps for Subscriber Secure Policy LAES Compliance . . . . .	645
	Configuring SNMPv3 Traps for Subscriber Secure Policy Mirroring . . . . .	646
<b>Chapter 60</b>	<b>Subscriber Secure Policy Mirroring Examples . . . . .</b>	<b>649</b>
	Example: Subscriber Secure Policy Mirroring Using RADIUS . . . . .	649
	Example: Subscriber Secure Policy Mirroring Using DTCP . . . . .	651
	Example: Subscriber Secure Policy Dynamic Profile . . . . .	654



	Example: SNMPv3 Traps Configuration for Subscriber Secure Policy Mirroring . . . . .	655
<b>Part 14</b>	<b>Class of Service for Subscriber Access</b>	
<b>Chapter 61</b>	<b>Dynamic CoS for Subscriber Access Overview . . . . .</b>	<b>659</b>
	CoS for Subscriber Access Overview . . . . .	659
	Guidelines for Configuring Dynamic CoS for Subscriber Access . . . . .	660
	Hardware Requirements for Dynamic CoS . . . . .	660
	Configuration Guidelines for Dynamic Scheduling and Queuing . . . . .	663
	Configuration Guidelines for Dynamic Classifiers and Rewrite Rules . . . . .	663
	Configuration Guidelines for Dynamic Excess Bandwidth Distribution . . . . .	666
	Configuration Guidelines for Dynamic CoS on Aggregated Ethernet Interfaces . . . . .	666
	Configuration Guidelines for Dynamic CoS on PPPoE Interfaces . . . . .	666
	Configuration Guidelines for Dynamic CoS on L2TP Interfaces . . . . .	666
	Configuration Guidelines for Dynamic CoS on Interface Sets . . . . .	667
<b>Chapter 62</b>	<b>Configuration Summary of Dynamic CoS for Subscriber Access . . . . .</b>	<b>669</b>
	Configuring Static Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access . . . . .	669
	Configuring Dynamic Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access . . . . .	671
	Configuring Per-Unit Scheduling in a Dynamic Profile for Subscriber Access . . . . .	673
<b>Chapter 63</b>	<b>Configuring Dynamic Shaping and Scheduling for Subscriber Access . . . . .</b>	<b>677</b>
	Configuring Traffic Scheduling and Shaping for Subscriber Access . . . . .	677
	Configuring Static Traffic Shaping and Scheduling Parameters in a Dynamic Profile . . . . .	677
	Configuring Dynamic Traffic Shaping and Scheduling Parameters in a Dynamic Profile . . . . .	678
	Configuring Schedulers in a Dynamic Profile for Subscriber Access . . . . .	679
	Configuring Static Schedulers in a Dynamic Profile . . . . .	680
	Configuring Dynamic Schedulers with Variables in a Dynamic Profile . . . . .	681
	Configuring a Combination of Static and Dynamic Scheduler Parameters in a Scheduler Definition . . . . .	682
	Applying CoS Parameters to a Subscriber Interface in a Dynamic Profile . . . . .	685
	Applying Traffic Shaping and Scheduling to a Subscriber Interface in a Dynamic Profile . . . . .	685
	Applying Minimal Shaping and Scheduling to Remaining Subscriber Traffic . . . . .	685
	Applying a Rewrite Rule Definition to a Subscriber Interface in a Dynamic Profile . . . . .	686
	Applying a Classifier to a Subscriber Interface in a Dynamic Profile . . . . .	687
	Verifying the Scheduling and Shaping Configuration for Subscriber Access . . . . .	688

<b>Chapter 64</b>	<b>RADIUS and Dynamic CoS Overview . . . . .</b>	<b>689</b>
	Subscriber Interfaces That Provide Initial CoS Parameters Dynamically Obtained from RADIUS . . . . .	689
	Dynamic Configuration of Initial CoS in Access Profiles . . . . .	689
	Predefined Variables for Dynamic Configuration of Initial Traffic Shaping . . . . .	690
	Predefined Variables for Dynamic Configuration of Initial Scheduling and Queuing . . . . .	690
	Changing CoS Services Overview . . . . .	693
	Types of CoS Variables Used in a Service Profile . . . . .	693
	Static and Dynamic CoS Configurations . . . . .	693
	Scenarios for Static and Dynamic Configuration of CoS Parameters . . . .	694
<b>Chapter 65</b>	<b>Configuring RADIUS for Dynamic CoS . . . . .</b>	<b>697</b>
	Configuring Initial CoS Parameters Dynamically Obtained from RADIUS . . . .	697
	Configuring User-Defined CoS Variables in a Dynamic Service Profile . . . .	698
<b>Chapter 66</b>	<b>Interface Solutions for Dynamic CoS Overview . . . . .</b>	<b>703</b>
	CoS and Static IP Demux Interface Set Overview . . . . .	703
	CoS for PPPoE Subscriber Interfaces Overview . . . . .	704
	CoS for L2TP Subscriber Interfaces Overview . . . . .	704
	Traffic from LAC to LNS . . . . .	705
	Traffic from LNS to LAC . . . . .	706
<b>Chapter 67</b>	<b>Configuring Interface Solutions for Dynamic CoS . . . . .</b>	<b>707</b>
	Configuring Hierarchical CoS for a Subscriber Interface of Aggregated Ethernet Links . . . . .	707
	Configuring Hierarchical CoS on a Static PPPoE Subscriber Interface . . . . .	708
	Configuring CoS on a Set of Static IP Demux Interfaces . . . . .	709
	Managing the IP Header Values for an L2TP LAC Tunnel with Dynamic CoS . . .	711
	Configuring an Interface Set of Subscribers in a Dynamic Profile . . . . .	712
<b>Chapter 68</b>	<b>Dynamic CoS for Subscriber Access Examples . . . . .</b>	<b>713</b>
	Example: Configuring Static Hierarchical Scheduling and Queuing for Subscriber Access . . . . .	713
	Example: Configuring Dynamic Hierarchical Scheduling and Queuing for Subscriber Access . . . . .	715
	Example: Configuring Initial CoS Parameters Dynamically Obtained from RADIUS . . . . .	721
	Example: Providing Unique Rate Configurations for Schedulers in a Dynamic Profile . . . . .	724
	Example: Configuring Aggregate Scheduling of Queues for Residential Subscribers on Static IP Demux Interfaces . . . . .	725
	Example: Configuring Hierarchical Scheduling and Queuing for a Static PPPoE Subscriber Interface . . . . .	727
	Example: Configuring Hierarchical Scheduling and Queuing for an Underlying Static PPPoE Subscriber Interface . . . . .	729
	Example: Configuring Hierarchical Scheduling and Queuing for an Interface Set of Static PPPoE Subscriber Interfaces . . . . .	731
	Example: Configuring a Dynamic Interface Set of VLAN Subscribers . . . . .	734

<b>Chapter 69</b>	<b>Bandwidth Management for Dynamic CoS Overview . . . . .</b>	<b>747</b>
	Bandwidth Management for Downstream Traffic in Edge Networks	
	Overview . . . . .	747
	Guidelines for Configuring the Shaping Mode . . . . .	747
	Guidelines for Configuring Byte Adjustments . . . . .	748
	Relationship with Other CoS Features . . . . .	748
	Dedicated Queue Scaling for CoS Configurations on Trio MPC/MIC Interfaces	
	Overview . . . . .	749
	Queue Scaling for Trio MPC/MIC Module Combinations . . . . .	749
	Determining Maximum Egress Queues per Port . . . . .	749
	Distribution of Queues on 30-Gigabit Ethernet Queuing MPC Modules . . . . .	750
	Distribution of Queues on 60-Gigabit Ethernet MPC Modules . . . . .	750
	Managing Remaining Queues . . . . .	751
	Hierarchical CoS Shaping-Rate Adjustments Overview . . . . .	752
	CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview . . . . .	753
	Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops . . . . .	754
<b>Chapter 70</b>	<b>Configuring Bandwidth Management Parameters for Dynamic CoS . . . . .</b>	<b>757</b>
	Managing Excess Bandwidth Distribution for Dynamic CoS . . . . .	757
	Configuring Dynamic Shaping Parameters to Account for Overhead in Downstream Traffic Rates . . . . .	758
	Managing Dedicated and Remaining Queues for Dynamic CoS Configurations on Trio MPC/MIC Interfaces . . . . .	759
	Configuring the Maximum Number of Queues for Trio MPC/MIC Interfaces . . . . .	759
	Configuring Remaining Common Queues on Trio MPC/MIC Interfaces . . . . .	760
	Verifying the Number of Dedicated Queues Configured on Trio MPC/MIC Interfaces . . . . .	761
	Providing Accurate Scheduling for a Demux Subscriber Interface of Aggregated Ethernet Links . . . . .	761
	Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops . . . . .	762
	Configuring Static Logical Interface Sets to Serve as CoS Hierarchical Scheduler Nodes for Subscriber Loops . . . . .	763
	Configuring the Logical Interfaces That Compose the Static Logical Interface Sets . . . . .	764
	Configuring Hierarchical CoS on the Static Logical Interface Sets That Serve as Hierarchical Scheduler Nodes for Subscriber Local Loops . . . . .	764
	Configuring ANCP Functionality That Supports and Drives Shaping-Rate Adjustments for Subscriber Local Loops . . . . .	766
	Disabling CoS Shaping-Rate Adjustments for Subscriber Local Loops . . . . .	767
	Disabling Hierarchical Bandwidth Adjustment for Subscriber Interfaces with Reverse-OIF Mapping . . . . .	768
	Verifying the Configuration of Shaping-Rate Adjustments for Subscriber Local Loops . . . . .	768
	Verifying the Configuration of ANCP for Shaping-Rate Adjustments . . . . .	769

<b>Chapter 71</b>	<b>Bandwidth Management for Dynamic CoS Examples . . . . .</b>	<b>771</b>
	Example: Configuring Dynamic Shaping Parameters to Account for Overhead in Downstream Traffic Rates . . . . .	771
	Managing Traffic with Different Encapsulations . . . . .	771
	Managing Downstream Cell-Based Traffic . . . . .	773
	Example: Configuring Hierarchical CoS Shaping-Rate Adjustments for Subscriber Local Loops . . . . .	774
<b>Part 15</b>	<b>Protocols for Subscriber Access</b>	
<b>Chapter 72</b>	<b>ANCP Overview . . . . .</b>	<b>781</b>
	ANCP Topology Discovery and Traffic Monitoring Overview . . . . .	781
<b>Chapter 73</b>	<b>Configuring ANCP . . . . .</b>	<b>785</b>
	Configuring ANCP . . . . .	786
	Configuring ANCP Neighbors . . . . .	786
	Associating an Access Node with Subscribers for ANCP Operations . . . . .	787
	Specifying the Interval Between ANCP Adjacency Messages . . . . .	788
	Specifying the Maximum Number of Discovery Table Entries . . . . .	788
	Configuring ANCP for Backward Compatibility . . . . .	789
	Specifying How Long Processes Wait for ANCP Restart to Complete . . . . .	789
	Configuring ANCP to Adjust CoS Traffic Shaping . . . . .	790
	Verifying and Monitoring ANCP Neighbors . . . . .	790
	Verifying and Monitoring ANCP Subscribers . . . . .	791
	Verifying and Monitoring CoS for ANCP Subscribers . . . . .	791
	Tracing ANCP Operations for Subscriber Access . . . . .	792
	Configuring the ANCP Trace Log Filename . . . . .	792
	Configuring the Number and Size of ANCP Log Files . . . . .	793
	Configuring Access to the ANCP Log File . . . . .	793
	Configuring a Regular Expression for ANCP Lines to Be Logged . . . . .	794
	Configuring the ANCP Tracing Flags . . . . .	794
<b>Chapter 74</b>	<b>Dynamic IGMP Configuration Overview . . . . .</b>	<b>797</b>
	Dynamic IGMP Configuration Overview . . . . .	797
<b>Chapter 75</b>	<b>Dynamic MLD Configuration Overview . . . . .</b>	<b>799</b>
	Dynamic MLD Configuration Overview . . . . .	799
<b>Chapter 76</b>	<b>Dynamic Router Advertisement Overview . . . . .</b>	<b>801</b>
	Dynamic Router Advertisement Configuration Overview . . . . .	801
<b>Part 16</b>	<b>Subscriber Access Examples</b>	
<b>Chapter 77</b>	<b>Service Profile Examples . . . . .</b>	<b>805</b>
	Example: Configuring a Tiered Service Profile for Subscriber Access . . . . .	805

<b>Part 17</b>	<b>Complete Configuration Statement Hierarchy and Summary of Statements for Subscriber Access</b>	
<b>Chapter 78</b>	<b>Subscriber Access Statement Hierarchy</b>	<b>811</b>
	[edit access address-assignment] Hierarchy Level	811
	[edit access domain] Hierarchy Level	812
	[edit access gx-plus] Hierarchy Level	813
	[edit access profile] Hierarchy Level	813
	[edit access tunnel-profile] Hierarchy Level	815
	[edit chassis] Hierarchy Level	816
	[edit diameter] Hierarchy Level	816
	[edit dynamic-profiles] Hierarchy Level	817
	[edit forwarding-options dhcp-relay] Hierarchy Level	822
	[edit jsr] Hierarchy Level	824
	[edit protocols ancp] Hierarchy Level	825
	[edit services captive-portal-content-delivery] Hierarchy Level	825
	[edit services l2tp] Hierarchy Level	826
	[edit services mobile-ip] Hierarchy Level	827
	[edit services radius-flow-tap] Hierarchy Level	828
	[edit system services dhcp-local-server] Hierarchy Level	828
	[edit system services packet-triggered-subscribers] Hierarchy Level	831
	[edit system services static-subscribers] Hierarchy Level	832
	[edit system services subscriber-management] Hierarchy Level	833
<b>Chapter 79</b>	<b>Subscriber Access Configuration Statements</b>	<b>835</b>
	aaa-logical-system (Domain Maps)	835
	aaa-routing-instance (Domain Maps)	836
	abatedUtilization (Address-Assignment Pools)	836
	abatedUtilization-v6 (Address-Assignment Pools)	837
	access	837
	access-concentrator	838
	access-identifier	839
	access-internal	839
	access-profile (Domain Maps)	840
	access-profile (Static Subscribers)	841
	access-type	842
	accounting (Access Profile)	843
	accounting (Dynamic IGMP Interface)	843
	accounting (Dynamic MLD Interface)	844
	accounting-port	844
	accounting-server	845
	accounting-session-id-format	845
	accounting-stop-on-access-deny	846
	accounting-stop-on-failure	846
	active-server-group	847
	address	848
	address (Diameter Peer)	848
	address (Diameter Transport)	849
	address (Tunnel Profile Remote Gateway)	849
	address (Tunnel Profile Source Gateway)	850

address-assignment (Address-Assignment Pools) . . . . .	851
address-pool (Domain Maps) . . . . .	852
adf (Dynamic Firewalls) . . . . .	853
adjacency-timer . . . . .	854
aggregate-clients (DHCP Local Server) . . . . .	855
aggregate-clients (DHCP Relay Agent) . . . . .	856
aggregate-clients (Static Subscribers) . . . . .	857
algorithm . . . . .	858
allow-snooped-clients . . . . .	859
always-write-giaddr . . . . .	860
always-write-option-82 . . . . .	861
ancp . . . . .	862
application . . . . .	863
attempts (DHCP Local Server) . . . . .	864
attribute . . . . .	865
attributes . . . . .	866
authenticate . . . . .	867
authentication (DHCP Local Server) . . . . .	868
authentication (DHCP Relay Agent) . . . . .	869
authentication (Static Subscribers) . . . . .	870
authentication-order . . . . .	871
authentication-server . . . . .	872
authorization-order . . . . .	872
autonomous (Dynamic Router Advertisement) . . . . .	873
boot-file . . . . .	873
boot-server . . . . .	874
buffer-size (Dynamic Scheduling) . . . . .	875
captive-portal-content-delivery . . . . .	876
captive-portal-content-delivery-rule . . . . .	877
captive-portal-content-delivery-rule-set . . . . .	877
chap (Dynamic PPP) . . . . .	878
circuit-id (Address-Assignment Pools) . . . . .	878
circuit-id (DHCP Relay Agent) . . . . .	879
circuit-type (DHCP Local Server) . . . . .	880
circuit-type (DHCP Relay Agent) . . . . .	881
class-of-service (Dynamic Profiles) . . . . .	882
classifiers (Dynamic CoS Application) . . . . .	882
clear-on-abort (DHCP Local Server) . . . . .	883
client-accounting-algorithm . . . . .	884
client-authentication-algorithm . . . . .	884
client-discover-match (DHCP Local Server) . . . . .	885
client-discover-match (DHCP Relay Agent) . . . . .	886
client-id . . . . .	887
client-idle-timeout . . . . .	888
client-session-timeout . . . . .	889
coa-immediate-update . . . . .	889
connect-actively . . . . .	890
current-hop-limit (Dynamic Router Advertisement) . . . . .	890
database-replication (Subscriber Session Database) . . . . .	891

default-lifetime (Dynamic Router Advertisement) . . . . .	891
default-local-server-group . . . . .	892
default-relay-server-group . . . . .	893
default-value . . . . .	894
delay-buffer-rate (Dynamic Traffic Shaping) . . . . .	894
delimiter (DHCP Local Server) . . . . .	895
delimiter (DHCP Relay Agent) . . . . .	896
delimiter (Domain Maps) . . . . .	897
demux0 (Dynamic Interface) . . . . .	898
demux-options . . . . .	899
demux-source (Dynamic IP Demux Interface) . . . . .	900
demux-source (Dynamic Underlying Interface) . . . . .	901
destination (Diameter Network Element) . . . . .	901
destination (Dynamic PPPoE) . . . . .	902
destination-address . . . . .	902
destination-host . . . . .	903
destination-host (Gx-Plus) . . . . .	903
destination-host (PTSP) . . . . .	904
destination-prefix-list . . . . .	904
destination-realm (Gx-Plus) . . . . .	905
destination-realm (JSRC) . . . . .	905
destination-realm (PTSP) . . . . .	906
dhcp-attributes (Address-Assignment Pools) . . . . .	907
dhcp-local-server . . . . .	908
dhcp-relay . . . . .	911
dhcpv6 . . . . .	914
diameter . . . . .	916
diameter-instance (Gx-Plus) . . . . .	917
diameter-instance (JSRC) . . . . .	917
diameter-instance (PTSP) . . . . .	918
disable (Dynamic IGMP) . . . . .	918
disable (Dynamic MLD) . . . . .	919
disable-calling-number-avp (L2TP LAC) . . . . .	919
disable-failover-protocol (L2TP LAC) . . . . .	920
disable-relay . . . . .	920
dns-server . . . . .	921
domain (Domain Maps) . . . . .	922
domain-name (Address-Assignment Pools) . . . . .	923
domain-name (DHCP Local Server) . . . . .	924
domain-name (DHCP Relay Agent) . . . . .	925
domain-name (Static Subscribers) . . . . .	926
drop . . . . .	927
drop-profile (Dynamic Schedulers) . . . . .	929
drop-profile-map (Dynamic Schedulers) . . . . .	930
dscp (Dynamic Classifiers) . . . . .	931
dscp (Dynamic Rewrite Rules) . . . . .	932
dscp-ipv6 (Dynamic Classifiers) . . . . .	933
dscp-ipv6 (Dynamic Rewrite Rules) . . . . .	933
duplicate-clients-on-interface (DHCP Local Server) . . . . .	934

duplicate-clients-on-interface (DHCP Relay Agent) . . . . .	934
duplicate-protection (Dynamic PPPoE) . . . . .	935
dynamic-home-assignment . . . . .	936
dynamic-profile (DHCP Local Server) . . . . .	937
dynamic-profile (DHCP Relay Agent) . . . . .	938
dynamic-profile (Domain Maps) . . . . .	938
dynamic-profile (Dynamic PPPoE) . . . . .	939
dynamic-profile (PPP) . . . . .	940
dynamic-profile (PPPoE Service Name Tables) . . . . .	941
dynamic-profile (Static Subscribers) . . . . .	942
dynamic-profiles . . . . .	943
enable-service . . . . .	947
encapsulation (Dynamic Interfaces) . . . . .	948
entity-type . . . . .	951
ethernet-port-type-virtual . . . . .	951
excess-priority (Dynamic Schedulers) . . . . .	952
excess-rate (Dynamic Schedulers) . . . . .	952
excess-rate (Dynamic Traffic Shaping) . . . . .	953
exclude . . . . .	954
exclude (Dynamic MLD Interface) . . . . .	956
external-authority . . . . .	956
fail-over-within-preference (L2TP LAC) . . . . .	957
family (Address-Assignment Pools) . . . . .	958
family (Dynamic Firewalls) . . . . .	959
family (Dynamic Demux Interface) . . . . .	960
family (Dynamic PPPoE) . . . . .	961
family (Dynamic Standard Interface) . . . . .	962
fast-update-filter (Dynamic Firewalls) . . . . .	964
filter (Dynamic Firewalls) . . . . .	965
firewall (Dynamic Firewalls) . . . . .	966
forward-snooped-clients (DHCP Local Server) . . . . .	967
forward-snooped-clients (DHCP Relay Agent) . . . . .	968
forwarding (Diameter Network Element) . . . . .	969
forwarding-class (Dynamic Scheduler Maps) . . . . .	969
forwarding-class (Subscriber Secure Policy) . . . . .	970
from . . . . .	970
function (Diameter Network Element) . . . . .	971
function (Diameter Route) . . . . .	972
gateway-name (Tunnel Profile Remote Gateway) . . . . .	972
gateway-name (Tunnel Profile Source Gateway) . . . . .	973
generic . . . . .	973
global (Gx-Plus) . . . . .	974
grace-period . . . . .	974
group (DHCP Local Server) . . . . .	975
group (DHCP Relay Agent) . . . . .	977
group (Dynamic IGMP Interface) . . . . .	979
group (Dynamic MLD Interface) . . . . .	980
group (Static Subscribers) . . . . .	981
group-count (Dynamic MLD Interface) . . . . .	982



group-increment (Dynamic MLD Interface) . . . . .	982
group-limit (Dynamic IGMP Interface) . . . . .	983
group-limit (Dynamic MLD Interface) . . . . .	984
group-policy (Dynamic IGMP Interface) . . . . .	985
group-policy (Dynamic MLD Interface) . . . . .	985
guaranteed-rate (Dynamic Traffic Shaping) . . . . .	986
gx-plus (Gx-Plus) . . . . .	987
hardware-address . . . . .	987
highUtilization (Address-Assignment Pools) . . . . .	988
highUtilization-v6 (Address-Assignment Pools) . . . . .	988
home-agent (Mobile IP Dynamic Assignment) . . . . .	989
home-agent (Mobile IP Network Address Identifier) . . . . .	990
home-agent (Mobile IP Networks) . . . . .	991
home-agent-address . . . . .	992
host (Address-Assignment Pools) . . . . .	993
host (Diameter Origin) . . . . .	993
identification (Tunnel Profile) . . . . .	994
ieee-802.1 (Dynamic Classifiers) . . . . .	994
ieee-802.1 (Dynamic Rewrite Rules) . . . . .	995
ietf-mode . . . . .	995
igmp (Dynamic Profiles) . . . . .	996
ignore . . . . .	997
immediate-leave (Dynamic IGMP Interface) . . . . .	998
immediate-leave (Dynamic MLD Interface) . . . . .	999
immediate-update . . . . .	1000
inet-precedence (Dynamic Classifiers) . . . . .	1000
inet-precedence (Dynamic Rewrite Rules) . . . . .	1001
inner-tag-protocol-id (Dynamic VLANs) . . . . .	1001
inner-vlan-id (Dynamic VLANs) . . . . .	1002
input (Dynamic Service Sets) . . . . .	1003
input-vlan-map (Dynamic Interfaces) . . . . .	1004
interface (DHCP Local Server) . . . . .	1005
interface (DHCP Relay Agent) . . . . .	1007
interface (Dynamic IGMP) . . . . .	1009
interface (Dynamic Interface Sets) . . . . .	1010
interface (Dynamic MLD) . . . . .	1011
interface (Dynamic Profiles) . . . . .	1012
interface (Dynamic Router Advertisement) . . . . .	1013
interface (Dynamic Routing Options) . . . . .	1014
interface (Static Subscriber Group) . . . . .	1015
interface (Static Subscriber Username) . . . . .	1016
interface-client-limit (DHCP Local Server) . . . . .	1017
interface-client-limit (DHCP Relay Agent) . . . . .	1018
interface-delete (Subscriber Management) . . . . .	1019
interface-description-format . . . . .	1019
interface-set (Dynamic CoS) . . . . .	1020
interface-traceoptions (DHCP Local Server) . . . . .	1021
interface-traceoptions (DHCP Relay Agent) . . . . .	1023
interfaces (Subscriber Secure Policy) . . . . .	1024

interfaces (ANCP) .....	1025
interfaces (Dynamic CoS Definition) .....	1026
interfaces (Static and Dynamic Subscribers) .....	1027
interface-set .....	1030
interface-specific (Dynamic Firewalls) .....	1031
ip-address .....	1031
ip-address-first .....	1032
jsrc (JSRC) .....	1033
jsrc-partition .....	1033
keepalives (Dynamic Profiles) .....	1034
key .....	1035
layer2-unicast-replies .....	1036
link (Address-Assignment Pools) .....	1037
local-server-group .....	1038
logical-interface-fpc-redundancy (Aggregated Ethernet Subscriber Interfaces) .....	1039
logical-system (Diameter Peer) .....	1039
logical-system (Diameter Transport) .....	1040
logical-system (Tunnel Profile) .....	1040
logical-system-name (DHCP Local Server) .....	1041
logical-system-name (DHCP Relay Agent) .....	1042
logical-system-name (Static Subscribers) .....	1043
loss-priority (Dynamic Schedulers) .....	1044
mac-address (DHCP Local Server) .....	1045
mac-address (DHCP Relay Agent) .....	1046
mac-address (Dynamic Access-Internal Routes) .....	1047
mac-validate (Dynamic IP Demux Interface) .....	1048
maintain-subscriber (Subscriber Management) .....	1048
managed-configuration (Dynamic Router Advertisement) .....	1049
mandatory .....	1049
map (Domain Maps) .....	1050
match-direction .....	1051
mask (Domain Maps) .....	1051
match-order (Dynamic Firewalls) .....	1052
max-advertisement-interval (Dynamic Router Advertisement) .....	1053
maximum-discovery-table-entries .....	1053
maximum-helper-restart-time .....	1054
maximum-lease-time .....	1054
max-outstanding-requests (Gx-Plus) .....	1055
max-sessions (Dynamic PPPoE) .....	1056
max-sessions (PPPoE Service Name Tables) .....	1057
max-sessions (Tunnel Profile) .....	1058
medium (Tunnel Profile) .....	1058
metric (Dynamic Access-Internal Routes) .....	1059
metric (Diameter Route) .....	1059
metric (Domain Maps) .....	1060
min-advertisement-interval (Dynamic Router Advertisement) .....	1060
mld (Dynamic Profiles) .....	1061
mobile-ip .....	1062

mode	1063
multicast (Dynamic Routing Options)	1064
nai	1065
name-server	1066
nas-identifier	1066
nas-port-extended-format	1067
neighbor (Associate with Access Identifier)	1068
neighbor (Define)	1068
neighbor-discovery-router-advertisement (Address-Assignment Pools)	1069
netbios-node-type	1069
network	1070
network-element (Diameter Base Protocol)	1071
next-hop (Dynamic Access-Internal Routes)	1072
no-accounting	1072
no-allow-snooped-clients	1073
no-arp (DHCP Local Server)	1074
no-arp (DHCP Relay Agent)	1075
no-bind-on-request (DHCP Relay Agent)	1076
no-keepalives (Dynamic Profiles)	1077
no-qos-adjust (Dynamic Routing Options)	1077
oif-map (Dynamic IGMP Interface)	1078
oif-map (Dynamic MLD Interface)	1078
on-link (Dynamic Router Advertisement)	1079
option	1080
option-60 (DHCP Local Server)	1081
option-60 (DHCP Relay Agent)	1082
option-82 (Address-Assignment Pools)	1083
option-82 (DHCP Local Server Authentication)	1084
option-82 (DHCP Local Server Pool Matching)	1085
option-82 (DHCP Relay Agent)	1086
option-match	1087
options	1088
order	1089
order (Mobile IP)	1090
origin (Diameter Base Protocol)	1091
other-stateful-configuration (Dynamic Router Advertisement)	1091
output (Dynamic Service Sets)	1092
output-traffic-control-profile (Dynamic CoS Definition)	1092
output-vlan-map (Dynamic Interfaces)	1093
overhead-accounting (Dynamic Traffic Shaping)	1094
overrides (DHCP Local Server)	1095
overrides (DHCP Relay Agent)	1097
packet-triggered-subscribers	1098
packet-triggered-subscribers-partition	1099
padn (Domain Maps)	1099
pap (Dynamic PPP)	1100
parse-direction (Domain Maps)	1100
partition	1101
partition (Gx-Plus)	1101

partition (PTSP) .....	1102
passive (Dynamic IGMP Interface) .....	1103
passive (Dynamic MLD Interface) .....	1104
password (DHCP Local Server) .....	1105
password (DHCP Relay Agent) .....	1106
password (Static Subscribers) .....	1107
peer .....	1108
peer (Diameter Base Protocol) .....	1109
peer (Diameter Network Element) .....	1109
pool (Address-Assignment Pools) .....	1110
pool-match-order .....	1111
pop (Dynamic VLANs) .....	1111
port .....	1112
port (Diameter Peer) .....	1112
post-service-filter (Dynamic Service Sets) .....	1113
pp0 (Dynamic PPPoE) .....	1114
pppoe-options (Dynamic PPPoE) .....	1115
pppoe-underlying-options (Static and Dynamic Subscribers) .....	1116
ppp-options (Dynamic PPP) .....	1117
ppp-subscriber-services .....	1118
precedence .....	1119
predefined-variable-defaults (Dynamic Profiles) .....	1120
preference .....	1120
preference (Tunnel Profile) .....	1121
preferred-lifetime (Dynamic Router Advertisement) .....	1121
prefix (Address-Assignment Pools) .....	1122
prefix (DHCP Relay Agent) .....	1123
prefix (Dynamic Router Advertisement) .....	1124
pre-ietf-mode .....	1125
priority (Diameter Peer) .....	1125
priority (Dynamic Schedulers) .....	1126
profile .....	1127
promiscuous-mode .....	1130
protocol (Dynamic Schedulers) .....	1130
protocols (Dynamic Profiles) .....	1131
provisioning-order .....	1133
proxy-arp .....	1133
proxy-mode .....	1134
push (Dynamic VLANs) .....	1135
qos-adjust .....	1135
qualified-next-hop .....	1136
radius (Access Profile) .....	1137
radius (Dynamic Profiles) .....	1138
radius-disconnect (DHCP Local Server) .....	1139
radius-flow-tap .....	1140
radius-server .....	1141
range (Address-Assignment Pools) .....	1142
reachable-time (Dynamic Router Advertisement) .....	1143
rebalance-periodic (Aggregated Ethernet Subscriber Interfaces) .....	1143

realm (Diameter Origin) .....	1144
reconfigure (DHCP Local Server) .....	1145
registration-lifetime .....	1146
relay-agent-interface-id .....	1147
relay-agent-remote-id .....	1148
relay-agent-subscriber-id .....	1149
relay-option-60 .....	1150
relay-option-82 .....	1151
relay-server-group .....	1152
remote-gateway (Tunnel Profile) .....	1153
remote-id .....	1153
replace-ip-source-with .....	1154
replay-method .....	1155
retransmit-timer (Dynamic Router Advertisement) .....	1156
retry .....	1156
revert-interval .....	1157
revocation-required .....	1158
rewrite-rules (Dynamic CoS Interfaces) .....	1159
route (Access) .....	1160
route (Access Internal) .....	1161
route (Diameter Network Element) .....	1162
router (Address-Assignment Pools) .....	1162
router-advertisement (Dynamic Profiles) .....	1163
routing-instance .....	1163
routing-instance (Diameter Peer) .....	1164
routing-instance (Diameter Transport) .....	1164
routing-instance (Tunnel Profile) .....	1165
routing-instance (PPPoE Service Name Tables) .....	1166
routing-instance-name (DHCP Local Server) .....	1167
routing-instance-name (DHCP Relay Agent) .....	1168
routing-instance-name (Static Subscribers) .....	1169
routing-instances .....	1170
routing-options (Dynamic Profiles) .....	1171
rpf-check (Dynamic Profiles) .....	1172
rule .....	1173
rule-set .....	1174
scheduler (Dynamic Scheduler Maps) .....	1174
scheduler-map (Dynamic Traffic Shaping) .....	1175
scheduler-maps (Dynamic CoS Definition) .....	1176
schedulers (Dynamic CoS Definition) .....	1177
secret .....	1178
secret (Tunnel Profile) .....	1178
send-release-on-delete (DHCP Relay Agent) .....	1179
server (Dynamic PPPoE) .....	1179
server-group .....	1180
server-identifier (Address-Assignment Pools) .....	1180
service (Dynamic Service Sets) .....	1181
service-filter (Dynamic Service Sets) .....	1182
service-name-table .....	1183

service-set (Dynamic Service Sets) . . . . .	1184
services . . . . .	1185
session-options . . . . .	1185
shaping-rate (Dynamic Traffic Shaping and Scheduling) . . . . .	1186
sip-server-address . . . . .	1187
sip-server-domain-name . . . . .	1187
source (Dynamic IGMP Interface) . . . . .	1188
source (Dynamic MLD Interface) . . . . .	1188
source-address . . . . .	1189
source-count (Dynamic MLD Interface) . . . . .	1189
source-gateway (Tunnel Profile) . . . . .	1190
source-increment (Dynamic MLD Interface) . . . . .	1190
source-ipv4-address . . . . .	1191
spi . . . . .	1192
ssm-map (Dynamic IGMP Interface) . . . . .	1193
ssm-map (Dynamic MLD Interface) . . . . .	1193
static (Dynamic IGMP Interface) . . . . .	1194
static (Dynamic MLD Interface) . . . . .	1195
static-subscribers . . . . .	1196
statistics . . . . .	1197
strict (DHCP Local Server) . . . . .	1198
strip-domain (Domain Maps) . . . . .	1198
subscriber-management (Subscriber Management) . . . . .	1199
swap (Dynamic VLANs) . . . . .	1199
tag (Access) . . . . .	1200
tag (Dynamic Profiles) . . . . .	1200
tag-protocol-id (Dynamic VLANs) . . . . .	1201
target-logical-system (Domain Maps) . . . . .	1202
target-routing-instance (Domain Maps) . . . . .	1203
targeted-distribution (Demux Interfaces over Aggregated Ethernet) . . . . .	1203
term . . . . .	1204
term (Captive Portal Content Delivery) . . . . .	1205
tftp-server . . . . .	1205
then . . . . .	1206
timeout (DHCP Local Server) . . . . .	1207
timeout (RADIUS) . . . . .	1208
timestamp-tolerance . . . . .	1209
token (DHCP Local Server) . . . . .	1210
trace (DHCP Local Server) . . . . .	1211
trace (DHCP Relay Agent) . . . . .	1212
traceoptions (General Authentication Service) . . . . .	1213
traceoptions (ANCP) . . . . .	1215
traceoptions (Captive Portal Content Delivery) . . . . .	1217
traceoptions (DHCP Local Server) . . . . .	1219
traceoptions (DHCP Relay Agent) . . . . .	1221
traceoptions (Diameter Base Protocol) . . . . .	1223
traceoptions (L2TP) . . . . .	1225
traceoptions (Mobile IP) . . . . .	1229
traceoptions (PTSP) . . . . .	1232

traceoptions (Static Subscribers) . . . . .	1234
traceoptions (Subscriber Management) . . . . .	1236
traceoptions (Subscriber Session Database Replication) . . . . .	1238
traffic-control-profiles (Dynamic CoS Definition) . . . . .	1240
transmit-rate (Dynamic Schedulers) . . . . .	1241
transport (Diameter Base Protocol) . . . . .	1242
transport (Diameter Peer) . . . . .	1242
trigger (DHCP Local Server) . . . . .	1243
trust-option-82 . . . . .	1244
tunnel (Tunnel Profile) . . . . .	1245
tunnel-profile (Domain Maps) . . . . .	1246
tunnel-profile (Tunnel Profile) . . . . .	1247
type (Tunnel Profile) . . . . .	1248
underlying-interface (demux0) . . . . .	1249
underlying-interface (Dynamic PPPoE) . . . . .	1250
unit (Dynamic Demux Interface) . . . . .	1251
unit (Dynamic PPPoE) . . . . .	1253
unit (Dynamic Traffic Shaping) . . . . .	1255
unit (Dynamic Profiles Standard Interface) . . . . .	1257
unnumbered-address (Dynamic Profiles) . . . . .	1259
unnumbered-address (Dynamic PPPoE) . . . . .	1260
update-interval . . . . .	1260
use-interface-description . . . . .	1261
use-primary (DHCP Local Server) . . . . .	1262
use-primary (DHCP Relay Agent) . . . . .	1263
user-prefix (DHCP Local Server) . . . . .	1264
user-prefix (DHCP Relay Agent) . . . . .	1265
user-prefix (Static Subscribers) . . . . .	1266
username-include (DHCP Local Server) . . . . .	1267
username-include (DHCP Relay Agent) . . . . .	1269
username-include (Static Subscribers) . . . . .	1270
valid-lifetime (Dynamic Router Advertisement) . . . . .	1271
variables . . . . .	1272
vendor-id . . . . .	1273
vendor-option . . . . .	1274
version (Dynamic IGMP Interface) . . . . .	1275
version (Dynamic MLD Interface) . . . . .	1276
virtual-network . . . . .	1277
vlan-id (Dynamic Profiles) . . . . .	1278
vlan-id (Dynamic VLANs) . . . . .	1279
vlan-nas-port-stacked-format . . . . .	1279
vlan-tag (Dynamic Classifiers) . . . . .	1280
vlan-tag (Dynamic Rewrite Rules) . . . . .	1281
vlan-tagging . . . . .	1282
vlan-tags . . . . .	1283
weighted-load-balancing (L2TP LAC) . . . . .	1284
wimax . . . . .	1284
wins-server . . . . .	1285

## Part 18

## Index

Index .....	1289
Index of Statements and Commands .....	1319



# List of Figures

<b>Part 1</b>	<b>Managing Access Networks</b>	
<b>Chapter 1</b>	<b>Subscriber Access Overview</b> . . . . .	<b>3</b>
	Figure 1: Subscriber Access Network Example . . . . .	5
	Figure 2: Subscriber Access Operation Flow . . . . .	8
	Figure 3: Subscriber Access Configuration Workflow . . . . .	11
<b>Part 6</b>	<b>L2TP for Subscriber Access</b>	
<b>Chapter 16</b>	<b>L2TP for Subscriber Access Overview</b> . . . . .	<b>231</b>
	Figure 4: Simple L2TP Topology . . . . .	231
	Figure 5: Protocol Stacking for L2TP Subscribers in Pass-Through Mode . . . . .	232
<b>Part 8</b>	<b>Mobile IP Access</b>	
<b>Chapter 30</b>	<b>Mobile IP Overview</b> . . . . .	<b>345</b>
	Figure 6: Mobile IP Network Without Reverse Tunneling . . . . .	346
	Figure 7: Mobile IP Network with Reverse Tunneling . . . . .	347
	Figure 8: Sample Mobile IP WiMAX Topology . . . . .	355
<b>Part 11</b>	<b>Subscriber Interfaces</b>	
<b>Chapter 38</b>	<b>Subscriber Interface Overview</b> . . . . .	<b>433</b>
	Figure 9: VLAN Subscriber Interfaces . . . . .	434
	Figure 10: IP Demux Subscriber Interface . . . . .	435
<b>Chapter 41</b>	<b>Subscriber Interfaces over Aggregated Ethernet Overview</b> . . . . .	<b>471</b>
	Figure 11: Targeted Subscriber Links . . . . .	475
<b>Part 12</b>	<b>Dynamic Firewall Filters, Service Sets and HTTP Redirect for Subscriber Access</b>	
<b>Chapter 51</b>	<b>Firewall Filter Examples</b> . . . . .	<b>597</b>
	Figure 12: Logical Flow Example for Filter Bypass Processing . . . . .	608
<b>Part 13</b>	<b>Subscriber Secure Policy Traffic Mirroring</b>	
<b>Chapter 55</b>	<b>Subscriber Secure Policy Overview</b> . . . . .	<b>625</b>
	Figure 13: RADIUS-Initiated Subscriber Secure Policy Architecture . . . . .	628
<b>Part 14</b>	<b>Class of Service for Subscriber Access</b>	
<b>Chapter 66</b>	<b>Interface Solutions for Dynamic CoS Overview</b> . . . . .	<b>703</b>

	Figure 14: CoS Configuration for Simple L2TP Topology . . . . .	705
<b>Chapter 69</b>	<b>Bandwidth Management for Dynamic CoS Overview . . . . .</b>	<b>747</b>
	Figure 15: Distribution of Queues on the 30-Gigabit Ethernet Queuing MPC Module . . . . .	750
	Figure 16: Distribution of Queues on the 60-Gigabit Ethernet Enhanced Queuing MPC . . . . .	751
<b>Chapter 71</b>	<b>Bandwidth Management for Dynamic CoS Examples . . . . .</b>	<b>771</b>
	Figure 17: Sample Network Topology for Downstream Traffic . . . . .	771

# List of Tables

	<b>About This Guide</b> . . . . .	<b>li</b>
	Table 1: Notice Icons . . . . .	lv
	Table 2: Text and Syntax Conventions . . . . .	lv
<b>Part 1</b>	<b>Managing Access Networks</b>	
<b>Chapter 1</b>	<b>Subscriber Access Overview</b> . . . . .	<b>3</b>
	Table 3: Subscriber Access Terms and Acronyms . . . . .	4
<b>Part 2</b>	<b>AAA Service Framework for Subscriber Access</b>	
<b>Chapter 2</b>	<b>Configuring the AAA Service Framework for Subscriber Access</b> . . . . .	<b>17</b>
	Table 4: RADIUS Attributes and VSAs Used for Per-Subscriber Session Accounting . . . . .	23
	Table 5: Juniper Network VSAs Used for Per-Service Session Accounting . . . . .	26
	Table 6: Attributes That Can Be Ignored in RADIUS Accept-Accept Messages . . . . .	31
	Table 7: Attributes That Can Be Excluded from RADIUS Messages . . . . .	32
	Table 8: Supported RADIUS IETF Attributes . . . . .	39
	Table 9: Supported Juniper Networks VSAs . . . . .	45
	Table 10: DSL Forum VSAs . . . . .	51
	Table 11: Error-Cause Codes (RADIUS Attribute 101) . . . . .	52
<b>Chapter 3</b>	<b>Configuring Address-Assignment Pools for Subscriber Access</b> . . . . .	<b>67</b>
	Table 12: DHCP Attributes . . . . .	73
	Table 13: DHCPv6 Attributes . . . . .	73
<b>Chapter 4</b>	<b>Configuring Domain Maps for Subscriber Access</b> . . . . .	<b>79</b>
	Table 14: Domain Map Options and Parameters . . . . .	80
	Table 15: Precedence Rules for Applying Access Profiles . . . . .	82
	Table 16: Precedence Rules for Applying Dynamic Profiles . . . . .	83
	Table 17: Precedence Rules for Determining the Address Pool to Use . . . . .	84
<b>Part 3</b>	<b>DHCP Local Server for Subscriber Access</b>	
<b>Chapter 6</b>	<b>DHCP Local Server Overview</b> . . . . .	<b>97</b>
	Table 18: Information in Authentication Grant . . . . .	100
	Table 19: RADIUS Attributes and VSAs for DHCPv6 Local Server . . . . .	102
<b>Chapter 7</b>	<b>Configuring DHCP Local Server</b> . . . . .	<b>107</b>
	Table 20: ARP Table in Trusted Environment . . . . .	117
	Table 21: ARP Table in Distrusted Environment . . . . .	118

	Table 22: Actions for DHCP Local Server Snooped Packets . . . . .	119
	Table 23: Action Taken for Events That Occur During a Reconfiguration . . . . .	133
<b>Part 4</b>	<b>DHCP Relay Agent for Subscriber Access</b>	
<b>Chapter 10</b>	<b>Configuring DHCP Relay Agent . . . . .</b>	<b>161</b>
	Table 24: ARP Table in Trusted Environment . . . . .	172
	Table 25: ARP Table in Distrusted Environment . . . . .	173
	Table 26: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Enabled . . . . .	179
	Table 27: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Disabled . . . . .	179
	Table 28: Actions for Snooped BOOTREPLY Packets . . . . .	180
	Table 29: DHCP Relay Agent Option 82 Value for Auto Logout . . . . .	182
<b>Part 6</b>	<b>L2TP for Subscriber Access</b>	
<b>Chapter 16</b>	<b>L2TP for Subscriber Access Overview . . . . .</b>	<b>231</b>
	Table 30: L2TP Terms . . . . .	233
<b>Part 7</b>	<b>Diameter Base Protocol and Applications for Subscriber Access</b>	
<b>Chapter 20</b>	<b>JSRC and Juniper Networks Session Resource Control (SRC) Overview . . . . .</b>	<b>271</b>
	Table 31: Diameter Messages Used by JSRC and the SAE . . . . .	272
	Table 32: Standard Diameter AVPs . . . . .	273
	Table 33: Juniper Networks Diameter AVPs . . . . .	274
<b>Chapter 25</b>	<b>PTSP and Juniper Networks Session and Resource Control (SRC) . . . . .</b>	<b>303</b>
	Table 34: Diameter Messages Used by PTSP and the SAE . . . . .	304
	Table 35: Standard Diameter AVPs for PTSP . . . . .	305
	Table 36: Juniper Networks Diameter AVPs . . . . .	306
<b>Chapter 27</b>	<b>Configuring Packet-Triggered Subscriber Services . . . . .</b>	<b>317</b>
	Table 37: PTSP Match Conditions . . . . .	320
	Table 38: PTSP Actions . . . . .	321
	Table 39: PTSP Forward Rule Match Conditions . . . . .	323
<b>Chapter 28</b>	<b>Gx-Plus Overview . . . . .</b>	<b>329</b>
	Table 40: Diameter Messages Used by Gx-Plus and the PCRF . . . . .	331
	Table 41: Standard Diameter AVPs for Gx-Plus . . . . .	333
	Table 42: Juniper Networks Diameter AVPs for Gx-Plus . . . . .	334
	Table 43: Router Events, Router Actions, and PCRF Actions . . . . .	337
<b>Part 8</b>	<b>Mobile IP Access</b>	
<b>Chapter 30</b>	<b>Mobile IP Overview . . . . .</b>	<b>345</b>
	Table 44: Juniper Networks VSAs Used by Mobile IP . . . . .	349
	Table 45: WiMAX Forum VSAs used by Mobile IP . . . . .	354

<b>Part 9</b>	<b>Dynamic Profiles for Access and Services</b>	
<b>Chapter 32</b>	<b>Dynamic Profiles Overview</b>	<b>369</b>
	Table 46: Junos OS Predefined Variables and Definitions	372
	Table 47: RADIUS Attributes and Corresponding Junos OS Predefined Variables	385
<b>Part 11</b>	<b>Subscriber Interfaces</b>	
<b>Chapter 41</b>	<b>Subscriber Interfaces over Aggregated Ethernet Overview</b>	<b>471</b>
	Table 48: Features Supported with Static or Dynamic Demux Subscriber Interfaces	474
<b>Chapter 46</b>	<b>Dynamic PPPoE Subscriber Interfaces Examples</b>	<b>547</b>
	Table 49: Dynamic PPPoE Subscriber Interface Creation Based on PPPoE Client Request Values	551
<b>Part 12</b>	<b>Dynamic Firewall Filters, Service Sets and HTTP Redirect for Subscriber Access</b>	
<b>Chapter 47</b>	<b>Dynamic Firewall Filters and Service Sets Overview</b>	<b>555</b>
	Table 50: Ascend-Data-Filter Attribute Fields	561
<b>Chapter 49</b>	<b>Configuring Fast Update Filters</b>	<b>581</b>
	Table 51: Fast Update Filter Match Conditions	584
	Table 52: Fast Update Filter Actions and Action Modifiers	585
<b>Chapter 51</b>	<b>Firewall Filter Examples</b>	<b>597</b>
	Table 53: Ascend-Data-Filter Rule	605
<b>Part 13</b>	<b>Subscriber Secure Policy Traffic Mirroring</b>	
<b>Chapter 55</b>	<b>Subscriber Secure Policy Overview</b>	<b>625</b>
	Table 54: Subscriber Secure Policy Terms	626
	Table 55: Subscriber Secure Policy Configuration Steps	629
	Table 56: RADIUS-Initiated Mirroring at Subscriber Login	629
	Table 57: RADIUS-Initiated Mirroring for Current Subscriber	629
	Table 58: DTCP-Initiated Traffic Mirroring	630
<b>Chapter 57</b>	<b>Configuring RADIUS-Initiated Subscriber Secure Policy Traffic Mirroring</b>	<b>635</b>
	Table 59: RADIUS Attributes Used as Traffic Mirroring Triggers	637
	Table 60: RADIUS-Based Mirroring Attributes	637
	Table 61: LI-Action VSA Action	638
<b>Chapter 58</b>	<b>Configuring DTCP-Initiated Subscriber Secure Policy Mirroring</b>	<b>641</b>
	Table 62: DTCP Mirroring Attributes	644
<b>Chapter 59</b>	<b>Subscriber Secure Policy Mirroring and SNMP Traps</b>	<b>645</b>
	Table 63: Subscriber Secure Policy SNMPv3 Traps for LAES Messages	646

<b>Part 14</b>	<b>Class of Service for Subscriber Access</b>	
<b>Chapter 61</b>	<b>Dynamic CoS for Subscriber Access Overview</b>	<b>659</b>
	Table 64: Hardware Required for Dynamic CoS Configurations	661
	Table 65: IP Demux Classification Rules	664
	Table 66: IP Demux Rewrite Rules	664
	Table 67: L2TP Classification Rules	665
	Table 68: L2TP LAC Rewrite Rules	665
<b>Chapter 64</b>	<b>RADIUS and Dynamic CoS Overview</b>	<b>689</b>
	Table 69: CoS Predefined Variables for Scheduler Map and Traffic Shaping	690
	Table 70: CoS Predefined Variables for Scheduling and Queuing	691
	Table 71: CoS Services and Variables	694
<b>Chapter 66</b>	<b>Interface Solutions for Dynamic CoS Overview</b>	<b>703</b>
	Table 72: Scheduler Mapping for Interface Sets	703
	Table 73: Ingress LAC Tunnel Classifier Options	705
	Table 74: Sample Result	706
<b>Chapter 68</b>	<b>Dynamic CoS for Subscriber Access Examples</b>	<b>713</b>
	Table 75: Initial Scheduler Map and Shaping Values at Subscriber Login	716
	Table 76: Initial CoS Values for the Voice Scheduler at Subscriber Login	717
	Table 77: Initial CoS Values for the Data Scheduler at Subscriber Login	717
	Table 78: Upgraded CoS Values for the Video Service	720
	Table 79: Upgraded CoS Values for the Video Scheduler	720
	Table 80: Initial CoS Values for the Expedited Forwarding Scheduler at Subscriber Login	720
	Table 81: Initial CoS Values for the Best Effort Scheduler at Subscriber Login	721
	Table 82: Scheduler Per Logical Interface Mapping	727
	Table 83: Scheduler per Underlying Interface Mapping	729
	Table 84: Scheduler per Logical Interface with Interface Set Mapping	732
<b>Chapter 69</b>	<b>Bandwidth Management for Dynamic CoS Overview</b>	<b>747</b>
	Table 85: Dedicated Queues for Trio MPC/MIC Interfaces	749
<b>Chapter 71</b>	<b>Bandwidth Management for Dynamic CoS Examples</b>	<b>771</b>
	Table 86: Initial Shaping Values at Subscriber Login	772
	Table 87: Initial Shaping Values at Subscriber Login	774

# About This Guide

This preface provides the following guidelines for using the *Junos<sup>®</sup> OS Subscriber Access Configuration Guide*:

- JUNOS Documentation and Release Notes on page li
- Objectives on page lii
- Audience on page lii
- Supported Routing Platforms on page liii
- Using the Indexes on page liii
- Using the Examples in This Manual on page liii
- Documentation Conventions on page liv
- Documentation Feedback on page lvi
- Requesting Technical Support on page lvi

## JUNOS Documentation and Release Notes

---

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

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

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

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at <http://www.juniper.net/books>.

## Objectives

---

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



**NOTE:** For additional information about Junos OS—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 Juniper Networks MX Series Ethernet Services Routers.

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 OS currently supports the following routing platforms:

- MX Series routers

## 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.xml;
    }
  }
}
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.xml; }
```

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 OS CLI User Guide](#).

---

## Documentation Conventions

Table 1 on page lv 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 lv defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  <code>user@host&gt; configure</code>
Fixed-width text like this	Represents output that appears on the terminal screen.	<code>user@host&gt; show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces important new terms.</li> <li>Identifies book names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS System Basics Configuration Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>
<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@# <b>set system domain-name</b> <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit protocols ospf area area-id] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Enclose optional keywords or variables.	<code>stub &lt;default-metric metric&gt;;</code>

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

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

## 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](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

## 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/us/en/local/pdf/resource-guides/7100059-en.pdf> .
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/> .
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

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

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

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

## Opening a Case with JTAC

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

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

For international or direct-dial options in countries without toll-free numbers, 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 Considerations on page 5
- Subscriber Access Licensing Overview on page 6
- Subscriber Management Unified ISSU Support on page 6
- Verifying and Monitoring Subscriber Management Unified ISSU State on page 7
- Subscriber Access Operation Flow Using DHCP Relay on page 7
- Subscriber Activation and Service Management in an Access Network on page 8
- Configuring Subscriber Access on page 9
- Collecting Subscriber Access Logs Before Contacting Juniper Technical Support on page 12

## Subscriber Access Overview

---

The Juniper Networks Junos OS 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 acts 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 after 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 3 on page 4 defines terms and acronyms that are used in this discussion of subscriber access.

**Table 3: Subscriber Access Terms and Acronyms**

Term	Definition
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.
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.
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.
Subscriber access technology	The technology used by a subscriber to access services (for example, DHCP).

### Related Documentation

- [Subscriber Access Environment on page 4](#)
- [Subscriber Access Licensing Overview on page 6](#)
- [Subscriber Access Operation Flow Using DHCP Relay on page 7](#)
- [Configuring Subscriber Access on page 9](#)

---

## Subscriber Access Environment

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

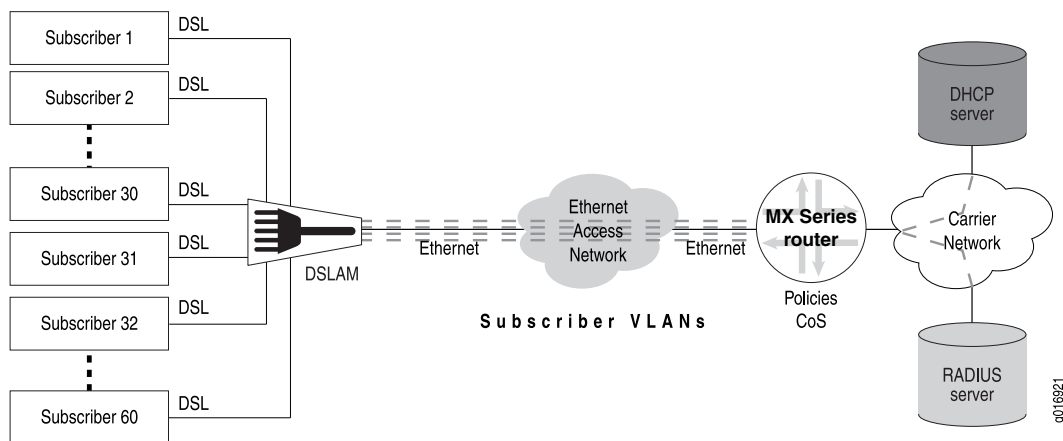
The subscriber access technologies include:

- Dynamic Host Configuration Protocol (DHCP) server
  - Local DHCP server
  - External DHCP server
- Point-to-Point Protocol (PPP)

The subscriber authentication protocols include the RADIUS server.

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

**Figure 1: Subscriber Access Network Example**



**Related Documentation**

- 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 one authenticated client or a group of clients on a single, authenticated VLAN.

**Related Documentation**

- Subscriber Interface Overview on page 433

## Subscriber Access Support Considerations

The subscriber access feature is limited to MX Series 3D Universal Edge 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 DHCP configuration on MX Series routers only. In addition, PPPoE configuration is currently supported on MX Series routers, M120 routers, and M320 routers.

## Interface Support

You can use dynamic profiles to configure statically created interfaces and also to create and configure interfaces dynamically. Subscriber interfaces support IPv4 and IPv6 addressing.

To identify subscribers statically, you can reference a static VLAN interface in a dynamic profile. To identify subscribers dynamically, you create variables for demux interfaces that are dynamically created when subscribers log in.

The subscriber access feature supports the following device types:

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

## DPC Support

Certain subscriber management features require the use of specific dense port concentrators (DPCs) on the MX series router. For a list of the MX series DPCs and the features they support, see the [MX Series 3D Universal Edge Routers Line Card Guide](#).

### Related Documentation

- Relationship Between Subscribers and Interfaces in an Access Network on page 5
- Configuring Subscriber Access on page 9

---

## Subscriber Access Licensing Overview

To enable some Juniper Networks Junos OS 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 Documentation

- For information about installing and managing Junos OS licenses, see the [Junos OS Installation and Upgrade Guide](#)

---

## Subscriber Management Unified ISSU Support

The unified in-service software upgrade (ISSU) feature supports the subscriber management DHCP access mode, which includes DHCP local server, DHCPv6 local server, DHCP relay, and DHCP relay proxy. The unified ISSU support ensures that the router preserves active DHCP subscriber sessions and session services after a unified ISSU has completed.



**NOTE:** Statistics for accounting, filter, and CoS are preserved after a unified ISSU on the EQ DPC, but are not preserved on the Trio MPC/MIC.

---

The *Junos OS High Availability Configuration Guide* describes the CLI statements and procedures you use to configure and initiate unified ISSU. You can use the **issu** flag with the **traceoptions** command to trace subscriber management unified ISSU events. You can also use the **show system subscriber-management summary** command to display information about the unified ISSU state.

- Related Documentation**
- Verifying and Monitoring Subscriber Management Unified ISSU State on page 7
  - For information about unified ISSU, see the “Unified ISSU” chapter in the *Junos OS High Availability Configuration Guide*

## Verifying and Monitoring Subscriber Management Unified ISSU State

**Purpose** Display the state of unified ISSU for subscriber management features.

**Action** The first example indicates that control plane quiescing as part of unified ISSU is not in progress (for example, unified ISSU has not been started, has already completed, or control plane quiescing has not started). The second example shows that unified ISSU is in progress and that a participating subscriber management daemon requires 198 seconds to quiesce the control plane.

```
user@host> show system subscriber-management summary
```

General:

Graceful Restart	Enabled
Mastership	Master
Database	Available
Chassisd ISSU State	IDLE
ISSU State	IDLE
ISSU Wait	0

```
user@host> show system subscriber-management summary
```

General:

Graceful Restart	Enabled
Mastership	Master
Database	Available
Chassisd ISSU State	DAEMON_ISSU_PREPARE
ISSU State	PREPARE
ISSU Wait	198

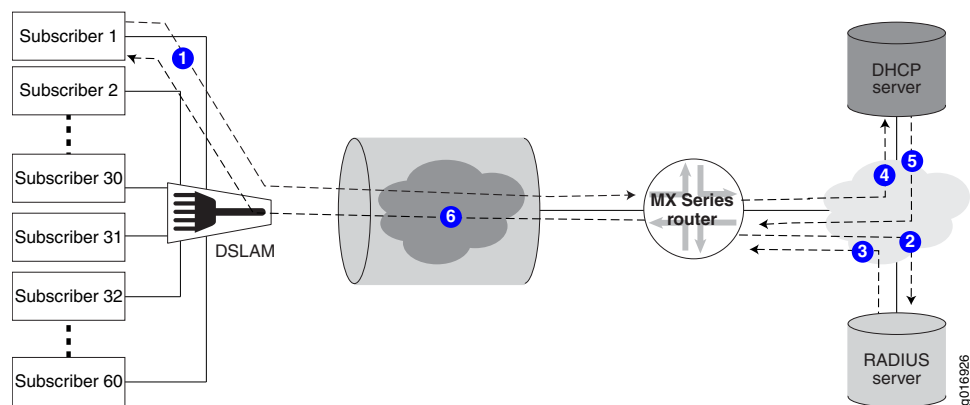
- Related Documentation**
- Subscriber Management Unified ISSU Support on page 6
  - See the “Unified ISSU” chapter in the *Junos OS High Availability Configuration Guide*

## Subscriber Access Operation Flow Using DHCP Relay

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

Figure 2 on page 8 shows the flow of operations that occurs 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 issues an authorization request to the RADIUS server.
3. The RADIUS server issues an authorization response to the router.
4. The router passes the DHCP discover message through to the DHCP server.
5. The DHCP server issues an IP address for the client.
6. The router DHCP component sends an acknowledgement back to the client.

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

#### Related Documentation

- Subscriber Access Overview on page 3
- Configuring Subscriber Access on page 9

## Subscriber Activation and Service Management 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 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 Predefined Variables Used by Dynamic Profiles

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

The predefined 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 Documentation

- Dynamic Profiles Overview on page 369
- Subscriber Interface Overview on page 433

---

## Configuring Subscriber Access

To configure subscriber access:

1. Configure the client access protocol.
  - Configure DHCP local server.  
See “Extended DHCP Local Server Overview” on page 98.
  - Configure DHCP relay.  
See “Extended DHCP Relay Agent Overview” on page 154.
  - Configure PPP.

See the “Configuring Logical Interface Properties” and “Configuring Point-to-Point Protocol over Ethernet” chapters of the *Junos OS Network Interfaces Configuration Guide*.

2. Configure subscriber authentication, accounting, and addressing.
  - a. Configure RADIUS:
    1. Specify the RADIUS servers.  
See “Specifying RADIUS Authentication and Accounting Servers for Subscriber Access” on page 27.
    2. Specify any optional server attributes.  
See “Configuring RADIUS Server Options for Subscriber Access” on page 29.
    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 38.
    4. Configure subscriber accounting (RADIUS accounting).  
See “Configuring Per-Subscriber Session Accounting” on page 24.
  - b. Configure addressing:
    - See “Configuring Address-Assignment Pools” on page 68.
3. Create and manage dynamic profiles for access and service.
  - a. Configure a basic dynamic profile.  
See “Configuring a Basic Dynamic Profile” on page 391.  
See “Example: Minimum PPPoE Dynamic Profile” on page 403
  - b. Configure a dynamic profile for access.  
See “Configuring a Dynamic Profile for Client Access” on page 395.
  - c. Configure a dynamic profile for services.  
See “Configuring a Dynamic Profile for Various Levels of Services” on page 397.
  - 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 440.
  - 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 441.
  - f. Add, modify, or delete dynamic profile values to manage subscriber access and services.  
See “Modifying Dynamic Profiles” on page 398.

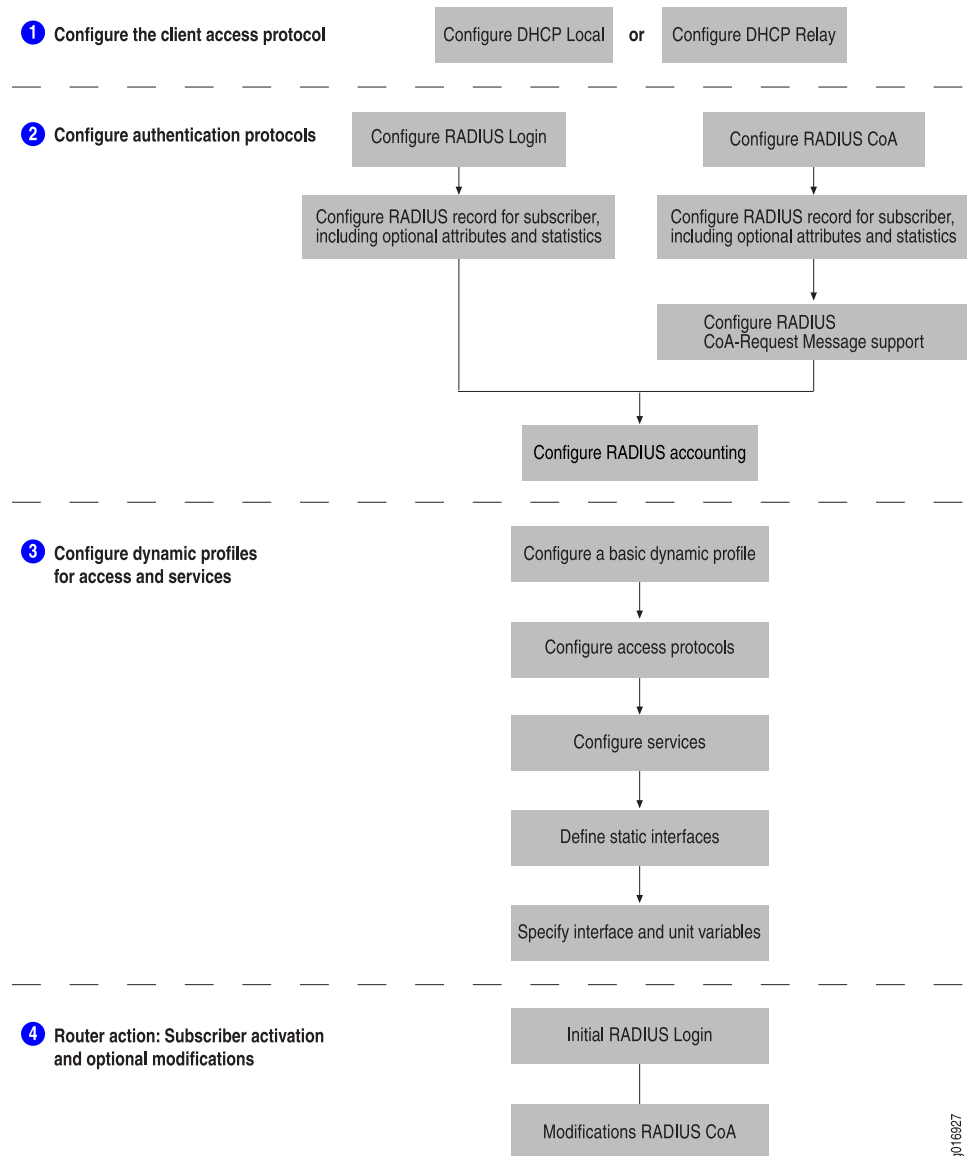


The router dynamically activates or modifies the subscriber service using the RADIUS configuration.

- When the subscriber logs in, the router dynamically activates the service.  
See “Dynamic Service Activation During Login Overview” on page 35.
- 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 35.

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

**Figure 3: Subscriber Access Configuration Workflow**



9016927

- Related Documentation**
- Subscriber Access Overview on page 3
  - Subscriber Access Support Considerations on page 5

## Collecting Subscriber Access Logs Before Contacting Juniper Technical Support

---

**Problem** When you experience a subscriber access problem in your network, we recommend that you collect certain logs before you contact Juniper Technical Support. This topic shows you the most useful logs for a variety of network implementations. In addition to the relevant log information, you must also collect standard troubleshooting information and send it to Juniper Technical Support in your request for assistance.

**Solution** To collect standard troubleshooting information:

- Redirect the command output to a file.

```
user@host> request support information | save rsi-1
```

To configure logging to assist Juniper Technical Support:

1. Review the following blocks of statements to determine which apply to your configuration.
2. Copy the relevant statements into a text file and modify the log filenames as you want.
3. Copy the statements from the text file and paste them into the CLI on your router to configure logging.
4. Commit the logging configuration to begin collecting information.



**NOTE:** The maximum file size for DHCP local server and DHCP relay log files is 1 GB. The maximum number of log files for DHCP local server and DHCP relay is 1000.



**BEST PRACTICE:** Enable these logs only to collect information when troubleshooting specific problems. Enabling these logs during normal operations can result in reduced system performance.

[edit]

```
set system syslog archive size 100m files 25
```

```
set system auto-configuration traceoptions file filename
```

```
set system auto-configuration traceoptions file filename size 100m files 25
```

```
set protocols ppp-service traceoptions file filename size 100m files 25
```

```
set protocols ppp-service traceoptions level all
```

```
set protocols ppp-service traceoptions flag all
```

```
set protocols ppp traceoptions file filename size 100m files 25
```

```
set protocols ppp traceoptions level all
set protocols ppp traceoptions flag all
set protocols ppp monitor-session all

set interfaces pp0 traceoptions flag all

set demux traceoptions file filename size 100m files 25
set demux traceoptions flag all

set system services dhcp-local-server traceoptions file filename
set system services dhcp-local-server traceoptions file size 100m
set system services dhcp-local-server traceoptions file files 25
set system services dhcp-local-server traceoptions flag auth
set system services dhcp-local-server traceoptions flag database
set system services dhcp-local-server traceoptions flag fwd
set system services dhcp-local-server traceoptions flag general
set system services dhcp-local-server traceoptions flag ha
set system services dhcp-local-server traceoptions flag interface
set system services dhcp-local-server traceoptions flag io
set system services dhcp-local-server traceoptions flag packet
set system services dhcp-local-server traceoptions flag packet-option
set system services dhcp-local-server traceoptions flag profile
set system services dhcp-local-server traceoptions flag rpd
set system services dhcp-local-server traceoptions flag rtsock
set system services dhcp-local-server traceoptions flag session-db
set system services dhcp-local-server traceoptions flag state
set system services dhcp-local-server traceoptions flag ui

set forwarding-options dhcp-relay traceoptions file filename
set forwarding-options dhcp-relay traceoptions file size 100m
set forwarding-options dhcp-relay traceoptions file files 25
set forwarding-options dhcp-relay traceoptions flag auth
set forwarding-options dhcp-relay traceoptions flag database
set forwarding-options dhcp-relay traceoptions flag fwd
set forwarding-options dhcp-relay traceoptions flag general
set forwarding-options dhcp-relay traceoptions flag ha
set forwarding-options dhcp-relay traceoptions flag interface
set forwarding-options dhcp-relay traceoptions flag io
set forwarding-options dhcp-relay traceoptions flag packet
set forwarding-options dhcp-relay traceoptions flag packet-option
set forwarding-options dhcp-relay traceoptions flag profile
set forwarding-options dhcp-relay traceoptions flag rpd
set forwarding-options dhcp-relay traceoptions flag rtsock
set forwarding-options dhcp-relay traceoptions flag session-db
set forwarding-options dhcp-relay traceoptions flag state
set forwarding-options dhcp-relay traceoptions flag ui

set class-of-service traceoptions file filename
set class-of-service traceoptions file size 100m
set class-of-service traceoptions flag all
set class-of-service traceoptions file files 25

set routing-options traceoptions file filename
set routing-options traceoptions file size 100m
set routing-options traceoptions flag all
set routing-options traceoptions flag state
set routing-options traceoptions flag general
set routing-options traceoptions flag route
set routing-options traceoptions flag policy
set routing-options traceoptions flag normal
set routing-options traceoptions flag graceful-restart
set routing-options traceoptions flag config-internal
```

```
set routing-options traceoptions flag parse
set routing-options traceoptions flag condition-manager
set routing-options traceoptions file files 25
```

```
set interfaces traceoptions file filename
set interfaces traceoptions file size 100m
set interfaces traceoptions flag all
set interfaces traceoptions file files 25
```

```
set system processes general-authentication-service traceoptions file filename
set system processes general-authentication-service traceoptions file size 100m
set system processes general-authentication-service traceoptions flag all
set system processes general-authentication-service traceoptions file files 25
```

## PART 2

# AAA Service Framework for Subscriber Access

- [Configuring the AAA Service Framework for Subscriber Access on page 17](#)
- [Configuring Address-Assignment Pools for Subscriber Access on page 67](#)
- [Configuring Domain Maps for Subscriber Access on page 79](#)
- [AAA and Remote Subscriber Access Configuration Examples on page 91](#)



## CHAPTER 2

# Configuring the AAA Service Framework for Subscriber Access

- AAA Service Framework Overview on page 18
- Configuring Router or Switch Interaction with RADIUS Servers on page 20
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 21
- Specifying the Authentication and Accounting Methods for Subscriber Access on page 21
- RADIUS Acct-On and Acct-Off Messages on page 22
- RADIUS Accounting Statistics for Subscriber Access Overview on page 23
- Configuring Per-Subscriber Session Accounting on page 24
- Configuring Per-Service Session Accounting on page 25
- Configuring RADIUS Server Parameters for Subscriber Access on page 26
- Specifying RADIUS Authentication and Accounting Servers for Subscriber Access on page 27
- RADIUS Server Options for Subscriber Access on page 28
- Configuring RADIUS Server Options for Subscriber Access on page 29
- Configuring How RADIUS Attributes Are Used for Subscriber Access on page 31
- Using RADIUS Dynamic Requests for Subscriber Access Management on page 34
- Dynamic Service Activation During Login Overview on page 35
- RADIUS-Initiated Change of Authorization (CoA) Overview on page 35
- RADIUS-Initiated Disconnect Overview on page 37
- Configuring RADIUS-Initiated Dynamic Request Support on page 38
- Verifying and Managing the RADIUS Dynamic-Request Feature on page 38
- RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 39
- RADIUS IETF Attributes Supported by the AAA Service Framework on page 39
- Juniper Networks VSAs Supported by the AAA Service Framework on page 45
- DSL Forum Vendor-Specific Attributes on page 50

- Error-Cause Codes (RADIUS Attribute 101) for Dynamic Requests on page 52
- Configuring an Access Profile for Subscriber Management on page 53
- Attaching Access Profiles on page 53
- Understanding Session Options for Subscriber Access on page 54
- Configuring Subscriber Session Options on page 55
- AAA Configuration Testing and Troubleshooting on page 56
- Testing a Subscriber AAA Configuration on page 56
- Tracing Subscriber Management Database Operations for Subscriber Access on page 58
- Configuring the Subscriber Management Database Trace Log Filename on page 59
- Configuring the Number and Size of Subscriber Management Database Log Files on page 59
- Configuring Access to the Subscriber Management Database Log File on page 59
- Configuring a Regular Expression for Subscriber Management Database to Be Logged on page 60
- Configuring the Subscriber Management Database Tracing Flags on page 60
- Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 61
- Configuring the Number and Size of Subscriber Management Session Database Replication Log Files on page 62
- Configuring a Regular Expression for Subscriber Management Session Database Replication to Be Logged on page 63
- Configuring Access to the Subscriber Management Session Database Replication Log File on page 63
- Configuring the Subscriber Management Session Database Replication Trace Log Filename on page 64
- Configuring the Subscriber Management Session Database Replication Tracing Flags on page 64
- Verifying and Managing Subscriber AAA Information on page 65

---

## AAA Service Framework Overview

The authentication, authorization, and accounting (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 change of authorization (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, *Remote Authentication Dial*



*In User Service (RADIUS), RFC-2866, RADIUS Accounting, and RFC-3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), 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. You can also configure AAA to enable the router to collect statistics on a per-service session basis for subscribers.
- **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 Documentation**

- [Configuring Router or Switch Interaction with RADIUS Servers on page 20](#)
- [RADIUS Acct-On and Acct-Off Messages on page 22](#)
- [Configuring Authentication and Accounting Parameters for Subscriber Access on page 21](#)
- [Address-Assignment Pools Overview on page 67](#)
- [RADIUS Accounting Statistics for Subscriber Access Overview on page 23](#)
- [Using RADIUS Dynamic Requests for Subscriber Access Management on page 34](#)
- [Subscriber Secure Policy Overview on page 625](#)

## Configuring Router or Switch Interaction with RADIUS Servers

---

You specify the RADIUS servers that the router or switch can use and you configure how the router or switch interacts with the servers. You can configure the router or switch to use multiple RADIUS servers on the network.

To specify a RADIUS server and how the router or switch interacts with the server:

1. Configure the IP address of the RADIUS server and specify that you want to configure the router or switch interaction with the server.

```
[edit access]
user@host# edit radius-server 192.168.1.250
```

2. (Optional) Configure the RADIUS server accounting port number. The default accounting port number is 1813.

```
[edit access radius-server 192.168.1.250]
user@host# set accounting-port 1813
```

3. (Optional) Configure the port number the router or switch uses to contact the RADIUS server. The default port number is 1812.

```
[edit access radius-server 192.168.1.250]
user@host# set port 18914
```

4. (Optional) Configure the number of times that the router or switch attempts to contact a RADIUS accounting server. You can configure the router or switch to retry from 1 through 16 times. The default setting is 3 retry attempts.

```
[edit access radius-server 192.168.1.250]
user@host# set retry 4
```

5. Configure the required secret (password) that the local router or switch passes to the RADIUS client. Secrets enclosed in quotation marks can contain spaces.

```
[edit access radius-server 192.168.1.250]
user@host# set secret "nt1UE1*7688+
```

6. Configure the 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 or switch interfaces.

```
[edit access radius-server 192.168.1.250]
user@host# set source-address 192.168.1.100
```

7. (Optional) Configure the length of time that the local router or switch waits to receive a response from a RADIUS server. By default, the router or switch waits 3 seconds. You can configure the timeout to be from 1 through 90 seconds.

```
[edit access radius-server 192.168.1.250]
user@host# set timeout 45
```

### Related Documentation

- AAA Service Framework Overview on page 18
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 21

- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 91

## 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.

To configure authentication and accounting for subscriber access:

1. Specify the authentication and accounting methods to use.  
See “Specifying the Authentication and Accounting Methods for Subscriber Access” on page 21.
2. Specify how accounting statistics are collected.  
See “Configuring Per-Subscriber Session Accounting” on page 24.

### Related Documentation

- AAA Service Framework Overview on page 18
- Configuring Router or Switch Interaction with RADIUS Servers on page 20
- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 91

## Specifying the Authentication and Accounting Methods for Subscriber Access

You can specify the authentication and accounting methods that subscriber access management uses.

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.

You can specify the following authentication methods:



**NOTE:** For this release, you must always specify the radius authentication method. Subscriber access management does not support the password keyword (the default), and authentication fails when no method is specified.

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

You can specify the following accounting methods:

- **radius**—RADIUS-based accounting

To configure the authentication and accounting methods for subscriber access management:

1. Specify the authentication methods and the order in which they are used. For this release, only **radius** is supported.

```
[edit access profile isp-bos-metro-fiber-basic]  
user@host# set authentication-order radius
```

2. Specify the accounting method.

```
[edit access profile isp-bos-metro-fiber-basic]  
user@host# set accounting order radius
```

#### Related Documentation

- Configuring Router or Switch Interaction with RADIUS Servers on page 20
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 21
- Configuring Per-Subscriber Session Accounting on page 24
- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 91

---

## RADIUS Acct-On and Acct-Off Messages

Subscriber management supports RADIUS Acct-On and Acct-Off messages to indicate the current state of RADIUS accounting support.

RADIUS Acct-On messages indicate that accounting is being supported. Subscriber management issues Acct-On messages in the following situations:

- Accounting is enabled through configuration (for example, an accounting server is configured).
- A new access profile is configured and committed for a logical system/routing instance context. However, no Acct-On message is sent if the accounting server exists prior to the access profile and if it is simply modified.
- The router performs a cold reboot.
- The router performs a warm reboot and there are no subscribers currently logged in.
- The Authd process restarts and there are no active subscribers.

RADIUS Acct-Off messages indicate that accounting is not supported. Subscriber management issues Acct-Off messages in the following situations:

- The Authd process is terminated and there are no active subscribers.
- The router is shut down and accounting servers are currently configured (this action also logs out all current subscribers).

- The router is rebooted and redundancy is disabled.

**Related  
Documentation**

- AAA Service Framework Overview on page 18
- Configuring Per-Subscriber Session Accounting on page 24

## RADIUS Accounting Statistics for Subscriber Access Overview

The AAA Service Framework enables you to configure how the router collects and uses accounting statistics for subscriber management.

For example, you can specify when statistics collection is terminated, the order in which different accounting methods are used, the types of statistics collected, and how often statistics are collected. You can also configure the router to request that the RADIUS server immediately update the accounting statistics when certain events occur, such as when a subscriber logs in or when a change of authorization (CoA) occurs.

Subscriber management provides two levels of subscriber accounting—subscriber session and service session. In subscriber session accounting, the router collects statistics for the entire subscriber session. In service session accounting, the router collects statistics for specific service sessions for the subscriber.

The router uses the RADIUS attributes and Juniper Networks VSAs listed in Table 4 on page 23 to provide the accounting statistics for subscriber and service sessions. If the session has both IPv4 and IPv6 families enabled, the router reports statistics for both families.



**NOTE:**

RADIUS reports subscriber statistics as an aggregate of both IPv4 statistics and IPv6 statistics.

- For an IPv4-only configuration, the standard RADIUS attributes report the IPv4 statistics and the IPv6 VSA results are all reported as 0.
- For an IPv6-only configuration, the standard RADIUS attributes and the IPv6 VSA statistics are identical, both reporting the IPv6 statistics.
- When both IPv4 and IPv6 are configured, the standard RADIUS attributes report the combined IPv4 and IPv6 statistics. The IPv6 VSAs report IPv6 statistics.

**Table 4: RADIUS Attributes and VSAs Used for Per-Subscriber Session Accounting**

Attribute Number	Attribute Name	Type of Statistics
26–151	IPv6-Acct-Input-Octets	IPv6
26–152	IPv6-Acct-Output-Octets	IPv6

**Table 4: RADIUS Attributes and VSAs Used for Per-Subscriber Session Accounting (*continued*)**

Attribute Number	Attribute Name	Type of Statistics
26–153	IPv6-Acct-Input-Packets	IPv6
26–154	IPv6-Acct-Output-Packets	IPv6
26–155	IPv6-Acct-Input-Gigawords	IPv6
26–156	IPv6-Acct-Output-Gigawords	IPv6
47	Acct-Input-Packets	IPv4 and IPv6 aggregation
48	Acct-Output-Packets	IPv4 and IPv6 aggregation
52	Acct-Input-Gigawords	IPv4 and IPv6 aggregation
53	Acct-Output-Gigawords	IPv4 and IPv6 aggregation

**Related Documentation**

- Configuring Per-Subscriber Session Accounting on page 24
- Configuring Per-Service Session Accounting on page 25
- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 91

## Configuring Per-Subscriber Session Accounting

To configure accounting for a subscriber session, you use an access profile, and specify how the subscriber access management feature collects and uses the accounting statistics. The router uses the RADIUS attributes and Juniper Networks VSAs discussed in “RADIUS Accounting Statistics for Subscriber Access Overview” on page 23 to provide the accounting statistics for the subscriber session.

To configure accounting for a subscriber session:

1. At the **[edit access profile *profile-name*]** hierarchy level, specify that you want to configure accounting.  

```
[edit access profile profile-name]
user@host# edit accounting
```
2. (Optional) Configure AAA to issue an Acct-Stop message if the AAA server denies access to the subscriber.  

```
[edit access profile profile-name accounting]
user@host# set accounting-stop-on-access-deny
```
3. (Optional) Configure AAA to send an Acct-Stop message if the subscriber fails AAA but is granted access by the AAA server.

```
[edit access profile profile-name accounting]
user@host# set accounting-stop-on-failure
```

4. (Optional) Configure the order in which multiple accounting methods are used.

```
[edit access profile profile-name accounting]
user@host# set order [ accounting-order ]
```

5. (Optional) Configure the types of statistics to gather. You can specify that the router or switch 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.

```
[edit access profile profile-name accounting]
user@host# set statistics (time | volume-time)
```

6. (Optional) Configure 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.

```
[edit access profile profile-name accounting]
user@host# set update-interval minutes
```

7. (Optional) Configure the router or switch to send an Acct-Update message to the RADIUS accounting server when the router or switch receives a response (for example, an ACK or timeout) to the Acct-Start message.

```
[edit access profile profile-name accounting]
user@host# set immediate-update
```

8. (Optional) Configure the router or switch to send an Acct-Update message to the RADIUS accounting server when a CoA occurs.

```
[edit access profile profile-name accounting]
user@host# set coa-immediate-update
```

#### Related Documentation

- RADIUS Accounting Statistics for Subscriber Access Overview on page 23
- Configuring Per-Service Session Accounting on page 25
- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 91

## Configuring Per-Service Session Accounting

Subscriber management enables you to configure the router to collect statistics on a per-service session basis for subscribers. Per-service session accounting requires two operations. First, RADIUS must be configured to provide the name of the service, the accounting interval to use, and the type of statistics to collect (either time statistics or a combination of time and volume statistics). Second, if RADIUS VSA 26-69 is configured for time and volume statistics, you must also configure a firewall or fast update firewall filter that counts service packets—the service packet information provides the volume statistics.

The router uses the RADIUS attributes and Juniper Networks VSAs discussed in “RADIUS Accounting Statistics for Subscriber Access Overview” on page 23 to provide the accounting statistics for the subscriber session.



**NOTE:** The collection of time-only service statistics is supported for all service sessions. However, time and volume statistics are provided for only firewall and fast update firewall service sessions.

To configure the router to provide per-service accounting statistics:

1. Ensure that the required RADIUS VSAs are configured.  
See Table 5 on page 26 for the VSAs that the router uses for per-service accounting.
2. Configure the classic firewall filter or fast update filter to count the service packets.  
See “Configuring Service Packet Counting” on page 576.

**Table 5: Juniper Network VSAs Used for Per-Service Session Accounting**

Attribute Number	Attribute Name	Description	Value
26-69	Service-Statistics	Enable or disable statistics for the service	<ul style="list-style-type: none"> <li>• 0 = disable</li> <li>• 1 = enable time statistics</li> <li>• 2 = enable time and volume statistics</li> </ul>
26-83	Service-Session	Name of the service	string: service-name
26-140	Service-Interim-Acct-Interval	Amount of time between interim accounting updates for this service	<ul style="list-style-type: none"> <li>• range = 600–86400 seconds</li> <li>• 0 = disabled</li> </ul>

- Related Documentation**
- Configuring Service Packet Counting on page 576
  - RADIUS Accounting Statistics for Subscriber Access Overview on page 23
  - Configuring Per-Subscriber Session Accounting on page 24
  - Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 91

## 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. The following list provides an overview of the parameters you can configure:

- The IP addresses of one or more RADIUS authentication and accounting servers.



- Options for the RADIUS servers, such as the format (decimal or description) used for the accounting session, the method (round-robin or direct) the router or switch uses to communicate with the servers, the NAS identifier to use for RADIUS requests, and the revert time setting that specifies when the router or switch reverts to using the primary RADIUS server.
- The RADIUS attributes to be ignored or excluded from RADIUS messages.

To configure RADIUS server parameters:

1. Specify that you want to configure RADIUS support.

```
[edit access profile isp-bos-metro-fiber-basic]  
user@host# edit radius
```

2. Specify the addresses of RADIUS authentication and accounting servers.

See “Specifying RADIUS Authentication and Accounting Servers for Subscriber Access” on page 27.

3. Configure the RADIUS server options.

See “Configuring RADIUS Server Options for Subscriber Access” on page 29.

4. Configure RADIUS attributes that are ignored or excluded from RADIUS messages.

See “Configuring How RADIUS Attributes Are Used for Subscriber Access” on page 31.

## Specifying RADIUS Authentication and Accounting Servers for Subscriber Access

You can specify one or more RADIUS authentication or accounting servers to use for subscriber access management.

To configure RADIUS authentication and accounting support:

1. Specify that you want to configure RADIUS support.

```
[edit access profile isp-bos-metro-fiber-basic]  
user@host# edit radius
```

2. Specify the IP address of the RADIUS server used for authentication.

```
[edit access profile isp-bos-metro-fiber-basic radius]  
user@host# set authentication-server 192.168.1.251
```

3. Specify the IP address of the RADIUS server used for accounting.

```
[edit access profile isp-bos-metro-fiber-basic radius]  
user@host# set accounting-server 192.168.1.250
```

To configure multiple RADIUS authentication or accounting servers:

- Specify the IP addresses of all RADIUS servers used for authentication or accounting.

```
[edit access profile isp-bos-metro-fiber-basic radius]  
user@host# set authentication-server 192.168.1.251 192.168.1.252  
user@host# set accounting-server 192.168.1.250 192.168.1.251
```

**Related Documentation**

- Configuring Router or Switch Interaction with RADIUS Servers on page 20
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 21
- Configuring RADIUS Server Options for Subscriber Access on page 29
- Configuring How RADIUS Attributes Are Used for Subscriber Access on page 31
- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 91

---

## RADIUS Server Options for Subscriber Access

---

You can specify options that the router uses when communicating with RADIUS authentication and accounting servers for subscriber access.

The following list describes the RADIUS options you can configure:

- **client-accounting-algorithm** and **client-authentication-algorithm**—The method the router uses to access RADIUS accounting and RADIUS authentication servers. You can specify the following methods:
  - **direct**—The default method, in which there is no load balancing. For example, in the direct method, the router always accesses **server1** (the primary server) first, and uses **server2** and **server3** as backup servers.
  - **round-robin**—The method that provides load balancing by rotating router requests among the list of configured RADIUS servers. For example, if three RADIUS servers are configured to support the router, the router sends the first request to **server1**, and uses **server2** and **server3** as backup servers. The router then sends the second request to **server2**, and uses **server3** and **server1** as backups.



**NOTE:** When a RADIUS server in the round-robin list becomes unreachable, the next reachable server in the round-robin list is used for the current request. That same server is also used for the next request since it is at the top of the list of available servers. As a result, after a server failure, the server that is used takes up the load of two servers.

- **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 of **virtual** that the router uses to authenticate clients. The port type is passed in RADIUS attribute 61 (NAS-Port-Type). By default the router passes a port type of **ethernet** in RADIUS attribute 61.

- **interface-description-format**—The information that is excluded 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. You can specify:
  - **exclude-adapter**—Exclude the adapter.
  - **exclude-subinterface**—Exclude the subinterface.
- **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 through 64 characters.
- **nas-port-extended-format**—The extended format for RADIUS attribute 5 (NAS-Port) and for the width of the fields in the NAS-Port attribute that the RADIUS client uses. You can specify:
  - **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.



**NOTE:** The total of the widths must not exceed 32 bits, or the configuration will fail.

- **revert-interval**—The number of seconds 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. You can configure from 0 (off) through 429496729 seconds. The default is 60 seconds.
- **vlan-nas-port-stacked-format**—The format that turns off RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.

#### Related Documentation

- Configuring RADIUS Server Options for Subscriber Access on page 29

## Configuring RADIUS Server Options for Subscriber Access

You can specify options that the router or switch uses when communicating with RADIUS authentication and accounting servers for subscriber access.

To configure RADIUS authentication and accounting server options:

1. Specify that you want to configure RADIUS.

```
[edit access profile isp-bos-metro-fiber-basic]
user@host# edit radius
```

2. Specify that you want to configure RADIUS options.

```
[edit access profile isp-bos-metro-fiber-basic radius]
user@host# edit options
```

3. (Optional) Configure the method the router or switch uses to access RADIUS accounting servers.

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set client-accounting-algorithm round-robin
```

4. (Optional) Configure the method the router or switch uses to access RADIUS authentication servers.

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set client-authentication-algorithm round-robin
```

5. (Optional) Configure the format the router or switch uses to identify the accounting session.

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set accounting-session-id-format decimal
```

6. (Optional) Configure the router or switch to use a port type of **virtual** to authenticate clients.

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set ethernet-port-type-virtual
```

7. (Optional) Specify the information that is excluded from the interface description that the router or switch passes to RADIUS for inclusion in RADIUS attribute 87 (NAS-Port-Id).

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set interface-description-format exclude-adapter
```

8. (Optional) Configure the value for the client RADIUS attribute 32 (NAS-Identifier), which is used for authentication and accounting requests.

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set nas-identifier 56
```

9. (Optional) 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. The total of the widths must not exceed 32 bits, or the configuration will fail.

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set nas-port-extended-format 16
```

10. (Optional) Configure the number of seconds that the router or switch waits after a server has become unreachable.

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set revert-interval port-width 1200
```

11. (Optional) Specify that RADIUS attribute 5 (NAS-Port) includes the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.

```
[edit access profile isp-bos-metro-fiber-basic radius options]
```

```
user@host# set vlan-nas-port-stacked-format
```

#### Related Documentation

- RADIUS Server Options for Subscriber Access on page 28
- Configuring Router or Switch Interaction with RADIUS Servers on page 20
- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 91

## Configuring How RADIUS Attributes Are Used for Subscriber Access

You can specify the attributes RADIUS ignores in RADIUS Access-Accept messages, and the attributes RADIUS excludes from specified message types.

To configure the attributes RADIUS ignores or excludes:

1. Specify that you want to configure RADIUS.

```
[edit access profile isp-bos-metro-fiber-basic]
user@host# edit radius
```

2. Specify that you want to configure how RADIUS attributes are ignored or excluded.

```
[edit access profile isp-bos-metro-fiber-basic radius]
user@host# edit attributes
```

3. Specify the attributes you want RADIUS to ignore when the attributes are in Access-Accept messages. See Table 6 on page 31 for the attributes you can configure.

```
[edit access profile isp-bos-metro-fiber-basic radius attributes]
user@host# set ignore input-filter output-filter
```

4. Configure RADIUS to exclude the specified attribute from the specified RADIUS message type. See Table 7 on page 32 for the attributes and message type combinations you can configure.

```
[edit access profile isp-bos-metro-fiber-basic radius attributes]
user@host# set exclude input-filter output-filter
```

You use the **ignore** statement to configure the router or switch to ignore a particular attribute in RADIUS Access-Accept messages. By default, the router or switch processes the attributes received from the external AAA server. Table 6 on page 31 lists the attributes supported in the **ignore** statement.

**Table 6: Attributes That Can Be Ignored in RADIUS Accept-Accept Messages**

CLI Entry	Attribute Name	Attribute Number
framed-ip-netmask	Framed-Ip-Netmask	RADIUS attribute 9
input-filter	Ingress-Policy-Name	Juniper Networks VSA 26–10
logical-system:routing-instance	Virtual-Router	Juniper Networks VSA 26–1

**Table 6: Attributes That Can Be Ignored in RADIUS Accept-Accept Messages (*continued*)**

CLI Entry	Attribute Name	Attribute Number
output-filter	Egress-Policy-Name	Juniper Networks VSA 26–11

You use the **exclude** statement to configure the router or switch 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 or switch includes the specified attributes in RADIUS Access-Request, Acct-On, Acct-Off, Acct-Start, and Acct-Stop messages. Table 7 on page 32 lists the attributes and message types supported in the **exclude** statement.

**Table 7: Attributes That Can Be Excluded from RADIUS Messages**

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
accounting-authentic	Acct-Authentic	RADIUS attribute 45	Accounting-On Accounting-Off
accounting-delay-time	Acct-Delay-Time	RADIUS attribute 41	Accounting-On Accounting-Off
accounting-session-id	Acct-Session-Id	RADIUS attribute 44	Access-Request Accounting-On Accounting-Off Accounting-Stop
accounting-terminate-cause	Acct-Terminate-Cause	RADIUS attribute 49	Accounting-Off
called-station-id	Called-Station-Id	RADIUS attribute 30	Access-Request Accounting-Start Accounting-Stop
calling-station-id	Calling-Station-Id	RADIUS attribute 31	Access-Request Accounting-Start Accounting-Stop
class	Class	RADIUS attribute 25	Accounting-Start Accounting-Stop

**Table 7: Attributes That Can Be Excluded from RADIUS Messages** (*continued*)

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
dhcp-gi-address	DHCP-GI-Address	Juniper Networks VSA 26–57	Access-Request Accounting-Start Accounting-Stop
dhcp-mac-address	DHCP-MAC-Address	Juniper Networks VSA 26–56	Access-Request Accounting-Start Accounting-Stop
event-timestamp	Event-Timestamp	RADIUS attribute 55	Accounting-On Accounting-Off Accounting-Start Accounting-Stop
framed-ip-address	Framed-IP-Address	RADIUS attribute 8	Accounting-Start Accounting-Stop
framed-ip-netmask	Framed-IP-Netmask	RADIUS attribute 9	Accounting-Start Accounting-Stop
input-filter	Ingress-Policy-Name	Juniper Networks VSA 26–10	Accounting-Start Accounting-Stop
input-gigapackets	Acct-Input-Gigapackets	Juniper Networks VSA 26–42	Accounting-Stop
input-gigawords	Acct-Input-Gigawords	RADIUS attribute 52	Accounting-Stop
interface-description	Interface-Desc	Juniper Networks VSA 26–53	Access-Request Accounting-Start Accounting-Stop
nas-identifier	NAS-Identifier	RADIUS attribute 32	Access-Request Accounting-on Accounting-off Accounting-Start Accounting-Stop

**Table 7: Attributes That Can Be Excluded from RADIUS Messages (*continued*)**

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
nas-port	NAS-Port	RADIUS attribute 5	Access-Request Accounting-Start Accounting-Stop
nas-port-id	NAS-Port-Id	RADIUS attribute 87	Access-Request Accounting-Start Accounting-Stop
nas-port-type	NAS-Port-Type	RADIUS attribute 61	Access-Request Accounting-Start Accounting-Stop
output-filter	Egress-Policy-Name	Juniper Networks VSA 26–11	Accounting-Start Accounting-Stop
output-gigapackets	Acct-Output-Gigapackets	Juniper Networks VSA 26–43	Accounting-Stop
output-gigawords	Acct-Output-Gigawords	RADIUS attribute 53	Accounting-Stop

**Related Documentation**

- Configuring Router or Switch Interaction with RADIUS Servers on page 20
- Configuring Authentication and Accounting Parameters for Subscriber Access on page 21
- Specifying RADIUS Authentication and Accounting Servers for Subscriber Access on page 27
- Configuring RADIUS Server Options for Subscriber Access on page 29
- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 91

## 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 Documentation**

- Dynamic Service Activation During Login Overview on page 35
- RADIUS-Initiated Change of Authorization (CoA) Overview on page 35
- RADIUS-Initiated Disconnect Overview on page 37
- Configuring RADIUS-Initiated Dynamic Request Support on page 38
- RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 39
- Error-Cause Codes (RADIUS Attribute 101) for Dynamic Requests on page 52

---

## 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.

**Related Documentation**

- Using RADIUS Dynamic Requests for Subscriber Access Management on page 34
- Configuring RADIUS-Initiated Dynamic Request Support on page 38
- RADIUS-Initiated Disconnect Overview on page 37

---

## 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 in the following list to uniquely identify subscribers. The request must also include the appropriate VSA 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.

---

- Related Documentation**
- Using RADIUS Dynamic Requests for Subscriber Access Management on page 34
  - Dynamic Service Activation During Login Overview on page 35
  - RADIUS-Initiated Disconnect Overview on page 37
  - Configuring RADIUS-Initiated Dynamic Request Support on page 38

---

## 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.

**Related  
Documentation**

- Using RADIUS Dynamic Requests for Subscriber Access Management on page 34
- Dynamic Service Activation During Login Overview on page 35
- Configuring RADIUS-Initiated Dynamic Request Support on page 38

---

## Configuring RADIUS-Initiated Dynamic Request Support

---

The router uses the list of specified RADIUS authentication servers for both authentication and dynamic request operations. The router listens on UDP port 3799 for dynamic requests.

To configure RADIUS dynamic request support:

- Specify the IP address of the RADIUS server.

```
[edit access profile isp-bos-metro-fiber-basic radius]
user@host# set authentication-server 192.168.1.3
```

To configure the router to support dynamic requests from more than one RADIUS server:

- Specify the IP addresses of multiple RADIUS servers.

```
[edit access profile isp-bos-metro-fiber-basic radius]
user@host# set authentication-server 192.168.1.3 192.168.10.15
```

**Related  
Documentation**

- Using RADIUS Dynamic Requests for Subscriber Access Management on page 34
- Dynamic Service Activation During Login Overview on page 35
- RADIUS-Initiated Change of Authorization (CoA) Overview on page 35
- RADIUS-Initiated Disconnect Overview on page 37
- RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 39
- Error-Cause Codes (RADIUS Attribute 101) for Dynamic Requests on page 52

---

## Verifying and Managing the RADIUS Dynamic-Request Feature

---

**Purpose** Display RADIUS dynamic request statistics and information.

- Action** • To display RADIUS dynamic request statistics:

```
user@host>show network-access aaa statistics dynamic-requests
```

- Related Documentation** • [Junos OS 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.

When you use dynamic profiles, the AAA Service Framework supports the use of Junos OS predefined variables to specify the RADIUS attribute or VSA for the information obtained from the RADIUS server.

- Related Documentation**
- [RADIUS IETF Attributes Supported by the AAA Service Framework on page 39](#)
  - [Juniper Networks VSAs Supported by the AAA Service Framework on page 45](#)
  - [DSL Forum Vendor-Specific Attributes on page 50](#)
  - [Junos OS Predefined Variables That Correspond to RADIUS Attributes and VSAs on page 385](#)

## RADIUS IETF Attributes Supported by the AAA Service Framework

Table 8 on page 39 describes the RADIUS IETF attributes that the Junos OS AAA Service Framework supports.



**NOTE:** A “Yes” entry in the Dynamic CoA Support column indicates that the attribute can be dynamically configured by Access-Accept messages and dynamically modified by CoA-Request messages.

**Table 8: Supported RADIUS IETF Attributes**

Attribute Number	Attribute Name	Description	Dynamic CoA Support
1	User-Name	<ul style="list-style-type: none"> <li>• Name of user to be authenticated.</li> <li>• Configurable username override.</li> </ul>	No

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

Attribute Number	Attribute Name	Description	Dynamic CoA Support
2	User-Password	<ul style="list-style-type: none"> <li>Password of user to be authenticated by Password Authentication Protocol (PAP).</li> <li>Configurable password override.</li> </ul>	No
4	NAS-IP-Address	IP address of the network access server (NAS) that is requesting authentication of the user.	No
5	NAS-Port	Physical port number of the NAS that is authenticating the user.	No
6	Service-Type	Type of service the user has requested or the type of service to be provided.	No
8	Framed-IP-Address	<ul style="list-style-type: none"> <li>IP address to be configured for the user.</li> <li>0.0.0.0 or absence is interpreted as 255.255.255.254.</li> </ul>	No
9	Framed-IP-Netmask	<ul style="list-style-type: none"> <li>IP network to be configured for the user when the user is a router or switch to a network.</li> <li>Absence implies 255.255.255.255.</li> </ul>	No
11	Filter-ID	<ul style="list-style-type: none"> <li>Name of the filter list for the user.</li> <li>Interpreted as input policy name.</li> </ul>	Yes
18	Reply-Message	<ul style="list-style-type: none"> <li>Text that may be displayed to the user.</li> <li>Only the first instance of this attribute is used.</li> </ul>	No
22	Framed-Route	<p>String that provides routing information to be configured for the user on the NAS in the format:</p> <pre>&lt;addr&gt;[/&lt;maskLen&gt;] [&lt;nexthop&gt; [&lt;cost&gt;]] [tag &lt;tagValue&gt;] [distance &lt;distValue&gt;]</pre>	Yes
25	Class	Arbitrary value that the NAS includes in all accounting packets for the user if supplied by the RADIUS server.	No
27	Session-Timeout	Maximum number of consecutive seconds of service to be provided to the user before termination of the session.	No
31	Calling-Station-ID	The NAS can send the phone number from which the call originated.	No

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

Attribute Number	Attribute Name	Description	Dynamic CoA Support
32	NAS-Identifier	NAS originating the request.	No
40	Acct-Status-Type	Whether this Accounting-Request marks the beginning of the user service (Start), the end (Stop), or the interim (Interim-Update).	No
41	Acct-Delay-Time	Number of seconds the client has been trying to send a particular record.	No
42	Acct-Input-Octets	The number of octets that have been received from the port during the time this service has been provided.	No
43	Acct-Output-Octets	The number of octets that have been sent to the port during the time this service has been provided.	No
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"> <li><b>decimal</b>—For example, 435264</li> <li><b>description</b>—In the generic format, <i>jnpr interface-specifier:subscriber-session-id</i>; For example, <i>jnpr fastEthernet 3/2.6:1010101010101</i></li> </ul>	No
45	Acct-Authentic	Method by which user was authentication: whether by RADIUS, the NAS itself, or another remote authentication protocol.	No
46	Acct-Session-Time	Number of seconds that the user has received service	No
47	Acct-Input-Packets	Number of packets that have been received from the port during the time this service has been provided to a framed user.	No
48	Acct-Output-Packets	Number of packets that have been sent to the port in the course of delivering this service to a framed user.	No

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

Attribute Number	Attribute Name	Description	Dynamic CoA Support
49	Acct-Terminate-Cause	Reason the service (a PPP session) was terminated. The service can be terminated for the following reasons: <ul style="list-style-type: none"> <li>• User Request (1)—User initiated the disconnect (log out).</li> <li>• Idle Timeout (4)—Idle timer has expired.</li> <li>• Session Timeout (5)—Client reached the maximum continuous time allowed on the service or session.</li> <li>• Admin Reset (6)—System administrator terminated the session.</li> <li>• Port Error (8)—PVC failed; no hardware or no interface.</li> <li>• NAS Error (9)—Negotiation failures, connection failures, or address lease expiration.</li> <li>• 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.</li> </ul>	No
52	Acct-Input-Gigawords	Number of 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	No
53	Acct-Output-Gigawords	Number of 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.	No
55	Event-Timestamp	Time that this event occurred on the NAS, in seconds, since January 1, 1970 00:00 UTC.	No
61	NAS-Port-Type	Type of physical port the NAS is using to authenticate the user.	No



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

Attribute Number	Attribute Name	Description	Dynamic CoA Support
64	Tunnel-Type	<ul style="list-style-type: none"> <li>Tunneling protocol to use (in the case of a tunnel initiator) or the tunneling protocol already in use (in the case of a tunnel terminator).</li> <li>Only L2TP tunnels are currently supported.</li> </ul>	No
65	Tunnel-Medium-Type	<ul style="list-style-type: none"> <li>Transport medium to use when creating a tunnel for protocols that can operate over multiple transports.</li> <li>Only IPv4 is currently supported.</li> </ul>	No
66	Tunnel-Client-Endpoint	Address of the initiator end of the tunnel (LAC).	No
67	Tunnel-Server-Endpoint	Address of the server end of the tunnel (LNS).	No
69	Tunnel-Password	Encrypted password used to authenticate to a remote server. Recommended over using VSA Tunnel-Password [26-9] because of the encryption. Do not use both this attribute and the VSA.	No
82	Tunnel-Assignment -Id	LAC the tunnel to which a session is assigned. When user profiles share the same values for Tunnel-Assignment-Id, Tunnel-Server-Endpoint, and Tunnel-Type, the LAC can group these users into the same tunnel. This enables fewer tunnels to be created.	No
83	Tunnel-Preference	<ul style="list-style-type: none"> <li>If more than one set of tunneling attributes is returned by the RADIUS server to the tunnel initiator, this attribute is included in each set to indicate the relative preference assigned to each tunnel.</li> <li>Included in the Tunnel-Link-Start, the Tunnel-Link-Reject, and the Tunnel-Link-Stop packets (LAC only).</li> </ul>	No

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

Attribute Number	Attribute Name	Description	Dynamic CoA Support
85	Acct-Interim-Interval	<p>Number of seconds between each interim accounting update for this session.</p> <p>The router uses the following guidelines for interim accounting:</p> <ul style="list-style-type: none"> <li>Attribute value is within the acceptable range (600 to 86,400 seconds)—Accounting is updated at the specified interval.</li> <li>Attribute value of 0—No RADIUS accounting is performed.</li> <li>Attribute value is less than the minimum acceptable value—Accounting is updated at the minimum interval (600 seconds).</li> <li>Attribute value is greater than the maximum acceptable value—Accounting is updated at the maximum interval (86,400 seconds).</li> </ul>	No
87	NAS-Port-ID	Text string that identifies the physical interface of the NAS that is authenticating the user.	No
88	Framed-Pool	Name of an assigned address pool to use to assign an address for the user.	No
90	Tunnel-Client-Auth-Id	Name of the tunnel initiator (LAC) used during the authentication phase of tunnel establishment.	No
91	Tunnel-Server-Auth-Id	Name of the tunnel terminator (LNS) used during the authentication phase of tunnel establishment.	No
95	NAS-IPv6-Address	Address of the NAS that is requesting authentication of the user.	No
96	Framed-Interface-ID	Interface identifier that is configured for the user.	No
97	Framed-IPv6-Prefix	IPv6 prefix that is configured for the user.	No
98	Login-IPv6-Host	System the user connects to when the Login-Service attribute is included.	No
99	Framed-IPv6-Route	IPv6 routing information that is configured for the user.	Yes

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

Attribute Number	Attribute Name	Description	Dynamic CoA Support
100	Framed-IPv6-Pool	Name of the assigned pool used to assign an IPv6 prefix for the user.	No
123	Delegated-IPv6-Prefix	Prefix that is delegated to the user.	No
242	Ascend-Data-Filter	Binary data that specifies RADIUS policy definitions.	Yes

## Juniper Networks VSAs Supported by the AAA Service Framework

Table 9 on page 45 describes Juniper Networks VSAs supported by the Junos OS AAA Service Framework. The AAA Service Framework uses vendor ID 4874, which is assigned to Juniper Networks by the Internet Assigned Numbers Authority (IANA).



**NOTE:** A “Yes” entry in the Dynamic CoA Support column indicates that the attribute can be dynamically configured by Access-Accept messages and dynamically modified by CoA-Request messages.

Table 9: Supported Juniper Networks VSAs

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-1	Virtual-Router	Client logical system:routing instance name. Allowed only from RADIUS server for “default” logical system:routing instance.	string: <i>logical system:routing instance</i>	No
26-4	Primary-DNS	Client DNS address negotiated during IPCP.	integer: 4-byte <i>primary-dns-address</i>	No
26-5	Secondary-DNS	Client DNS address negotiated during IPCP	integer: 4-byte <i>secondary-dns-address</i>	No
26-6	Primary-WINS	Client WINS (NBNS) address negotiated during IPCP.	integer: 4-byte <i>primary-wins-address</i>	No
26-7	Secondary-WINS	Client WINS (NBNS) address negotiated during IPCP.	integer: 4-byte <i>secondary-wins-address</i>	No
26-8	Tunnel-Virtual-Router	Virtual router name for tunnel connection.	string: <i>tunnel-virtual-router</i>	No

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

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-9	Tunnel-Password	Tunnel password in cleartext.  Do not use both this VSA and the standard RADIUS attribute Tunnel-Password [69]. The standard attribute is recommended because the password is encrypted when that attribute is used.	string: <i>tunnel-password</i>	No
26-10	Ingress-Policy-Name	Input policy name to apply to client interface.	string: <i>input-policy-name</i>	Yes
26-11	Egress-Policy-Name	Output policy name to apply to client interface.	string: <i>output-policy-name</i>	Yes
26-12	Ingress-Statistics	Enable or disable input statistics on a client interface.	integer: <ul style="list-style-type: none"> <li>0=disable</li> <li>1=enable</li> </ul>	No
26-13	Egress-Statistics	Enable or disable output statistics on a client interface.	integer: <ul style="list-style-type: none"> <li>0=disable</li> <li>1=enable</li> </ul>	No
26-23	IGMP-Enable	Enable or disable IGMP on a client interface.	integer: <ul style="list-style-type: none"> <li>0=disable</li> <li>1=enable</li> </ul>	Yes
26-25	Redirect-VRouter-Name	Client logical system:routing instance name indicating to which logical system:routing instance the request is redirected for user authentication.	string: <i>logical-system:routing-instance</i>	No
26-33	Tunnel-Max-Sessions	Maximum number of sessions allowed in a tunnel.	integer: 4-octet	No
26-34	Framed-IP-Route-Tag	Route tag to apply to returned framed-ip-address.	integer: 4-octet	No
26-42	Input-Gigapackets	Number of times the input-packets attribute rolls over its 4-octet field.	integer	No
26-43	Output-Gigapackets	Number of times the output-packets attribute rolls over its 4-octet field.	integer	No

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

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-55	DHCP-Options	Client DHCP options.	string: <i>dhcp-options</i>	No
26-56	DHCP-MAC-Address	Client MAC address.	string: <i>mac-address</i>	No
26-57	DHCP-GI-Address	DHCP relay agent IP address.	integer: 4-octet	No
26-58	LI-Action	Traffic mirroring action.  For dynamic CoA, VSA 26-58 changes the action on the mirrored traffic identified by VSA 26-59.	0=stop mirroring 1=start mirroring 2=no action	Yes (together with 26-59)
26-59	Med-Dev-Handle	Identifier that associates mirrored traffic to a specific subscriber.  For dynamic CoA, VSA 26-58 changes the action on the mirrored traffic identified by VSA 26-59.	Salt-encrypted string	Yes (together with 26-58)
26-60	Med-Ip-Address	IP address of content destination device to which mirrored traffic is forwarded.	Salt-encrypted IP address	No
26-61	Med-Port-Number	UDP port in the content destination device to which mirrored traffic is forwarded.	Salt-encrypted integer	No
26-63	Interface-Desc	Text string that identifies the subscriber's access interface.	string: <i>interface-description</i>	No
26-64	Tunnel-Group	Name of the tunnel group (profile) assigned to a domain map.	string: <i>tunnel-group-name</i>	No
26-65	Activate-Service	Service to activate for the subscriber.	string: <i>service-name</i>	No
26-66	Deactivate-Service	Service to deactivate for the subscriber.	string: <i>service-name</i>	No
26-69	Service-Statistics	Enable or disable statistics for the service.	<ul style="list-style-type: none"> <li>0 = disable</li> <li>1 = enable time statistics</li> <li>2 = enable time and volume statistics</li> </ul>	Yes
26-71	IGMP-Access-Name	Access list to use for the group (G) filter.	string: 32-octet	Yes

Table 9: Supported Juniper Networks VSAs (continued)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-72	IGMP-Access-Src-Name	Access list to use for the source-group (S,G) filter.	string: 32-octet	Yes
26-74	MLD-Access-Name	Access list to use for the group (G) filter.	string: 32-octet	Yes
26-75	MLD-Access-Src-Name	Access list to use for the source-group (S,G) filter.	string: 32-octet	Yes
26-77	MLD-Version	MLD protocol version.	integer: 1-octet <ul style="list-style-type: none"> <li>1=MLD version 1</li> <li>2=MLD version 2</li> </ul>	Yes
26-78	IGMP-Version	IGMP protocol version.	integer: 1-octet <ul style="list-style-type: none"> <li>1=IGMP version 1</li> <li>2=IGMP version 2</li> <li>3=IGMP version 3</li> </ul>	Yes
26-83	Service-Session	Name of the service.	string: <i>service-name</i>	No
26-84	Mobile-IP-Algorithm	Authentication algorithm used for Mobile IP registration.	integer: 4-octet	No
26-85	Mobile-IP-SPI	Security parameter index number for Mobile IP registration.	integer: 4-octet	No
26-86	Mobile-IP-Key	Security association MD5 key for Mobile IP registration.	string: key	No
26-87	Mobile-IP-Replay	Replay timestamp for Mobile IP registration.	integer: 4-octet	No
26-89	Mobile-IP-Lifetime	Registration lifetime for Mobile IP registration.	integer: 4-octet	No
26-97	IGMP-Immediate-Leave	IGMP Immediate Leave.	integer: 4-octet <ul style="list-style-type: none"> <li>0=disable</li> <li>1=enable</li> </ul>	Yes
26-100	MLD-Immediate-Leave	MLD Immediate Leave.	integer: 4-octet <ul style="list-style-type: none"> <li>0=disable</li> <li>1=enable</li> </ul>	Yes
26-106	IPv6-Ingress-Policy-Name	Input policy name to apply to a user IPv6 interface.	string: <i>policy-name</i>	Yes

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

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-107	IPv6-Egress-Policy-Name	Output policy name to apply to a user IPv6 interface.	string: <i>policy-name</i>	Yes
26-108	CoS-Parameter-Type	CoS traffic-shaping parameter type and description: <ul style="list-style-type: none"> <li>• <b>T01:</b> Scheduler-map name</li> <li>• <b>T02:</b> Shaping rate</li> <li>• <b>T03:</b> Guaranteed rate</li> <li>• <b>T04:</b> Delay-buffer rate</li> </ul>	Two parts, delimited by white space: <ul style="list-style-type: none"> <li>• Parameter type</li> <li>• Parameter value</li> </ul> Examples: <ul style="list-style-type: none"> <li>• <b>T01 smap_basic</b></li> <li>• <b>T02 50m</b></li> <li>• <b>T03 1m</b></li> <li>• <b>T04 2000</b></li> </ul>	Yes
26-109	DHCP-Guided-Relay-Server	IP address of DHCP server DHCP relay agent uses to forward the discover PDUs.	integer: 4-byte <i>ip-address</i>	No
26-129	IPv6-NdRa-Prefix	Prefix value in IPv6 neighbor discovery route advertisements.	hexadecimal string	No
26-130	Qos-Set-Name	Interface set to apply to the dynamic profile.	string: <i>interface-set-name</i>	Yes
26-140	Service-Interim-Acct-Interval	Amount of time between interim accounting updates for this service.	<ul style="list-style-type: none"> <li>• range = 600–86400 seconds</li> <li>• 0 = disabled</li> </ul>	Yes
26-143	Max-Clients-Per-Interface	Maximum allowable client sessions per interface. For DHCP clients, the maximum sessions per logical interface.	integer: 4-octet	No

Table 9: Supported Juniper Networks VSAs (continued)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-146	CoS-Scheduler-Pmt-Type	CoS scheduler parameter type and description: <ul style="list-style-type: none"> <li>• Null: CoS scheduler name</li> <li>• <b>T01</b>: CoS scheduler transmit rate</li> <li>• <b>T02</b>: CoS scheduler buffer size</li> <li>• <b>T03</b>: CoS scheduler priority</li> <li>• <b>T04</b>: CoS scheduler drop-profile low</li> <li>• <b>T05</b>: CoS scheduler drop-profile medium-low</li> <li>• <b>T06</b>: CoS scheduler drop-profile medium-high</li> <li>• <b>T07</b>: CoS scheduler drop-profile high</li> <li>• <b>T08</b>: CoS scheduler drop-profile any</li> </ul>	Three parts, delimited by white space: <ul style="list-style-type: none"> <li>• Scheduler name</li> <li>• Parameter type</li> <li>• Parameter value</li> </ul> Examples: <ul style="list-style-type: none"> <li>• <b>be_sched</b></li> <li>• <b>be_sched T01 12m</b></li> <li>• <b>be_sched T02 26</b></li> </ul>	Yes
26-151	IPv6-Acct-Input-Octets	IPv6 receive octets.	integer	No
26-152	IPv6-Acct-Output-Octets	IPv6 transmit octets.	integer	No
26-153	IPv6-Acct-Input-Packets	IPv6 receive packets.	integer	No
26-154	IPv6-Acct-Output-Packets	IPv6 transmit packets.	integer	No
26-155	IPv6-Acct-Input-Gigawords	IPv6 receive gigawords.	integer	No
26-156	IPv6-Acct-Output-Gigawords	IPv6 transmit gigawords.	integer	No
26-157	IPv6-NdRa-Pool-Name	IPv6 ND/RA pool name used to locally allocate an ND/RA prefix.	string	No

## DSL Forum Vendor-Specific Attributes

Digital Subscriber Line (DSL) attributes are RADIUS vendor-specific attributes (VSAs) that are defined by the DSL Forum. The attributes transport DSL information that is not supported by standard RADIUS attributes and which convey information about the associated DSL subscriber and data rate. The attributes are defined in RFC 4679, *DSL Forum Vendor-Specific RADIUS Attributes*.



**NOTE:** Junos OS uses the vendor ID 3561, which is assigned by the Internet Assigned Numbers Authority (IANA), for the DSL Forum VSAs.



Subscriber management does not process DSL values—the router simply passes the values received from the subscriber to the RADIUS server, without performing any parsing or manipulation. However, you can manage the content of DSL VSA values either by using the client configuration to restrict the DSL VSAs that the client sends, or by configuring the RADIUS server to ignore unwanted DSL VSAs.

Table 10 on page 51 describes the DSL Forum VSAs.

**Table 10: DSL Forum VSAs**

Attribute Number	Attribute Name	Description	Value
[26-1]	Agent-Circuit-Id	Identifier for the subscriber agent circuit ID that corresponds to the DSLAM interface from which subscriber requests are initiated	string
[26-2]	Agent-Remote-Id	Unique identifier for the subscriber associated with the DSLAM interface from which requests are initiated	string
[26-129]	Actual-Data-Rate-Upstream	Actual upstream data rate of the subscriber's synchronized DSL link	integer: 4-octet
[26-130]	Actual-Data-Rate-Downstream	Actual downstream data rate of the subscriber's synchronized DSL link	integer: 4-octet
[26-131]	Minimum-Data-Rate-Upstream	Minimum upstream data rate configured for the subscriber	integer: 4-octet
[26-132]	Minimum-Data-Rate-Downstream	Minimum downstream data rate configured for the subscriber	integer: 4-octet
[26-133]	Attainable-Data-Rate-Upstream	Upstream data rate that the subscriber can attain	integer: 4-octet
[26-134]	Attainable-Data-Rate-Downstream	Downstream data rate that the subscriber can attain	integer: 4-octet
[26-135]	Maximum-Data-Rate-Upstream	Maximum upstream data rate configured for the subscriber	integer: 4-octet
[26-136]	Maximum-Data-Rate-Downstream	Maximum downstream data rate configured for the subscriber	integer: 4-octet
[26-137]	Minimum-Data-Rate-Upstream-Low-Power	Minimum upstream data rate in low power state configured for the subscriber	integer: 4-octet
[26-138]	Minimum-Data-Rate-Downstream-Low-Power	Minimum downstream data rate in low power state configured for the subscriber	integer: 4-octet
[26-139]	Maximum-Interleaving-Delay-Upstream	Maximum one-way upstream interleaving delay configured for the subscriber	integer: 4-octet

Table 10: DSL Forum VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value
[26-140]	Actual-Interleaving-Delay-Upstream	Subscriber's actual one-way upstream interleaving delay	integer: 4-octet
[26-141]	Maximum-Interleaving-Delay-Downstream	Maximum one-way downstream interleaving delay configured for the subscriber	integer: 4-octet
[26-142]	Actual-Interleaving-Delay-Downstream	Subscriber's actual one-way downstream interleaving delay	integer: 4-octet
[26-144]	Access-Loop-Encapsulation	Encapsulation used by the subscriber associated with the DSLAM interface from which requests are initiated	string: 3-byte
[26-254]	IWF-Session	Indication that the interworking function (IWF) has been performed for the subscriber's session	No data field required

## 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 11 on page 52 describes the error-cause codes.

Table 11: 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 request	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).

## Configuring an Access Profile for Subscriber Management

Access profiles enable you to specify subscriber access authentication and accounting parameters. After access profiles are created, you can attach them at the **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name*]** hierarchy level or for use in automatically configuring VLANs or stacked VLANs at the **[edit interfaces *interface-name* auto-configure *vlan-ranges*]** or **[edit interfaces *interface-name* auto-configure *stacked-vlan-ranges*]** hierarchy levels.

To configure an access profile:

1. Edit the access stanza.

```
[edit]
user@host# edit access
```

2. Specify an existing or new access profile name.

```
[edit access]
user@host# edit profile profile-name
```

3. Specify any desired subscriber access authentication and accounting parameters for the access profile.

### Related Documentation

- Attaching Access Profiles on page 53
- Configuring Dynamic Authentication for VLAN Interfaces on page 424
- **profile** on page 1127

## Attaching Access Profiles

After you have created the access profile that specifies the subscriber access management authentication and accounting parameters, you can attach the profile. Subscriber access management supports attaching access profiles at the following hierarchy levels:

- **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name*]**
- **[edit interfaces *interface-name* auto-configure *vlan-ranges*]**
- **[edit interfaces *interface-name* auto-configure *stacked-vlan-ranges*]**

To attach an access profile:

1. Edit the desired hierarchy level.

```
[edit]
user@host# edit logical-systems LS1 routing-instances R11
```

2. Specify the name of the access profile that you want to attach.

```
[edit logical-systems logical-system-name routing-instances routing-instance-name]
user@host# set access-profile vz-bos-metro-fios-basic
```

**Related Documentation**

- AAA Service Framework Overview on page 18

## Understanding Session Options for Subscriber Access

---

You can limit subscriber access by configuring a session timeout or an idle timeout. Use a session timeout to specify a fixed period of time that the subscriber is permitted to have access. Use an idle timeout to specify a maximum period of time that the subscriber can be idle. You can use these timeouts separately or together. By default, neither timeout is present.



**NOTE:** For all subscriber types other than DHCP, the session timeout value limits the subscriber session. For DHCP subscribers, the session timeout value is used to limit the lease. The lease expires when the timeout value expires. If this value is not supplied by either the CLI or RADIUS, the DHCP lease does not expire.

The idle timeout is based on accounting statistics for the subscriber. The router determines subscriber inactivity by monitoring data traffic, both upstream from the user and downstream to the user. Control traffic is ignored. The subscriber is not considered idle as long as traffic is detected in either direction.

When either timeout period expires, the non-DHCP subscribers are gracefully logged out, similarly to a RADIUS-initiated disconnect or a CLI-initiated logout. DHCP subscribers are disconnected. The Acct-Terminate-Cause [RADIUS attribute 49] value includes a reason code of 5 for a session timeout and a code of 4 for an idle timeout.

You can configure these limitations to subscriber access on a per-subscriber basis by using the RADIUS attributes Session-Timeout [27] and Idle-Timeout [28]. RADIUS returns these attributes in Access-Accept messages in response to Access-Request messages from the access server.

However, service providers often choose to apply the same limitations to large numbers of subscribers. You can reduce the RADIUS provisioning effort for this scenario by defining the limitations for subscribers in an access profile on a per-routing-instance basis. If you do so, RADIUS attributes subsequently returned for a particular subscriber logged in with the profile override the per-routing-instance values.

The available range for setting a timeout is the same whether you configure it in the CLI or through the RADIUS attributes. Session timeouts can be set for 1 minute through 527,040 minutes in the CLI and the corresponding number of seconds (60 through 31,622,400) in the Session-Timeout attribute [27]. Idle timeouts can be set for 10 minutes through 1440 minutes in the CLI and the corresponding number of seconds (600 through 86,400) in the Idle-Timeout attribute [28].

The router interprets the values in the attributes to conform to the supported ranges. For example, for Session-Timeout [27]:

- A value of zero is treated as no timeout.

- A value in the range 1 through 59 is raised to 60 seconds.
- A value that exceeds 31,622,400 is reduced to 31,622,400 seconds.

For Idle-Timeout [28]:

- A value of zero is treated as no timeout.
- A value in the range 1 through 599 is raised to 600 seconds.
- A value that exceeds 86,400 is reduced to 86,400 seconds.

**Related  
Documentation**

- RADIUS IETF Attributes Supported by the AAA Service Framework on page 39
- Configuring Subscriber Session Options on page 55

## Configuring Subscriber Session Options

Subscriber session timeouts enable you to place limits on subscriber access based on how long the session has been up, how long the user has been inactive, or both.



**NOTE:** To configure the timeout attributes in RADIUS, refer to the documentation for your RADIUS server.

To configure limitations on subscriber sessions:

1. Configure the maximum period a subscriber session can be active.

```
[edit access profile profile-name]
user@host# set client-session-timeout minutes
```

2. Configure the maximum period a subscriber session can be idle.

```
[edit access profile profile-name]
user@host# set client-idle-timeout minutes
```

For example, to configure a client session timeout of 2 hours and an idle timeout of 15 minutes in the **acc-prof** profile:

```
[edit]
access {
  profile {
    acc-prof {
      session-options {
        client-session-timeout 120;
        client-idle-timeout 15;
      }
    }
  }
}
```

**Related  
Documentation**

- Understanding Session Options for Subscriber Access on page 54
- **client-idle-timeout** on page 888

- [client-session-timeout](#) on page 889

## AAA Configuration Testing and Troubleshooting

---

Subscriber management supports a test feature that enables you to check the AAA configuration of a subscriber. You might use the test feature to verify the subscriber's AAA settings and to help troubleshoot or isolate subscriber login problems. The AAA test process creates a pseudo session that authenticates the subscriber, allocates an address for the subscriber, and issues an accounting start packet. The process then issues an accounting stop request, releases the address, and terminates the pseudo session.

The AAA test results provide details about the attributes that subscriber management assigns to the subscriber during login. The attributes might be assigned by RADIUS, a dynamic profile, static interface configuration, or might be statically assigned. You can test the AAA configuration for DHCP, PPP, and authd-lite subscribers. For L2TP clients, the AAA test process displays all tunnel parameters but does not create an actual tunnel session.



**NOTE:** The **test** command does not support volume-time accounting. If volume-time accounting is configured for the test subscriber, the **test** command replaces the statistics with time-only accounting statistics.

### Related Documentation

- [Testing a Subscriber AAA Configuration](#) on page 56

## Testing a Subscriber AAA Configuration

---

**Purpose** Display the AAA attributes that subscriber management assigns to the subscriber during login.

The following example tests the AAA configuration for a PPP subscriber. You can use the **test aaa dhcp user** command to perform a similar test for DHCP subscribers and the **test aaa authd-lite user** command to test authd-lite subscribers.



**NOTE:** The **test** command does not support volume-time accounting. If volume-time accounting is configured for the test subscriber, the **test** command replaces the statistics with time-only accounting statistics.

**Action** `user@host>test aaa ppp user thomastank password 00N15&`

```
Authentication Grant
*****User Attributes*****
  User Name -                thomastank
  Client IP Address -        192.168.1.1
  Client IP Netmask -        255.255.0.0
  Virtual Router Name -      default
  Reply Message -            NULL
```

```

Primary DNS IP Address -          0.0.0.0
Secondary DNS IP Address -       0.0.0.0
Primary WINS IP Address -        0.0.0.0
Secondary WINS IP Address -      0.0.0.0
Framed Pool -                    addr_pool2
Session Timeout -                0
Idle Timeout -                   0
Service Type -                   0
Client Ipv6 Address -            ::
Client Ipv6 Mask -               null
Framed Ipv6 Prefix -             ::/0
Framed Ipv6 Pool -              not-set
Nas Ipv6 Address -               ::
NDRA Ipv6 Prefix -              not-set
Login Ipv6 Host -                ::
Framed Interface Id: -          0:0:0:0
Delegated Ipv6 Prefix -         ::/0
Delegated Ipv6 Pool -           not-set
User Password -                  00N15&
CHAP Password -                 NULL
NAS Ip Address -                 0.0.0.0
NAS Port -                       0
NAS Port Type -                  5
Client Session Activate request sent
Client Session Activated
Filter Id -                      not set
Framed MTU -                     (null)
Framed Route -                   not set
Ingress Policy Name -            not set
Egress Policy Name -             not set
IGMP -                           disabled
Redirect VR Name -               default
Service Bundle -                 Null
Framed Ip Route Tag -            not set
LI Action -                      0
LI Intercpet Id -                0
Med Ipaddress -                  0.0.0.0
Med Port Number -                0
Ignore DF Bit -                  disabled
IGMP Access Group Name -         not set
IGMP Access Source Group Name -  not set
MLD Access Group Name -          not set
MLD Access Source Group Name -   not set
IGMP Version -                   IGMP Version not set
MLD Version -                     MLD Version not set
IGMP Immediate Leave -           disabled
MLD Immediate Leave -            disabled
IPv6 Ingress Policy Name -        not set
IPv6 Egress Policy Name -         not set
Cos Parameter Type -              not-set
Cos Scheduler Parameter Type -    not-set
Acct Session ID-                  8
Acct Interim Interval -           0
Acct Type -                       0
Ingress Statistics                 disabled
Egress Statistics                  disabled
****Pausing 10 seconds before disconnecting the test user*****
Logging out subscriber

```

Test complete. Exiting

**Related Documentation** • AAA Configuration Testing and Troubleshooting on page 56

---

## Tracing Subscriber Management Database Operations for Subscriber Access

The Junos OS trace feature tracks subscriber management database operations and records events 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 **smid** located in the **/var/log** directory. You cannot change the directory (**/var/log**) in which trace files are located.
2. When the file **smid** reaches 128 kilobytes (KB), it is renamed **smid.0**, then **smid.1**, and finally **smid.2**, until there are three trace files. Then the oldest trace file (**smid.2**) is overwritten.

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

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To configure all aspects of subscriber management database tracing operations:

1. Configure a trace log filename.  
See “Configuring the Subscriber Management Database Trace Log Filename” on page 59.
2. Configure the number and size of trace logs.  
See “Configuring the Number and Size of Subscriber Management Database Log Files” on page 59.
3. Configure user access to trace logs.  
See “Configuring Access to the Subscriber Management Database Log File” on page 59.
4. Configure a regular expression to filter the information to be included in the trace log.  
See “Configuring a Regular Expression for Subscriber Management Database to Be Logged” on page 60.
5. Configure flags to specify which events are logged.  
See “Configuring the Subscriber Management Database Tracing Flags” on page 60.



## Related Documentation

### Configuring the Subscriber Management Database Trace Log Filename

By default, the name of the file that records trace output for the subscriber management database is **smid**. You can specify a different name with the **file** option.

To configure the filename for subscriber management database tracing operations:

- Specify the name of the file used for the trace output.

```
[edit system services subscriber-management traceoptions]
user@host# set file smi_logfile_1
```

## Related Documentation

- Tracing Subscriber Management Database Operations for Subscriber Access on page 58
- traceoptions on page 1236

### Configuring the Number and Size of Subscriber Management Database Log Files

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

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

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.

```
[edit system services subscriber-management traceoptions]
user@host# set file smi_1_logfile_1 files 20 size 2097152
```

## Related Documentation

- Tracing Subscriber Management Database Operations for Subscriber Access on page 58
- traceoptions on page 1236

### Configuring Access to the Subscriber Management Database Log File

By default, only the user who configures the tracing operation can access the log files. 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 system services subscriber-management traceoptions]
user@host# set file smi_1_logfile_1 world-readable
```

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

- Configure the log file to be no-world-readable.

```
[edit system services subscriber-management traceoptions]
user@host# set file smi_1_logfile_1 no-world-readable
```

#### Related Documentation

- Tracing Subscriber Management Database Operations for Subscriber Access on page 58
- [traceoptions on page 1236](#)

## Configuring a Regular Expression for Subscriber Management Database 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 to be matched.

To configure regular expressions to be matched:

- Configure the regular expression.

```
[edit system services subscriber-management traceoptions]
user@host# set file smi_1_logfile_1 match regex
```

#### Related Documentation

- Tracing Subscriber Management Database Operations for Subscriber Access on page 58
- [traceoptions on page 1236](#)

## Configuring the Subscriber Management Database 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
<b>all</b>	Trace all operations
<b>database</b>	Trace database events
<b>general</b>	Trace general events
<b>issu</b>	Trace unified ISSU events

Flag	Description
<b>server</b>	Trace server events
<b>session-db</b>	Trace session database interactions
<b>ui</b>	Trace user interface events

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit system services subscriber-management traceoptions]
user@host# set flag flag
```

**Related  
Documentation**

- Tracing Subscriber Management Database Operations for Subscriber Access on page 58
- **traceoptions** on page 1236

## Tracing Subscriber Management Session Database Replication Operations for Subscriber Access

The Junos OS trace feature tracks subscriber management database replication operations and records events 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 **bdbrepd** located in the **/var/log** directory. You cannot change the directory (**/var/log**) in which trace files are located.
2. When the file **bdbrepd** reaches 128 kilobytes (KB), it is renamed **bdbrepd.0**, then **bdbrepd.1**, and finally **bdbrepd.2**, until there are three trace files. Then the oldest trace file (**bdbrepd.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 OS System Log Messages Reference](#).)

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To configure all aspects of subscriber management database replication tracing operations:

1. Configure a trace log filename.

See “Configuring the Subscriber Management Session Database Replication Trace Log Filename” on page 64.

2. Configure the number and size of trace logs.

See “Configuring the Number and Size of Subscriber Management Session Database Replication Log Files” on page 62.

3. Configure user access to trace logs.

See “Configuring Access to the Subscriber Management Session Database Replication Log File” on page 63.

4. Configure a regular expression to filter the information to be included in the trace log.

See “Configuring a Regular Expression for Subscriber Management Session Database Replication to Be Logged” on page 63.

5. Configure flags to specify which events are logged.

See “Configuring the Subscriber Management Session Database Replication Tracing Flags” on page 64.

---

## Configuring the Number and Size of Subscriber Management Session Database Replication Log Files

---

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

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

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.

```
[edit system services database-replication traceoptions]  
user@host# set file bdrep_1_logfile_1 files 20 size 2097152
```

### Related Documentation

- Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 61

- [traceoptions on page 1238](#)

## Configuring a Regular Expression for Subscriber Management Session Database Replication 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 to be matched.

To configure regular expressions to be matched:

- Configure the regular expression.

```
[edit system services database-replication traceoptions]  
user@host# set file bdrep_1_logfile_1 match regex
```

### Related Documentation

- [Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 61](#)
- [traceoptions on page 1238](#)

## Configuring Access to the Subscriber Management Session Database Replication Log File

---

By default, only the user who configures the tracing operation can access the log files. 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 system services database-replication traceoptions]  
user@host# set file bdrep_1_logfile_1 world-readable
```

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

- Configure the log file to be no-world-readable.

```
[edit system services database-replication traceoptions]  
user@host# set file bdrep_1_logfile_1 no-world-readable
```

### Related Documentation

- [Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 61](#)
- [traceoptions on page 1238](#)

## Configuring the Subscriber Management Session Database Replication Trace Log Filename

By default, the name of the file that records trace output for the subscriber management database is **bdbrepd**. You can specify a different name with the **file** option.

To configure the filename for subscriber management database tracing operations:

- Specify the name of the file used for the trace output.

```
[edit system services database-replication traceoptions]  
user@host# set file bdbrep_logfile_1
```

### Related Documentation

- Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 61
- traceoptions** on page 1238

## Configuring the Subscriber Management Session Database Replication 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
<b>all</b>	Trace all operations
<b>database</b>	Trace database events
<b>general</b>	Trace general events
<b>mirror</b>	Trace mirroring events
<b>replication</b>	Trace database replication events
<b>server</b>	Trace server events
<b>session-db</b>	Trace session database interactions
<b>ui</b>	Trace user interface events

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit system services database-replication traceoptions]  
user@host# set flag flag
```

- Related Documentation**
- [Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 61](#)
  - [traceoptions on page 1238](#)

---

## Verifying and Managing Subscriber AAA Information

---

**Purpose** View or clear subscriber access statistics and information.

- Action**
- To display subscriber AAA statistics:  
user@host> **show network-access aaa statistics**
  - To display subscriber access AAA information:  
user@host> **show network-access aaa subscribers**
  - To display subscriber session information:  
user@host> **show network-access aaa subscribers session-id session-id**
  - To clear subscriber access statistics and to log out specific subscribers:  
user@host> **clear network-access aaa subscriber**
  - To clear AAA accounting statistics:  
user@host> **clear network-access aaa statistics accounting**
  - To clear AAA address-assignment statistics for a client:  
user@host> **clear network-access aaa statistics address-assignment client**
  - To clear AAA address-assignment pool statistics:  
user@host> **clear network-access aaa statistics address-assignment pool pool-name**
  - To clear AAA authentication statistics:  
user@host> **clear network-access aaa statistics authentication**

- Related Documentation**
- [Junos OS System Basics and Services Command Reference](#)





## CHAPTER 3

# Configuring Address-Assignment Pools for Subscriber Access

- Address-Assignment Pools Overview on page 67
- Configuring Address-Assignment Pools on page 68
- Configuring an Address-Assignment Pool Name and Addresses on page 69
- Configuring a Named Address Range for Dynamic Address Assignment on page 69
- Configuring Address-Assignment Pool Linking on page 70
- Configuring Static Address Assignment on page 71
- Configuring Address-Assignment Pool Usage Threshold Traps on page 71
- Configuring DHCP Client-Specific Attributes on page 72
- DHCP Attributes for Address-Assignment Pools on page 73
- Address-Assignment Pools Licensing Requirements on page 74
- Tracing General Authentication Service Processes on page 74

### Address-Assignment Pools Overview

---

The address-assignment pool feature supports subscriber management functionality by enabling you to create IPv4 and IPv6 address pools that different client applications can share. 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, which is supported for IPv4 pools only, 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.

You can configure named address ranges within an address-assignment pool. A named range is a subset of the overall address range. A client application can use named ranges to manage address assignment based on client-specific criteria. For example, for IPv4 address-assignment pools, 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.

You can link address-assignment pools together to provide backup pools for address assignment. When the primary pool is fully allocated, the router switches to the linked, or secondary, pool and begins allocating addresses from that pool.

You can also explicitly identify that an address-assignment pool is used for ND/RA.

**Related  
Documentation**

- [Configuring Address-Assignment Pools on page 68](#)
- [Address-Assignment Pools Licensing Requirements on page 74](#)
- [Example: Configuring an Address-Assignment Pool on page 93](#)

---

## 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. An address-assignment pool can support either IPv4 address or IPv6 addresses. You cannot use the same pool for both types of address.



.....

**NOTE:** You cannot use address-assignment pools with the J Series Services Routers 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:

1. Configure the address-assignment pool name and specify the addresses for the pool.  
See “Configuring an Address-Assignment Pool Name and Addresses” on page 69.
2. (Optional) Configure named ranges (subsets) of addresses.  
See “Configuring a Named Address Range for Dynamic Address Assignment” on page 69.
3. (Optional) Configure address-assignment pool linking and specify the secondary pool to use when the primary pool is fully allocated.  
See “Configuring Address-Assignment Pool Linking” on page 70.
4. (Optional) Create static address bindings (IPv4 only).  
See “Configuring Static Address Assignment” on page 71.
5. (Optional) Configure attributes for DHCP clients.  
See “Configuring DHCP Client-Specific Attributes” on page 72.
6. (Optional) Specify that the address-assignment pool is used for router advertisement.  
See [Configuring an Address-Assignment Pool for Router Advertisement](#).

- Related Documentation**
- Address-Assignment Pools Overview on page 67
  - Address-Assignment Pools Licensing Requirements on page 74
  - Example: Configuring an Address-Assignment Pool on page 93

## Configuring an Address-Assignment Pool Name and Addresses

---

To configure an address-assignment pool, you must specify the name of the pool and configure the addresses for the pool.

To configure an IPv4 address-assignment pool:

1. Configure the name of the pool and specify the IPv4 family.  

```
[edit access]  
user@host# edit address-assignment pool isp_1 family inet
```
2. Configure the network address and the prefix length of the addresses in the pool.  

```
[edit access address-assignment pool isp_1 family inet]  
user@host# set network 192.168.0.0/16
```

To configure an IPv6 address-assignment pool:

1. Configure the name of the pool and specify the IPv6 family.  

```
[edit access]  
user@host# edit address-assignment pool isp_2 family inet6
```
2. Configure the IPv6 network prefix for the address pool. The prefix specification is required when you configure an IPv6 address-assignment pool.  

```
[edit access address-assignment pool isp_2 family inet6]  
user@host# set prefix 2008:2009::/32
```

- Related Documentation**
- Address-Assignment Pools Overview on page 67
  - Configuring Address-Assignment Pools on page 68

## Configuring a Named Address Range for Dynamic Address Assignment

---

You can optionally configure multiple named ranges, or 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, you specify a name for the range and define the address range.

To create a named range within an IPv4 address-assignment pool:

1. Specify the name of the address-assignment pool and the IPv4 family.  

```
[edit access]  
user@host# edit address-assignment pool isp_1 family inet
```

2. Configure the name of the range and the lower and upper boundaries of the addresses in the range.

```
[edit access address-assignment pool isp_1 family inet]
user@host# set range southeast low 192.168.102.2 high 192.168.102.254
```

To create a named range within an IPv6 address-assignment pool:

1. Specify the name of the address-assignment pool and the IPv6 family.

```
[edit access]
user@host# edit address-assignment pool isp_2 family inet6
```

2. Configure the name of the range and define the range. You can define the range based on the lower and upper boundaries of the prefixes in the range, or based on the length of the prefixes in the range.

```
[edit access address-assignment pool isp_2 family inet6]
user@host# set range dsl-range low 2008:2010:2011:0100::/64 high
2008:2010:2011:ffff::/64
user@host# set range fiber-east prefix-length 48
```

- Related Documentation**
- Address-Assignment Pools Overview on page 67
  - Configuring Address-Assignment Pools on page 68

---

## Configuring Address-Assignment Pool Linking

---

Address-assignment pool linking enables you to specify a secondary address pool for the router to use when the primary address-assignment pool is fully allocated. When the primary pool is has no available addresses, the router automatically switches over to the linked secondary pool and begins allocating addresses from that pool. The router uses a secondary pool only when the primary address-assignment pool is fully allocated.

You can create a chain of multiple linked pools. For example you can link pool A to pool B, and link pool B to pool C. When pool A has no available addresses, the router switches to using pool B for addresses. When pool B is exhausted, the router switches to pool C. There is no limit to the number of linked pools in a chain. However, you cannot create multiple links to or from the same pool—a pool can be linked to only one secondary pool, and a secondary pool can be linked from only one primary pool. Also, two linked primary and secondary pools must be of the same family type, either IPv4 or IPv6.

To link an address-assignment pool to a secondary pool:

1. Specify the name of the primary address-assignment pool.

```
[edit access]
user@host# edit address-assignment pool pool-name
```

2. Configure the secondary pool to which the primary pool will be linked.

```
[edit access address-assignment pool isp_1]
user@host# set link pool-name
```

- Related Documentation**
- Address-Assignment Pools Overview on page 67
  - Address-Assignment Pools Licensing Requirements on page 74
  - Example: Configuring an Address-Assignment Pool on page 93

## Configuring Static Address Assignment

You can optionally create a static IPv4 address binding by reserving a specific address for a particular client. The address is removed from the address-assignment pool so that it is not assigned to another client. When you reserve an address, you identify the client host and create a binding between the client MAC address and the assigned IP address. IPv6 address-assignment pools do not support static address binding.

To configure a static binding for an IPv4 address:

1. Specify the name of the IPv4 address-assignment pool containing the IP address you want to reserve for the client.

```
[edit access]
user@host# edit address-assignment pool isp_1 family inet
```

2. Specify the name of the client for the static binding, the client MAC address, and the IP address to reserve for the client. This configuration specifies that the client with MAC address 90:00:00:01:00:01 is always assigned IP address 192.168.44.12.

```
[edit access address-assignment pool isp_1 family inet]
user@host# set host svale6_boston_net hardware-address 90:00:00:01:00:01
ip-address 192.168.44.12
```

- Related Documentation**
- Address-Assignment Pools Overview on page 67
  - Configuring Address-Assignment Pools on page 68

## Configuring Address-Assignment Pool Usage Threshold Traps

You can receive advanced warning that an address pool or linked set of address pools is running short on available addresses by setting usage threshold traps. An address pool has SNMP thresholds associated with it that allow the local address server to signal SNMP traps when certain conditions exist. These thresholds include high utilization threshold and abated utilization threshold. If a pool's outstanding addresses exceed the high utilization threshold and the SNMP trap signaling is enabled, SNMP is notified. Likewise, when a pool's utilization drops below the abated threshold utilization threshold, SNMP is notified. When the system reaches the high utilization value, it sends warning messages. When memory usage falls to the abated utilization value, the system stops sending warning messages.

To set the usage for threshold traps:

- Specify the percentage after which the address pool usage is exceeded that an SNMP trap is generated.

```
[edit access]
user@host# edit address-assignment highUtilization 95
```

To set the abated value for the trap:

- Specify the percentage below which the address pool usage is abated that an SNMP trap is generated.

```
[edit access]
user@host# edit address-assignment abatedUtilization 80
```

**Related  
Documentation**

- Address-Assignment Pools Overview on page 67
- Example: Configuring an Address-Assignment Pool on page 93

---

## Configuring DHCP Client-Specific Attributes

You 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.

You use the **dhcp-attributes** statement to configure DHCP client-specific attributes for address-assignment pools. “DHCP Attributes for Address-Assignment Pools” on page 73 describes the supported attributes you can configure for IPv4 and IPv6 address-assignment pools.

To configure address-assignment pool attributes for DHCP clients:

1. Specify the name and IP family of the address-assignment pool.

```
[edit access]
user@host# edit address-assignment pool isp_1 family inet
```

2. Configure optional DHCP client attributes.

```
[edit access address-assignment pool isp_1 family inet]
user@host# set dhcp-attributes boot-server 192.168.200.100 grace-period 3600
maximum-lease-time 18000
```

**Related  
Documentation**

- Address-Assignment Pools Overview on page 67
- Configuring Address-Assignment Pools on page 68
- DHCP Attributes for Address-Assignment Pools on page 73

## DHCP Attributes for Address-Assignment Pools

Table 12 on page 73 describes the DHCP client attributes that you can use with the **dhcp-attributes** statement when you configure address-assignment pools. Table 13 on page 73 describes the DHCPv6 client attributes for configuring IPv6 address-assignment pools.

Table 12: DHCP Attributes

Attribute	Description	DHCP Option
<b>boot-file</b>	Boot filename advertised to the client, and used by the client to complete configuration.	67
<b>boot-server</b>	Boot server containing the boot file.	66
<b>domain-name</b>	Domain in which clients search for a DHCP server host.	15
<b>grace-period</b>	Grace period offered with the lease.	—
<b>maximum-lease-time</b>	Maximum lease time allowed by the DHCP server.	51
<b>name-server</b>	IP address of domain name server.	6
<b>netbios-node-type</b>	NetBIOS node type.	46
<b>option</b>	User-defined options.	—
<b>option-match</b>	Maps option 82 value to named address range.	—
<b>router</b>	IP address for routers on the subnetwork.	3
<b>server-identifier</b>	IP address used as the DHCP source address	54
<b>tftp-server</b>	Trivial File Transfer Protocol (TFTP) server that the client uses to obtain the client configuration file.	150
<b>wins-server</b>	IP address of the Windows NetBIOS name server.	44

Table 13: DHCPv6 Attributes

Attribute	Description	DHCPv6 Option
<b>dns-server</b>	IPv6 address of DNS server to which clients can send DNS queries.	23
<b>grace-period</b>	Grace period offered with the lease.	—
<b>maximum-lease-time</b>	Maximum lease time allowed by the DHCP server.	—

Table 13: DHCPv6 Attributes (*continued*)

Attribute	Description	DHCPv6 Option
<b>option</b>	User-defined options.	—
<b>sip-server-address</b>	IPv6 address of SIP outbound proxy server.	22
<b>sip-server-domain-name</b>	Domain name of the SIP outbound proxy server.	21

**Related Documentation**

- Address-Assignment Pools Overview on page 67
- Configuring Address-Assignment Pools on page 68
- Configuring DHCP Client-Specific Attributes on page 72

## Address-Assignment Pools Licensing Requirements

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

**Related Documentation**

- For information about installing and managing Junos OS licenses, see the “Managing Junos OS Licenses” chapter of the *Junos OS Installation and Upgrade Guide*

## Tracing General Authentication Service Processes

The Junos OS trace operations feature tracks general authentication service operations and records events in a log file. By default, the tracing operation is inactive. To trace general authentication service processes, you 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 located in the **/var/log** directory. By default, the router uses the filename, **authd**. You can specify a different filename, but you cannot change the directory (**/var/log**) in which trace files are located.
- When the file **authd** reaches 128 kilobytes (KB), it is renamed **authd.0**, then **authd.1**, and finally **authd.2**, until there are three trace files. Then the oldest trace file (**authd.2**) is overwritten. For more information about how log files are created, see the *Junos OS System Log Messages Reference*.



- By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

The general authentication service tracing operations are described in the following sections:

- Configuring the General Authentication Service Processes Trace Log Filename on page 75
- Configuring the Number and Size of General Authentication Service Processes Log Files on page 75
- Configuring Access to the Log File on page 76
- Configuring a Regular Expression for Lines to Be Logged on page 76
- Configuring the Trace Operation on page 76

### Configuring the General Authentication Service Processes Trace Log Filename

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

To configure the filename for general authentication service tracing operations:

- Specify the name of the file used for the trace output.

```
[edit system processes general-authentication-service traceoptions]
user@host# set file aap_logfile_1
```

### Configuring the Number and Size of General Authentication Service Processes Log Files

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

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

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, by including the **files** and **size** options with the **traceoptions** statement.

```
[edit system processes general-authentication-service traceoptions]
user@host# set file aap_logfile_1 files 20 size 2097152
```

## Configuring Access to the Log File

By default, log files can be accessed only by the user who configures the tracing operation. You can allow 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 system processes general-authentication-service traceoptions]  
user@host# set file aap_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 system processes general-authentication-service traceoptions]  
user@host# set file aap_logfile_1 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 regular expressions (regex) that will be matched.

To configure regular expressions to match:

- Configure the regular expression.

```
[edit system processes general-authentication-service traceoptions]  
user@host# set file aap_logfile_1 match regular-expression
```

## Configuring the Trace Operation

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
address-assignment	Trace all address-assignment pool events
all	Trace all tracing operations
configuration	Trace configuration events
framework	Trace authentication framework events
gx-plus	Trace Gx-Plus events
jsrc	Trace JSRC events
ldap	Trace LDAP authentication events

Flag	Description
local-authentication	Trace local authentication events
radius	Trace RADIUS authentication events

To configure the flags for the event to be logged:

- Configure the flags.

```
[edit system processes general-authentication-service traceoptions]  
user@host# set flag address-assignment
```



## CHAPTER 4

# Configuring Domain Maps for Subscriber Access

- Domain Mapping Overview on page 80
- Configuring Domain Maps on page 81
- Specifying an Access Profile in a Domain Map on page 82
- Specifying a Dynamic Profile in a Domain Map on page 83
- Specifying an Address Pool in a Domain Map on page 83
- Specifying an AAA Logical System/Routing Instance in a Domain Map on page 84
- Specifying a Target Logical System/Routing Instance in a Domain Map on page 85
- Configuring Domain Name Usage for Domain Maps on page 86
- Specifying Domain Name Delimiters on page 87
- Specifying the Parsing Direction for Domain Names on page 87
- Enabling Domain Name Stripping on page 88
- Specifying a Tunnel Profile in a Domain Map on page 88
- Configuring PADN Parameters for a Domain Map on page 89
- Verifying and Managing Domain Map Configuration on page 89

## Domain Mapping Overview

Domain mapping enables you to configure a map that specifies access options and session-specific parameters. The map is based on the domain name of subscriber sessions — the router applies the mapped options and parameters to sessions for subscribers that have the specified domains. For example, you might configure a domain map that is based on the domain name **xyz.com**. The options and parameters in that domain map are then applied when subscribers with the specified domain name (for example, **bob@xyz.com**, **raj@xyz.com**, and **juan@xyz.com**) request an AAA service.

Domain maps provide efficiency, and enable you to make changes for a large number of subscribers in one operation. For example, if an address assignment pool becomes exhausted due to the number of subscribers obtaining addresses from the pool, you can create a domain map that specifies that subscribers in a particular domain obtain addresses from a different pool. In another use of domain maps, you might create a new dynamic profile and then configure a domain map to specify which subscribers (by their domain) use that dynamic profile.

Table 14 on page 80 describes the access options and parameters you can configure in domain maps.

**Table 14: Domain Map Options and Parameters**

Option	Description
AAA logical system/routing instance	Logical system/routing instance in which AAA sends authentication and accounting requests for the subscriber sessions..
Access profile	Access profile applied to subscriber sessions.
Address pool	Address pool used to allocate addresses to subscribers.
Domain name rules	Rules for domain name usage, including domain name stripping, supported delimiters, and parse direction (delimiters and the parse direction are configured globally).
Dynamic profile	Dynamic profile applied to subscriber sessions.
PADN parameters	PPPoE route information for subscriber sessions.
Target logical system/routing instance	Logical system/routing instance to which the subscriber interface is attached.
Tunnel profile	Tunnel profile applied to subscriber sessions.

### Default Domain Map

You can configure a default domain map that the router uses for subscribers whose domain name does not explicitly match any existing domain maps. The router also uses the default domain map when a subscriber username does not include a domain name.

You might configure the default domain map to provide limited feature support for guest subscribers, such as a specific address pool used for guests or the logical system that provides AAA services. When the router is unable to match a subscriber request to a domain map, the router then uses the rules specified in the default domain map configuration to handle the subscriber request.

**Related Documentation**

- Configuring Domain Maps on page 81

## Configuring Domain Maps

To configure domain maps:

1. Create the domain map. For the map name, specify the domain name that you want the domain map to use. (Use **default** for the name of the default domain map.)

```
[edit access]
user@host# edit domain map domain-map-name
```

- For example, to create a domain map to be mapped to subscribers with the domain name **xyz.com**:

```
[edit access]
user@host# edit domain map xyz.com
```

- To create a default domain map to be mapped to subscribers with non-matching domain names and subscribers without domain names:

```
[edit access]
user@host# edit domain map default
```

2. (Optional) Specify the access profile used to apply access rules for the domain map.  
See “Specifying an Access Profile in a Domain Map” on page 82.
3. (Optional) Configure the dynamic profile that provides dynamic access rules for the domain map.  
See “Specifying a Dynamic Profile in a Domain Map” on page 83.
4. (Optional) Specify the address pool used to allocate address for the domain map.  
See “Specifying an Address Pool in a Domain Map” on page 83.
5. (Optional) Configure a non-default logical system/routing instance in which AAA requests are sent for the domain map.  
See “Specifying an AAA Logical System/Routing Instance in a Domain Map” on page 84.
6. (Optional) Configure a non-default target logical system/routing instance for the subscriber context.  
See “Specifying a Target Logical System/Routing Instance in a Domain Map” on page 85.
7. (Optional) Configure rules for domain names; for example; delimiters, parsing direction, and domain stripping. Delimiters and parsing direction are configured globally for all domain maps. Domain stripping is enabled in the domain map.

See “Configuring Domain Name Usage for Domain Maps” on page 86.

8. (Optional) Configure the tunnel profile that provides tunnel definitions for the domain map..

See “Specifying a Tunnel Profile in a Domain Map” on page 88.

9. (Optional) Configure the PADN parameters used for PPPoE route information for the domain map.

See “Configuring PADN Parameters for a Domain Map” on page 89.

- Related Documentation**
- Domain Mapping Overview on page 80
  - Verifying and Managing Domain Map Configuration on page 89

## Specifying an Access Profile in a Domain Map

You use access profiles to specify the access rules and options (for example, the RADIUS authentication server and attributes) that the router applies to subscriber sessions. The domain map feature enables you to apply a specific access profile for subscribers in a particular domain.

Access profiles can be specified or modified in several different ways. If conflicts occur, the router applies the access profiles based on the precedence rules shown in Table 15 on page 82.

**Table 15: Precedence Rules for Applying Access Profiles**

Precedence (High to Low)	How the Access Profile Is Applied
1	Specified by the RADIUS Redirect-VRouter-Name attribute (VSA 26-25)
2	Specified in the domain map configuration stanza
3	Indirectly specified in the domain map configuration stanza by the AAA logical system/routing instance mapping
4	Specified in the client configuration stanza
5	Specified in the logical system/routing instance configuration stanza

To include an access profile in a domain map:

1. Specify the domain map you want to configure.

```
[edit access]
user@host# edit domain map domain-map-name
```

2. Specify the access profile you want to include in the domain map.

```
[edit access domain map domain-map-name]
user@host# set access-profile profile-name
```



- Related Documentation**
- Domain Mapping Overview on page 80
  - Configuring Domain Maps on page 81

## Specifying a Dynamic Profile in a Domain Map

A dynamic profile defines the set of characteristics that provide dynamic access and services for subscriber sessions (such as class-of-service, protocols, and interface support). The domain map feature enables you to apply a specific dynamic profile based on subscriber domains.

Dynamic profiles are configured at the **[edit dynamic-profiles]** hierarchy, and can be specified or modified in several different ways. If conflicts occur, the router applies the dynamic profiles based on the precedence rules shown in Table 16 on page 83.

**Table 16: Precedence Rules for Applying Dynamic Profiles**

Precedence (High to Low)	How the Dynamic Profile Is Applied
1	Specified by the RADIUS Virtual-Router attribute (VSA 26-1) or the Redirect-VRouter-Name attribute (VSA 26-25)
2	Specified in the domain map configuration stanza
3	Specified in the client configuration stanza

To include a dynamic profile in a domain map:

1. Specify the domain map you want to configure.

```
[edit access]
user@host# edit domain map domain-map-name
```

2. Specify the dynamic profile you want to include in the domain map.

```
[edit access domain map domain-map-name]
user@host# set dynamic-profile profile-name
```

- Related Documentation**
- Domain Mapping Overview on page 80
  - Configuring Domain Maps on page 81

## Specifying an Address Pool in a Domain Map

You can use the domain map feature to specify the address pool that the router uses to allocate address for subscriber sessions. The address pool can include both IPv4 and IPv6 address ranges.

Address pools can be specified or modified in several different ways. If conflicts occur, the router applies the address pool based on the precedence rules shown in Table 17 on page 84.

Table 17: Precedence Rules for Determining the Address Pool to Use

Precedence (High to Low)	How the Address Pool Reference Is Provided
1	Specified by the RADIUS Framed-Pool attribute (RADIUS attribute 88)
2	Configured in the domain map configuration stanza
3	Specified in the client configuration stanza (by address match rules)

To specify the address pool used for a domain map:

1. Specify the domain map you want to configure.

```
[edit access]
user@host# edit domain map domain-map-name
```

2. Specify the address pool you want to use for the domain map.

```
[edit access domain map domain-map-name]
user@host# set address-pool pool-name
```

#### Related Documentation

- Domain Mapping Overview on page 80
- Configuring Domain Maps on page 81

## Specifying an AAA Logical System/Routing Instance in a Domain Map

By default a domain map uses the subscriber logical system/routing instance as the context in which the **authd** daemon sends AAA authentication and accounting requests. You can optionally configure the domain map to direct AAA requests to a particular context based on the subscriber domain name. Specifying a non-default AAA context enables you to manage workflow and traffic load, and to efficiently make changes for a large number of subscribers. For example, after upgrading your RADIUS services, you might configure a domain map to specify that all subscribers in the domain **xyz.com** are now authenticated by a RADIUS server in a particular non-default AAA context.



**NOTE:** When you specify a non-default AAA context, that context also becomes the subscriber's context unless the domain map or the authentication server explicitly specifies the subscriber context. You use the **target-logical-system** command to explicitly configure the target logical system/routing instance for subscribers.

To configure a non-default logical system in which you want the **authd** daemon to send AAA requests:

1. Specify the domain map you want to configure.

```
[edit access]
```

```
user@host# edit domain map domain-map-name
```

2. Specify the logical system and optionally the non-default routing instance for AAA requests.

- To configure a non-default logical system and default routing instance for AAA requests:

```
[edit access domain map domain-map-name]
user@host# set aaa-logical-system logical-system-name
```

- To configure a non-default logical system and a non-default routing instance for AAA requests:

```
[edit access domain map domain-map-name]
user@host# set aaa-logical-system logical-system-name aaa-routing-instance
routing-instance-name
```

To configure the default logical system and a non-default routing instance for AAA requests:

1. Specify the domain map you want to configure.

```
[edit access]
user@host# edit domain map domain-map-name
```

2. Specify the non-default routing instance. The AAA logical system is automatically set to the default.

```
[edit access domain map domain-map-name]
user@host# set aaa-routing-instance routing-instance-name
```

#### Related Documentation

- Domain Mapping Overview on page 80
- Configuring Domain Maps on page 81
- Specifying a Target Logical System/Routing Instance in a Domain Map on page 85

## Specifying a Target Logical System/Routing Instance in a Domain Map

By default, the router places a subscriber in the logical system/routing instance of the interface on which the subscriber negotiations start. Subscriber management can then use the authentication server or a domain map to change the subscriber's logical system/routing instance.

To use the domain map method, you configure the domain map to specify the target logical system and routing instance for the subscriber's interface. You can optionally configure the domain map to use the default logical system and a specific non-default routing instance.

To configure a non-default target logical system for a subscriber's interface:

1. Specify the domain map you want to configure.

```
[edit access]
user@host# edit domain map domain-map-name
```

2. Specify the target logical system and, optionally, the non-default target routing instance for the subscriber's interface.

- To configure a non-default target logical system and default target routing instance:

```
[edit access domain map domain-map-name]  
user@host# set target-logical-system logical-system-name
```

- To configure a non-default target logical system and a non-default target routing instance:

```
[edit access domain map domain-map-name]  
user@host# set target-logical-system logical-system-name target-routing-instance  
routing-instance-name
```

To configure a default target logical system and a non-default routing instance for a subscriber's interface:

1. Specify the domain map you want to configure.

```
[edit access]  
user@host# edit domain map domain-map-name
```

2. Specify the non-default target routing instance. The target logical system is automatically set to the default.

```
[edit access domain map domain-map-name]  
user@host# set target-routing-instance routing-instance-name
```

**Related  
Documentation**

- Domain Mapping Overview on page 80
- Configuring Domain Maps on page 81

---

## Configuring Domain Name Usage for Domain Maps

You can configure how the router determines domain names for the domain mapping feature. At the global level, you can specify rules that are used for all domain maps. The global rules enable you to specify additional characters that the router can recognize as domain name delimiters and to specify the direction the router uses to parse domain names. At the domain map level, you can enable domain name stripping. Domain name stripping specifies that the router remove the domain name from the subscriber username prior to performing any additional processing for the domain map.

To configure domain name usage rules for domain maps:

1. (Optional) Configure the domain name delimiters you want the router to recognize for all domain maps.

See "Specifying Domain Name Delimiters" on page 87.

2. (Optional) Configure the parse direction you want the router to use when determining domain names for all domain maps.

See "Specifying the Parsing Direction for Domain Names" on page 87.

3. (Optional) Configure the router to remove the domain name from usernames in the domain map before using AAA services.

See “Enabling Domain Name Stripping” on page 88.

- Related Documentation**
- Domain Mapping Overview on page 80
  - Configuring Domain Maps on page 81

## Specifying Domain Name Delimiters

A delimiter is the character that separates a subscriber username from the domain name. Delimiters are commonly used for domain name parsing or stripping. You can specify a maximum of eight delimiters that the router uses to recognize domain names for all domain maps. If you do not configure any delimiters, the router uses the @ character by default.

For example, your network might include the subscribers **bob@abc.com**, **pete!xyz.com**, and **maria\pqr.com**. In this case, you configure the router to recognize the characters @, !, and \ as delimiters.

Keep the following guidelines in mind when specifying delimiters:

- You cannot use the semicolon (;) as a delimiter.
- If you configure optional delimiters, you must also specify the @ character (the default delimiter) if you want to continue to use it as a delimiter.
- If you configure optional delimiters and then unconfigure them, the router sets the domain map delimiter back to the default @ character.

To configure domain name delimiters for all domain maps:

1. Specify that you want to configure domain attributes.

```
[edit]
user@host# edit access domain
```

2. Specify the characters you want to use as delimiters. Do not include spaces between the delimiters.

```
[edit access domain]
user@host# set delimiter [delimiter-character]
```

- Related Documentation**
- Configuring Domain Name Usage for Domain Maps on page 86

## Specifying the Parsing Direction for Domain Names

You can specify the direction in which the router performs the parsing operation it uses to identify subscriber domain names for all domain maps. During the parsing operation, the router searches the username until it recognizes a delimiter. It then considers anything

to the right of the delimiter as the domain. By default, the router parses from right to left, starting at the right-most character in the username.

The parsing direction you use is important when there are nested domain names. For example, for the username `user1@abc.com@xyz.com`, right-to-left parsing produces a domain name of `xyz.com`. For the same username, left-to-right parsing produces a domain name of `abc.com@xyz.com`.

To configure the domain name parsing direction for all domain maps:

1. Specify that you want to configure domain attributes.

```
[edit]
user@host# edit access domain
```

2. Specify the parsing direction you want the router to use.

```
[edit access domain]
user@host# set parse-direction (left-to-right | right-to-left)
```

**Related  
Documentation**

- Configuring Domain Name Usage for Domain Maps on page 86

---

## Enabling Domain Name Stripping

You can configure the router to strip the domain name from usernames before any AAA services are used. Domain name stripping is done for domain maps. The router uses the delimiters and parsing direction you globally configure to determine the domain name that is removed. For example, if the router uses the default delimiter and parsing direction **right-to-left**, the username `user1@xyz.com` is stripped to be `user1`.

To configure the router to strip the domain name from usernames in a domain map:

1. Specify the domain map for the stripping operation.

```
[edit]
user@host# edit access domain map domain-map-name
```

2. Enable domain name stripping.

```
[edit access domain map domain-map-name]
user@host# set strip-domain
```

**Related  
Documentation**

- Configuring Domain Name Usage for Domain Maps on page 86

---

## Specifying a Tunnel Profile in a Domain Map

Tunnel profiles specify tunnel definitions (for example, a set of L2TP tunnels and their attributes) that the router applies to subscriber sessions. The domain map feature enables you to apply a specific tunnel profile to subscribers in a particular domain.



**NOTE:** A tunnel profile specified by a RADIUS server in the Tunnel-Group attribute (VSA 26-64) takes precedence over the tunnel profile specified in the domain map.

To include an tunnel profile in a domain map:

1. Specify the domain map you want to configure.

```
[edit access]
user@host# edit domain map domain-map-name
```

2. Specify the tunnel profile you want to include in the domain map.

```
[edit access domain map domain-map-name]
user@host# set tunnel-profile profile-name
```

**Related  
Documentation**

- Domain Mapping Overview on page 80
- Configuring Domain Maps on page 81

## Configuring PADN Parameters for a Domain Map

You can configure PPPoE to receive PPPoE Active Discovery Network (PADN) messages when a subscriber connects to a PPPoE server. The PADN information associates the PPPoE session with a set of routes that the session can use. You can configure the route information in domain maps, which enables you to apply specific PADN information to subscribers in a particular domain. You can configure a maximum of 16 routes in a domain map.

To configure PADN parameters in a domain map:

1. Specify the domain map you want to configure.

```
[edit access]
user@host# edit domain map domain-map-name
```

2. Specify the PADN route information you want to include in the domain map. For each route, include the destination IP address, subnet mask, and route metric.

```
[edit access domain map domain-map-name]
user@host# set padn destination-address mask destination-mask metric route-metric
```

**Related  
Documentation**

- Domain Mapping Overview on page 80
- Configuring Domain Maps on page 81

## Verifying and Managing Domain Map Configuration

**Purpose** Display information related to domain maps.

**Action** • To display statistics for domain maps:

`user@host> show network-access domain-map`

- To display domain map information for a specific subscriber session:

`user@host> show network-access aaa subscribers session-id`

**Related  
Documentation**

- Domain Mapping Overview on page 80
- Configuring Domain Maps on page 81



## CHAPTER 5

# AAA and Remote Subscriber Access Configuration Examples

- Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 91
- Example: Configuring an Address-Assignment Pool on page 93

### Example: Configuring RADIUS-Based Subscriber Authentication and Accounting

---

This example shows a RADIUS-based authentication and accounting configuration.

```
[edit access]
radius-server {
  192.168.1.250 {
    port 1812;
    accounting-port 1813;
    retry 3;
    secret &tIUeI*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;
      client-accounting-algorithm round-robin;
      client-authentication-algorithm round-robin;
      nas-identifier 56;
    }
    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-cmborg-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;
      }
    }
  }
}
```

**Related  
Documentation**

- [Configuring Router or Switch Interaction with RADIUS Servers on page 20](#)

## Example: Configuring an Address-Assignment Pool

This example shows an address-assignment pool configuration that creates two pools, one for IPv4 DHCP clients (**isp\_1**), and a second pool (**chi-fiber-ra**) that is used for router advertisement.

```
[edit access]
address-assignment {
  network-discovery-router-advertisement chi-fiber-ra;
  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;
    }
  }
}
pool chi-fiber-ra {
  family inet6 {
    prefix 2008:2009:2010::/48;
    range fiber3 {
      low 2008:2009:2010::1/64;
      high 2008:2009:2010::5/64;
    }
  }
}
```

This example creates an IPv4 address-assignment pool named **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**. The ISP\_1 pool configuration

also includes the **dhcp-attributes** statement, indicating that the pool is used for DHCP clients. 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.

The second address-assignment pool created in this example is **chi-fiber-ra**. The **neighbor-discovery-router-advertisement** statement at the beginning of the syntax specifies that this named address-assignment pool is used for router advertisement. The syntax at the end of the example configures the address-assignment pool named **chi-fiber-ra**.

**Related  
Documentation**

- Address-Assignment Pools Overview on page 67
- Configuring Address-Assignment Pools on page 68
- Configuring an Address-Assignment Pool for Router Advertisement

## PART 3

# DHCP Local Server for Subscriber Access

- DHCP Local Server Overview on page 97
- Configuring DHCP Local Server on page 107
- DHCP Local Server Examples on page 147



## CHAPTER 6

# DHCP Local Server Overview

- [Extended DHCP Local Server Overview on page 98](#)
- [DHCPv6 Local Server Overview on page 102](#)
- [Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview on page 104](#)

## 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.

You can also configure the extended DHCP local server to support IPv6 clients. Both DHCP local server and DHCPv6 local server support the specific address request feature, which enables you to assign a particular address to a client. See “DHCPv6 Local Server Overview” on page 102 for information about the DHCPv6 local server feature.

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 68 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 828 for the complete DHCP local server syntax.

This overview covers:

- Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools on page 99



- Providing DHCP Client Configuration Information on page 99
- Minimal Configuration for Clients on page 100
- DHCP Local Server and Address-Assignment Pools on page 100

## 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 selected to 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. Table 18 on page 100 lists 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 39 for a complete list of RADIUS attributes and Juniper Networks VSAs that the extended DHCP applications supports for subscriber access management.

**Table 18: Information in Authentication Grant**

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 27	Session-Timeout	Lease time
RADIUS attribute 88	Framed-Pool	Address assignment pool name
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 Documentation

- [Configuring Address-Assignment Pools on page 68](#)
- [Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 111](#)
- [Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview on page 104](#)
- [Using External AAA Authentication Services with DHCP on page 110](#)
- [Use of DHCP Option 50 and DHCPv6 IA\\_NA Option to Request a Specific IP Address on page 123](#)
- [Graceful Routing Engine Switchover on page 139](#)
- [Subscriber Management Unified ISSU Support on page 6](#)
- [Tracing Extended DHCP Operations on page 139](#)
- [Verifying and Managing DHCP Local Server Configuration on page 138](#)
- [Example: Minimum Extended DHCP Local Server Configuration on page 147](#)
- [Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 147](#)

## DHCPv6 Local Server Overview

The DHCPv6 local server enhances the extended DHCP local server by providing support for IPv6. When a DHCPv6 client logs in, the DHCPv6 local server uses the AAA service framework to interact with the RADIUS server. The RADIUS server, which is configured independently of DHCP, authenticates the client and supplies the IPv6 prefix and client configuration parameters.

You can configure DHCPv6 local server to communicate the following attributes to the AAA service framework and RADIUS at login time:

- Client username
- Client password



**NOTE:** The client username, which uniquely identifies a subscriber, must be present in the configuration in order for DHCPv6 local server to use RADIUS authentication.

Based on the attributes that the DHCPv6 local server provides, RADIUS returns the information listed in Table 19 on page 102 to configure the client:

**Table 19: RADIUS Attributes and VSAs for DHCPv6 Local Server**

Attribute Number	Attribute Name	Description
27	Session-Timeout	Lease time, in seconds. If not supplied, the lease does not expire
123	Delegated-IPv6-Prefix	Prefix that is delegated to the client
26-143	Max-Clients-Per-Interface	Maximum number of clients allowed per interface

The DHCPv6 local server is compatible with the extended DHCP local server and the extended DHCP relay agent, and can be enabled on the same interface as either the extended DHCP local server or DHCP relay agent.

The DHCPv6 local server provides many of the same features as the extended DHCP local server, including:

- Configuration for a specific interface or for a group of interfaces
- Site-specific usernames and passwords
- Numbered Ethernet interfaces
- Statically configured CoS and filters

- AAA directed login
- Use of the IA\_NA option to assign a specific address to a client



**NOTE:** DHCPv6 local server does not support dynamic profiles or the local address-assignment pool feature, which the DHCP local server does support.

To configure the extended DHCPv6 local server on the router, you include the **dhcpx6** statement at the **[edit system services dhcp-local-server]** hierarchy level. See the “[edit system services dhcp-local-server] Hierarchy Level” on page 828 for the complete DHCP local server syntax, including the DHCPv6 syntax.

You can also include the **dhcpx6** statement at the following hierarchy levels:

- **[edit logical-systems *logical-system-name* system services dhcp-local-server]**
- **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server]**
- **[edit routing-instances *routing-instance-name* system services dhcp-local-server]**

#### Related Documentation

- Extended DHCP Local Server Overview on page 98
- Using External AAA Authentication Services with DHCP on page 110
- Grouping Interfaces with Common DHCP Configurations on page 112
- Group-Specific DHCP Local Server Options on page 115
- Overriding Default DHCP Local Server Configuration Settings on page 115
- Configuring Passwords for Usernames on page 127
- Creating Unique Usernames for DHCP Clients on page 128
- Use of DHCP Option 50 and DHCPv6 IA\_NA Option to Request a Specific IP Address on page 123
- Verifying and Managing DHCPv6 Local Server Configuration on page 138
- Example: Extended DHCPv6 Local Server Configuration on page 148

## 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** statement 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. The **aggregate-clients** statement provides the option of either merging (chaining) or replacing software components for each client.

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.

When you specify the **merge** option, the router aggregates 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.

When you specify the **replace** option, the entire logical interface is replaced whenever a new client logs in to the network using the same VLAN logical interface. For example, if a customer subscribes to voice, video, and data services on the network, when a voice client logs in, instead of applying a specific voice filter for only that service, the entire voice, video, and data filter chain is applied.



**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 IP demux interfaces are used to represent subscribers. To conserve interfaces, make sure the primary profile that you specify does not create a demux interface, but provides the initial policies for the primary interface subscriber.

### Related Documentation

- [Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125](#)





## CHAPTER 7

# Configuring DHCP Local Server

- DHCP Duplicate Client Differentiation Using Client Subinterface Overview on page 108
- Guidelines for Configuring Support for DHCP Duplicate Clients on page 109
- Configuring DHCP Duplicate Client Support on page 109
- Using External AAA Authentication Services with DHCP on page 110
- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 111
- Grouping Interfaces with Common DHCP Configurations on page 112
- Guidelines for Configuring Interface Ranges on page 113
- Group-Specific DHCP Local Server Options on page 115
- Overriding Default DHCP Local Server Configuration Settings on page 115
- Specifying the Maximum Number of DHCP Clients Per Interface on page 116
- Disabling ARP Table Population on page 117
- Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server on page 119
- DHCP Auto Logout Overview on page 120
- Automatically Logging Out DHCP Clients on page 121
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 122
- Use of DHCP Option 50 and DHCPv6 IA\_NA Option to Request a Specific IP Address on page 123
- Subscriber Binding Retention During Interface Delete Events on page 123
- Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 124
- Verifying and Managing the DHCP Maintain Subscribers Feature on page 125
- Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125
- Configuring Passwords for Usernames on page 127
- Creating Unique Usernames for DHCP Clients on page 128
- Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients on page 130
- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 133

- [Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 134](#)
- [Configuring Deletion of the Client When Dynamic Reconfiguration Fails on page 135](#)
- [Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 136](#)
- [Configuring a Token for DHCP Local Server Authentication on page 136](#)
- [Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings on page 137](#)
- [Verifying and Managing DHCP Local Server Configuration on page 138](#)
- [Verifying and Managing DHCPv6 Local Server Configuration on page 138](#)
- [Graceful Routing Engine Switchover on page 139](#)
- [Tracing Extended DHCP Operations on page 139](#)

---

## DHCP Duplicate Client Differentiation Using Client Subinterface Overview

---

In some network environments, client IDs and MAC addresses might not be unique, resulting in duplicate clients. For example, two network adapters might be manufactured with the same hardware address, resulting in a duplicate MAC address among the DHCP clients attached to the router. A duplicate DHCP client occurs when a client attempts to get a lease, and that client has the same client ID or the same MAC address as an existing DHCP client.

When DHCP server receives a request from a new client that has a duplicate ID or MAC address, DHCP server terminates the address lease for the existing client and returns the address to its original address pool. DHCP server then assigns a new address and lease to the new client.

By default, both DHCP local server and DHCP relay use the subnet information to differentiate between duplicate clients. However, in some cases, this level of differentiation is not adequate. For example, when multiple subinterfaces share the same underlying loopback interface with the same preferred source address, the interfaces appear to be on the same subnet. In this situation, the default configuration prevents duplicate clients.

You can provide greater differentiation between duplicate clients by configuring DHCP to consider the client subinterface when duplicate clients occur. In this optional configuration, DHCP uniquely identifies:

- The subnet on which the client resides
- The subinterface on which the client resides
- The client within the subnet

### Related Documentation

- [Configuring DHCP Duplicate Client Support on page 109](#)
- [Guidelines for Configuring Support for DHCP Duplicate Clients on page 109](#)

## Guidelines for Configuring Support for DHCP Duplicate Clients

---

This topic describes the guidelines for configuring DHCP to include the client subinterface in order to distinguish between duplicate clients (clients with the same MAC address or client ID) in a subscriber access environment.

When configuring DHCP duplicate client support, consider the following guidelines:

- The optional DHCP duplicate client support feature is used for DHCPv4 clients. For DHCPv6, client identification is independent of MAC address.
- For DHCP relay agent configuration:
  - DHCP relay must be configured to insert option 82, regardless of whether or not the incoming packet has option 82.
  - Option 82 must include the Agent Circuit ID suboption (suboption 1).
  - Option 82 must be the interface name, not the interface description.
  - DHCP server must echo option 82 in the server's reply. This is required because of the following:
    - The giaddr inserted by DHCP relay is the same for duplicate clients on different subinterfaces. The DHCP local server uses option 82 when allocating the IP address.
    - DHCP relay uses the echoed option 82 to learn the client subinterface and to construct the client key.
- For the Layer 3 wholesale model:
  - The wholesaler and retailer logical system/routing instances must have the same **duplicate-clients-on-interface** statement configuration.
  - For DHCP relay, the wholesaler and the retailer routing contexts must both be configured with the Agent Circuit ID suboption (suboption 1) in option 82.

### Related Documentation

- DHCP Duplicate Client Differentiation Using Client Subinterface Overview on page 108
- Configuring DHCP Duplicate Client Support on page 109

## Configuring DHCP Duplicate Client Support

---

You can optionally configure DHCP local server and DHCP relay to include a client subinterface when distinguishing between two clients that have the same MAC address or client ID. The configuration is a global setting for each logical system/routing instance.

To configure DHCP local server to include the client subinterface:

1. Specify that you want to configure DHCP local server.

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

2. Configure the optional duplicate client support.

```
[edit system services dhcp-local-server]
user@host# set duplicate-clients-on-interface
```

To configure DHCP relay agent to include the client subinterface:

1. Specify that you want to configure DHCP relay agent.

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

2. Configure the optional duplicate client support.

```
[edit system services dhcp-relay]
user@host# set duplicate-clients-on-interface
```

**Related  
Documentation**

- DHCP Duplicate Client Differentiation Using Client Subinterface Overview on page 108
- Guidelines for Configuring Support for DHCP Duplicate Clients on page 109

---

## Using External AAA Authentication Services with DHCP

---

The extended DHCP local server, including DHCPv6 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 responds as though it were 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
```

- For DHCPv6 local server:

```
[edit system services dhcp-local-server dhcpv6]
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 127.

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

See “Creating Unique Usernames for DHCP Clients” on page 128.

#### Related Documentation

- Extended DHCP Local Server Overview on page 98
- Extended DHCP Relay Agent Overview on page 154
- DHCPv6 Local Server Overview on page 102

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

You can specify the match order in which the extended DHCP local server uses the client data to determine the address-assignment pool that provides the IP address and configuration for a DHCP client. You use the **pool-match-order** statement to specify the match order. If you do not specify the **pool-match-order**, the router uses the default **ip-address-first** matching to select the address pool. After DHCP local server determines the address assignment pool to use, the server performs the matching based on the criteria you specified in the pool configuration.

In the default **ip-address-first** matching, 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.

In **external-authority** matching, the DHCP local server receives the address assignment from an external authority, such as RADIUS or Diameter. If RADIUS is the external authority, the DHCP local server uses the Framed-IPv6-Pool attribute (RADIUS attribute 100) to select the pool. If Diameter is the external authority, the server uses the Diameter counterpart of the Framed-IPv6-Pool attribute to determine the pool.

For IPv4 address-assignment pools, 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, which you can configure when you create the address-assignment pool.



**NOTE:** To use the DHCP local server option 82 matching feature with an IPv4 address-assignment pool, you must ensure that the **option-82** statement is included in the **dhcp-attributes** statement for the address-assignment pool.

To configure the matching order the extended DHCP local server uses to determine the address-assignment pool used for a client:

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

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

2. Specify the pool matching methods in the order in which the router performs the methods. You can specify the methods in any order. All methods are optional—the router uses the **ip-address-first** method by default.

- Configure the router to use an external addressing authority.

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

- Configure the router to use the ip-address-first method.

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

- (IPv4 address-assignment pools only) Specify the option 82 matching method.

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

#### Related Documentation

- Address-Assignment Pools Overview on page 67
- Configuring Address-Assignment Pools on page 68
- Extended DHCP Local Server Overview on page 98
- Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 147

---

## 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, including the DHCPv6 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 the DHCPv6 local server and 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# set interface fe-1/0/1.1 upto fe-1/0/1.102
user@host# set interface fe-1/0/1.6 exclude
user@host# set interface fe-1/0/1.70 upto fe-1/0/1.80 exclude
```

#### Related Documentation

- Extended DHCP Local Server Overview on page 98
- Extended DHCP Relay Agent Overview on page 154
- DHCPv6 Local Server Overview on page 102
- Group-Specific DHCP Local Server Options on page 115
- Group-Specific DHCP Relay Options on page 167
- Guidelines for Configuring Interface Ranges on page 113

## Guidelines for Configuring Interface Ranges

This topic describes guidelines to consider when configuring interface ranges for named interface groups for DHCP local server and DHCP relay. The guidelines refer to the following configuration statement:

```
user@host# set interface interface-name upto upto-interface-name
```

- The start subunit, **interface *interface-name***, serves as the key for the stanza. The remaining configuration settings are considered attributes.
- If the subunit is not included, an implicit **.0** subunit is enforced. The implicit subunit is applied to all interfaces when autoconfiguration is enabled. For example, **interface ge-2/2/2** is treated as **interface ge-2/2/2.0**.
- Ranged entries contain the **upto** option, and the configuration applies to all interfaces within the specified range. The start of a ranged entry must be less than the end of the range. Discrete entries apply to a single interface, except in the case of autoconfiguration, in which a **0** (zero) subunit acts as a wildcard.
- Interface stanzas defined within the same router context are dependent and can constrain each other—both DHCP local server and DHCP relay are considered. Interface stanzas defined across different router contexts are independent and do not constrain one another.
- Each interface stanza, whether discrete or ranged, has a unique start subunit across a given router context. For example, the following configuration is not allowed within the same group because **ge-1/0/0.10** is the start subunit for both.

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.10
```

- Two groups cannot share interface space. For example, the following configuration is not allowed because the three stanzas share the same space and interfere with one another—interface **ge-1/0/0.26** is common to all three.

```
dhcp-relay group diamond interface ge-1/0/0.10 upto ge-1/0/0.30
dhcp-local-server group ruby interface ge-1/0/0.26
dhcp-relay group sapphire interface ge-1/0/0.25 upto ge-1/0/0.35
```

- Two ranges cannot overlap, either within a group or across groups. Overlapping occurs when two interface ranges share common subunit space but neither range is a proper subset of the other. The following ranges overlap:

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.20 upto ge-1/0/0.40
```

- A range can contain multiple nested ranges. A nested range is a proper subset of another range. When ranges are nested, the smallest matching range applies.

In the following example, the three ranges nest properly:

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.12 upto ge-1/0/0.15 exclude
interface ge-1/0/0.25 upto ge-1/0/0.29 exclude
```

- Discrete interfaces take precedence over ranges. In the following example, interface **ge-1/0/0.20** takes precedence and enforces an interface client limit of 5.

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.15 upto ge-1/0/0.25 exclude
interface ge-1/0/0.20 overrides interface-client-limit 5
```

#### Related Documentation

- Grouping Interfaces with Common DHCP Configurations on page 112



## 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 115.

The DHCPv6 local server supports the same set of statements with the exception of the **dynamic-profile** statement.

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 Documentation

- Grouping Interfaces with Common DHCP Configurations on page 112

## Overriding Default DHCP Local Server Configuration Settings

Subscriber management enables you to override certain default DHCP and DHCPv6 local server configuration settings. You can override settings at the global level, for a named group of interfaces, or for a specific interface within a named group.

- 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]** or **[edit system services dhcp-local-server dhcpv6]** 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]** or **[edit system services dhcp-local-server dhcpv6 group]** hierarchy level.
- To override DHCP local server configuration options for a specific interface within a named group of interfaces, include the statements at the **[edit system services dhcp-local-server group group-name interface]** or **[edit system services dhcp-local-server dhcpv6 group group-name interface]** hierarchy level.

To override default DHCP local server configuration settings:

1. Specify that you want to configure override options.

Global override:

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

Group level override:

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

Per-interface override:

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

2. (Optional) Override the maximum number of DHCP clients allowed per interface.  
See “Specifying the Maximum Number of DHCP Clients Per Interface” on page 116.
3. (Optional) Override ARP table population in distrusted environments.  
See “Disabling ARP Table Population” on page 117.
4. (Optional) Configure DHCP client auto logout.  
See “Automatically Logging Out DHCP Clients” on page 121.
5. (Optional) Delete DHCP override settings.  
See “Deleting DHCP Local Server and DHCP Relay Override Settings” on page 122.

**Related  
Documentation**

- Group-Specific DHCP Local Server Options on page 115
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 122

---

## 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 through 500,000. When the number of clients on the interface reaches the specified limit, no additional DHCP Discover PDUs or DHCPv6 Solicit PDUs are accepted. When the number of clients subsequently drops below the limit, new clients are again accepted.



**NOTE:** The maximum number of DHCP (and DHCPv6) 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 DHCPv6 local server:

```
[edit system services dhcp-local-server dhcpv6]
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, DHCPv6 local server, and DHCP relay agent all support the **interface-client-limit** statement.)

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

#### Related Documentation

- Overriding Default DHCP Local Server Configuration Settings on page 115
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 122
- Extended DHCP Local Server Overview on page 98
- Extended DHCP Relay Agent Overview on page 154

## 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 20: 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 21: 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
```

#### Related Documentation

- Overriding Default DHCP Local Server Configuration Settings on page 115
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 122
- Extended DHCP Local Server Overview on page 98
- DHCPv6 Local Server Overview on page 102
- Extended DHCP Relay Agent Overview on page 154
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 122

## Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server

You can configure how DHCP local server handles DHCP snooped packets. Depending on the configuration, DHCP local server either forwards or drops the snooped packets it receives.

Table 22 on page 119 indicates the action the router takes for DHCP local server snooped packets.



**NOTE:** Configured interfaces are those interfaces that have been configured with the `group` statement in the `[edit system services dhcp-local-server]` hierarchy. Non-configured interfaces are those that are in the logical system/routing instance but have not been configured by the `group` statement.

**Table 22: Actions for DHCP Local Server Snooped Packets**

forward-snooped-clients Configuration	Action on Configured Interfaces	Action on Non-Configured Interfaces
<b>forward-snooped-clients</b> not configured	dropped	dropped
<b>all-interfaces</b>	forwarded	forwarded
<b>configured-interfaces</b>	forwarded	dropped
<b>non-configured-interfaces</b>	dropped	forwarded

To configure DHCP snooped packet forwarding for DHCP local server:

1. Specify that you want to configure DHCP local server.

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

2. Enable DHCP snooped packet forwarding for DHCP local server.

```
[edit system services dhcp-local-server]
user@host# edit forward-snooped-clients
```

3. Specify the interfaces that are supported for snooped packet forwarding.

```
[edit system services dhcp-local-server forward-snooped-clients]
user@host# set (all-interfaces | configured-interfaces | non-configured-interfaces)
```

For example, to configure DHCP local server to forward DHCP snooped packets on only configured interfaces:

```
[edit]
system {
  services {
```

```
        dhcp-local-server {  
            forward-snooped-clients configured-interfaces;  
        }  
    }  
}
```

**Related Documentation**

- DHCP Snooping Support on page 174

---

## 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 120
- How DHCP Identifies and Releases Clients on page 120
- Option 60 and Option 82 Requirements on page 121

### 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 discover 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 182.

### Related Documentation

- Automatically Logging Out DHCP Clients on page 121
- DHCP Relay Agent Option 82 Value for Auto Logout on page 182

## 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# set client-discover-match
```

- For DHCP relay:

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

- DHCP Auto Logout Overview on page 120
- DHCP Relay Agent Option 82 Value for Auto Logout on page 182
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 122
- Extended DHCP Local Server Overview on page 98
- Extended DHCP Relay Agent Overview on page 154

---

## Deleting DHCP Local Server and DHCP Relay Override Settings

You can delete override settings for DHCP local server and DHCP relay globally, for a named group, or for a specific interface within a named group. You can delete a specific override setting or all overrides.



- To delete a specific DHCP override setting at a particular hierarchy level, include the **overrides** statement with the appropriate subordinate statements. For example, to delete the DHCP local server override **no-arp** setting for a group named **marin20**:

```
[edit system services dhcp-local-server]
user@host# delete group marin20 overrides no-arp
```

- To delete all DHCP override settings at a hierarchy level, include the **overrides** statement without any subordinate statements. For example, to delete all DHCP relay overrides for interface **fxp0.0**, which is in group **marin20**:

```
[edit forwarding-options dhcp-relay]
user@host# delete group marin20 interface fxp0.0 overrides
```

#### Related Documentation

- Overriding Default DHCP Local Server Configuration Settings on page 115
- Extended DHCP Local Server Overview on page 98
- Extended DHCP Relay Agent Overview on page 154

## Use of DHCP Option 50 and DHCPv6 IA\_NA Option to Request a Specific IP Address

Subscriber management enables you to specify that DHCP local server assign a particular address to a client. For example, if a client is disconnected, you might use this capability to assign the same address that the client was using prior to being disconnected. If the requested address is available, DHCP assigns it to the client. If the address is unavailable, the DHCP local server offers another address, based on the address allocation process.

Both DHCP local server and DHCPv6 local server support the specific address request feature. DHCP local server uses DHCP option 50 in DHCP DISCOVER messages to request a particular address, while DHCPv6 local server uses the IA\_NA option (Identity Association for Non-Temporary Addresses) in DHCPv6 SOLICIT messages.



**NOTE:** The DHCPv6 IA\_NA option allows multiple addresses; subscriber management supports only a single address. If you specify more than one address, the DHCPv6 local server uses only the first address you specify. The DHCPv6 local server also ignores any preferred lifetime or valid lifetime settings in the IA\_NA option.

## Subscriber Binding Retention During Interface Delete Events

You can configure the router to maintain DHCP subscribers when an event occurs that normally results in the router deleting the subscriber. For example, by default, the router logs out DHCP subscribers when an interface delete event occurs, such as a DPC reboot or failure. However, if you configure the router to maintain subscribers, the router identifies each subscriber that was on the deleted interface, and resumes normal packet processing for the subscriber when the interface is restored.



**NOTE:** Subscribers are logged off as usual when their lease expires, even if the router is configured to maintain subscribers and the subscriber is on a deleted interface that has not yet been restored.

You configure the router to maintain subscribers on a global basis— the configuration applies to DHCP local server, DHCPv6 local server, and DHCP relay clients in all logical routers and routing instances. When you enable the maintain subscribers feature, the router applies the feature to existing subscribers as well as subscribers who later connect.

If the maintain subscribers feature is enabled on the router, you can explicitly delete a subscriber binding and log out the subscriber by either specifying a lease expiration timeout or using one of the following commands, as appropriate:

- **clear dhcp server binding**
- **clear dhcpv6 server binding**
- **clear dhcp relay binding**

**Related  
Documentation**

- [Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 124](#)
- [Verifying and Managing the DHCP Maintain Subscribers Feature on page 125](#)

## Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events

You can specify a configuration in which the router does not log out a subscriber when the subscriber's interface is deleted.

To configure the router to maintain DHCP subscribers when the subscriber interface is deleted:

1. Specify that you want to configure subscriber management.

```
[edit system services]  
user@host# edit subscriber-management
```

2. Configure the router to support the maintain-subscriber feature.

```
[edit system services subscriber-management]  
user@host# edit maintain-subscriber
```

3. Configure the router to enable the maintain-subscriber feature when an interface-delete event occurs.

```
[edit system services subscriber-management maintain-subscriber]  
user@host# set interface-delete
```

**Related  
Documentation**

- [Subscriber Binding Retention During Interface Delete Events on page 123](#)
- [Verifying and Managing the DHCP Maintain Subscribers Feature on page 125](#)

## Verifying and Managing the DHCP Maintain Subscribers Feature

<b>Purpose</b>	Display information related to the DHCP maintain-subscribers feature and explicitly log out maintained clients.
<b>Action</b>	<ul style="list-style-type: none"> <li>To display DHCP local server binding information for the DHCP maintain subscribers feature:  <pre>user@host&gt;show dhcp server binding detail</pre> </li> <li>To display DHCPv6 local server binding information for the DHCP maintain subscribers feature:  <pre>user@host&gt;show dhcpv6 server binding detail</pre> </li> <li>To display DHCP relay binding information for the DHCP maintain subscribers feature:  <pre>user@host&gt;show dhcp relay binding detail</pre> </li> <li>To explicitly log out a DHCP local server subscriber when the maintain subscriber feature is enabled:  <pre>user@host&gt;clear dhcp server binding <i>binding-type</i></pre> </li> <li>To explicitly log out a DHCPv6 local server subscriber when the maintain subscriber feature is enabled:  <pre>user@host&gt;clear dhcpv6 server binding <i>binding-type</i></pre> </li> <li>To explicitly log out a DHCP relay subscriber when the maintain subscriber feature is enabled:  <pre>user@host&gt;clear dhcp relay binding <i>binding-type</i></pre> </li> </ul>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Subscriber Binding Retention During Interface Delete Events on page 123</li> <li>Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 124</li> </ul>

## 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 126
- Attaching a Dynamic Profile to a Group of DHCP Subscriber Interfaces on page 126

## 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 **aggregate-clients** option does not apply to demux subscriber interfaces. 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 merge
```

- 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

Before you begin:

- Configure the interface group.

See “Grouping Interfaces with Common DHCP Configurations” on page 112.

To attach a dynamic profile to a group of interfaces:

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 **aggregate-clients** option does not apply to demux subscriber interfaces. 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 merge
```

- To use the primary dynamic profile:

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

#### Related Documentation

- Dynamic Profiles Overview on page 369
- Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview on page 104
- Example: Configuring Dynamic Subscriber Interfaces on IP Demux Interfaces on page 453

## 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 DHCPv6 local server:

```
[edit system services dhcp-local-server dhcpv6]
user@host# edit authentication
```

- For DHCP relay agent:

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

2. Configure the password. (DHCP local server, DHCPv6 local server, and DHCP relay agent all support the **password** statement.)

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

#### Related Documentation

- Extended DHCP Local Server Overview on page 98
- DHCPv6 Local Server Overview on page 102
- Extended DHCP Relay Agent Overview on page 154
- Using External AAA Authentication Services with DHCP on page 110

- For information about supported characters in passwords, see “Configuring Special Requirements for Plain-Text Passwords” in the *Junos OS 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.

When you use the DHCPv6 local server, you must configure authentication and the client username; otherwise client login fails.

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**.
- **client-id**—The client identifier option (option 1). (DHCPv6 local server only)
- **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 a 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**. (Not supported for DHCPv6 local server)
- **option-60**—The portion of the option 60 payload that follows the length field. (Not supported for DHCPv6 local server)
- **option-82 <circuit-id> <remote-id>**—The specified contents of the option 82 payload. (Not supported for DHCPv6 local server)
  - **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.



**NOTE:** For DHCP relay agent, the option 82 value used in creating the username is based on the option 82 value that is encoded in the outgoing (relayed) PDU.

- **relay-agent-interface-id**—The Interface-ID option (option 18). (DHCPv6 local server only)
- **relay-agent-remote-id**—The DHCPv6 Relay Agent Remote-ID option (option 37). (DHCPv6 local server only)
- **relay-agent-subscriber-id**—The DHCPv6 Relay Agent Subscriber-ID option (option 38). (DHCPv6 local server only)
- **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.

For DHCP local server and DHCP relay agent:

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

For DHCPv6 local server:

```
user-prefix[delimiter]logical-system-name[delimiter]routing-instance-name[delimiter]
circuit-type[delimiter]relay-agent-remote-id[delimiter]
relay-agent-subscriber-id[delimiter]relay-agent-interface-id[delimiter]client-id@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 DHCPv6 local server:

```
[edit system services dhcp-local-server dhcpv6]
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, DHCPv6 local server, and DHCP relay agent all 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 Documentation

- Extended DHCP Local Server Overview on page 98
- DHCPv6 Local Server Overview on page 102
- Extended DHCP Relay Agent Overview on page 154
- Using External AAA Authentication Services with DHCP on page 110

---

## Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients

Dynamic reconfiguration of clients enables the extended DHCP local server to initiate a client update without waiting for the client to initiate a request.

### Default Client/Server Interaction

Typically the DHCP client initiates all of the basic DHCP client/server interactions. The DHCP server sends information to a client only in response to a request from that client. In subscriber management scenarios, this behavior does not enable a client to be quickly updated with its network address and configuration in the event of server changes.

For example, suppose a service provider restructured its addressing scheme or changed the server IP addresses that it provided to clients. Without dynamic reconfiguration, the service provider typically clears the DHCP server binding table, but cannot inform the DHCP clients that their bindings have been cleared. Consequently, the DHCP client operates as though its IP address is still valid, but it is now unable to communicate over the access network, resulting in an outage. The DHCP local server has to wait for the client to send a message to renew its lease or rebind to the server. In response, the server sends a NAK message to the client to force it to begin the DHCP connection process again. Alternatively, the provider can wait for customers to make a service call about the network failures and then instruct them to power cycle their customer premises equipment to reinitiate the connection. Neither of these actions is timely or convenient for customers.



## Dynamic Client/Server Interaction for DHCPv4

Dynamic reconfiguration for DHCPv4 is available through a partial implementation of RFC 3203, *DHCP Reconfigure Extension* for DHCPv4. It enables the DHCPv4 local server to send a message to the client to force reconfiguration.

The server sends a `forcerenew` message to a DHCPv4 client, initiating a message exchange. In response, DHCPv4 clients that support the `forcerenew` message then send a lease renewal message to the server. The server rejects the lease renewal request and sends a NAK to the client, causing the client to reinitiate the DHCP connection. A successful reconnection results in the reconfiguration of the DHCP client. Only the exchange of `forcerenew`, `renew`, and NAK messages is supported from RFC 3202. DHCP relay and DHCP relay proxy do not participate in the client reconfiguration or react to `forcerenew` messages other than to forward them to the client.

When the local server state machine starts the reconfiguration process on a bound client, the client transitions to the reconfiguring state and the local server sends a `forcerenew` message to the client. Because the client was in the bound state before entering the reconfiguring state, all subscriber services, such as forwarding and statistics, continue to work. Client statistics are not maintained in the interval between a successful reconfiguration and the subsequent client binding. When the server responds to the client renewal request with a NAK, the client entry is removed from the binding table and final statistics are reported. New statistics are collected when the client sends a discover message to establish a new session.

## Dynamic Client/Server Interaction for DHCPv6

Dynamic reconfiguration for DHCPv6 is available through a partial implementation of RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*. It enables the DHCPv6 local server to send a message to the client to force reconfiguration.

DHCPv6 servers send reconfigure messages to DHCPv6 clients, initiating a message exchange. In response, DHCPv6 clients that support the reconfigure message transition to the renewing state and send a renew message to the server. The server returns a reply message with a lifetime of zero (0). The client transitions to the init state and sends a solicit message. The server sends an advertise message to indicate that it is available for service. The client sends a request for configuration parameters, which the server then includes in its reply. DHCP relay and DHCP relay proxy do not participate in the client reconfiguration or react to reconfigure messages other than to forward them to the client.

When a DHCPv6 server is triggered to initiate reconfiguration on a bound DHCPv6 client, the client transitions to the reconfigure state. All subscriber services, such as forwarding and statistics, continue to work. The server then sends the reconfigure message to the client. If the DHCPv6 client is already in the reconfigure state, the DHCPv6 server ignores the reconfiguration trigger. For clients in any state other than bound or reconfigure, the server clears the binding state of the client, as if the `clear dhcpv6 server binding` command had been issued.

## Dynamic Configuration Options

You can enable dynamic reconfiguration for all DHCP clients or only the DHCP clients serviced by a specified group of interfaces, and you can modify the behavior accordingly.

- To enable dynamic reconfiguration with default reconfiguration values for all DHCP clients, include the **reconfigure** statement at the **[edit system services dhcp-local-server]** hierarchy level for DHCPv4 clients, and at the **[edit system services dhcp-local-server dhcpv6]** hierarchy level for DHCPv6 clients.
- Alternatively, to enable dynamic reconfiguration for only the DHCP clients serviced by a specified group of interfaces, include the **reconfigure** statement at the **[edit system services dhcp-local-server group group-name]** hierarchy level for DHCPv4 clients, and at the **[edit system services dhcp-local-server dhcpv6 group group-name]** hierarchy level for DHCPv6 clients.

You can optionally modify the behavior of the reconfiguration process by including the appropriate statements at the **[edit system services dhcp-local-server reconfigure]** hierarchy level for all DHCPv4 clients, and at the **[edit system services dhcp-local-server dhcpv6 reconfigure]** hierarchy level for all DHCPv6 clients. To override this global configuration for only the DHCP clients serviced by a specified group of interfaces, you can include the statements with different values at the **[edit system services dhcp-local-server group group-name reconfigure]** hierarchy level for DHCPv4 clients, and at the **[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]** hierarchy level for DHCPv6 clients.

Include the **attempts** statement to specify how many times the local server sends the **forcerenew** or **reconfigure** message to initiate client reconfiguration. Include the **timeout** statement to set the interval between the first and second attempts. The interval between each subsequent attempt doubles the previous value. For example, if the first value is 2, the first retry is attempted 2 seconds after the first attempt fails. The second retry is attempted 4 seconds after the first retry fails. The third retry is attempted 8 seconds after the second retry fails, and so on.

By default, the DHCP client's original configuration is restored if all of the reconfiguration attempts fail. Include the **clear-on-abort** statement to delete the client instead.

You can configure an authentication token by including the **token** statement. The DHCP local server then includes this token inside the authentication option when it sends **forcerenew** or **reconfigure** messages. If the service provider has previously configured the DHCP client with this token, then the client can compare that token against the newly received token, and reject the message if the tokens do not match. This functionality corresponds to RFC 3118, *Authentication for DHCP Messages*, section 4.

In the event of a RADIUS-initiated disconnect (RID), the client is deleted by default. You can configure the client to be reconfigured instead of deleted by including the **radius-disconnect** statement. The client is deleted if all attempts to reconfigure the client fail.

For the DHCPv6 server only, you can include the **strict** statement. By default, the server accepts solicit messages from clients that do not support server-initiated reconfiguration.

Including this statement causes the server to discard solicit messages from nonsupporting clients; consequently the server does not bind these clients.

You can force the local server to initiate the reconfiguration process for clients by issuing the **request dhcp server reconfigure** command for DHCPv4 clients, and the **request dhcpv6 server reconfigure** command for DHCPv6 clients. Command options determine whether reconfiguration is then attempted for all clients or specified clients.

Events that take place while a reconfiguration is in process take precedence over the reconfiguration. Table 23 on page 133 lists the actions taken in response to several different events.

**Table 23: Action Taken for Events That Occur During a Reconfiguration**

Event	Action
Server receives a discover (DHCPv4) or solicit (DHCPv6) message from the client.	Server drops packet and deletes client.
Server receives a request, renew, rebind, or init-reboot message from the client.	DHCPv4—Server sends NAK message and deletes client.  DHCPv6—Server drops packet and deletes client. Server replies to renew message with lease time of zero (0).
Server receives a release or decline message from the client.	Server deletes client.
The client lease times out.	Server deletes client.
The <b>clear dhcp server binding</b> command is issued.	Server deletes client.
The <b>request dhcp server reconfigure</b> (DHCPv4) or <b>request dhcpv6 server reconfigure</b> (DHCPv6) command is issued.	Command is ignored.
GRES or DHCP restart occurs.	Reconfiguration process is halted.

**Related Documentation**

- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 133

## Configuring Extended DHCP Local Server Dynamic Client Reconfiguration

The DHCP local server can initiate reconfiguration of its clients to avoid extended outages because of server configuration changes. In addition to requesting that the DHCP local server initiate reconfiguration, you can specify the reconfiguration behavior.

To configure dynamic reconfiguration of DHCP clients:

1. Enable dynamic reconfiguration with default values for all clients.

For DHCPv4:

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

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6]
user@host# set reconfigure
```

2. (Optional) Override the global configuration for a particular group of clients.

For DHCPv4:

```
[edit system services dhcp-local-server group-name]
user@host# set reconfigure
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 group group-name]
user@host# set reconfigure
```

3. (Optional) Configure how the server attempts reconfiguration.

See “Configuring Dynamic Reconfiguration Attempts for DHCP Clients” on page 134.

4. (Optional) Configure the response to a failed reconfiguration.

See “Configuring Deletion of the Client When Dynamic Reconfiguration Fails” on page 135.

5. (Optional) Configure the behavior in response to a RADIUS-initiated disconnect.

See “Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect” on page 136.

6. (Optional) Configure a token for rudimentary server authentication.

See “Configuring a Token for DHCP Local Server Authentication” on page 136.

7. (Optional) Initiate reconfiguration of some or all client bindings.

See “Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings” on page 137.

8. (Optional) Prevent DHCPv6 clients from binding if they do not support reconfigure messages.

See Preventing Binding of Clients That Do Not Support Reconfigure Messages.

---

## Configuring Dynamic Reconfiguration Attempts for DHCP Clients

---

You can configure how many attempts the local server makes to initiate reconfiguration of the DHCP client by sending `forcerenew` messages. You can also specify how long the server waits between attempts. By default, eight attempts are made and the initial interval is two seconds.

(Optional) To configure DHCP local server reconfiguration behavior for all DHCP clients:

1. Specify the number of reconfiguration attempts.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set attempts 5
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set attempts 5
```

2. Specify the interval between reconfiguration attempts.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set timeout 8
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set timeout 8
```

To override the global configuration for a particular group of clients, include the statements at the `[edit system services dhcp-local-server group group-name reconfigure]` hierarchy level or the `[edit system services dhcpv6 dhcp-local-server group group-name reconfigure]` hierarchy level.

#### Related Documentation

- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 133
- **attempts** on page 864
- **timeout** on page 1207

## Configuring Deletion of the Client When Dynamic Reconfiguration Fails

You can configure the local server to delete the client when the maximum number of reconfiguration attempts has been made without success. By default, the client's original configuration is restored.

(Optional) To configure the DHCP local server to delete the client when reconfiguration is not successful, for all clients:

- Specify the client deletion.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set clear-on-abort
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set clear-on-abort
```

To override the global configuration for a particular group of clients, include the statement at the `[edit system services dhcp-local-server group group-name reconfigure]` hierarchy

level or the `[edit system services dhcpv6 dhcp-local-server group group-name reconfigure]` hierarchy level.

- Related Documentation**
- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 133
  - `clear-on-abort` on page 883

## Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect

---

You can configure the local server to reconfigure the client when the client receives a RADIUS-initiated disconnect. By default, the client is deleted when a RADIUS-initiated disconnect is received.

(Optional) To configure the DHCP local server to reconfigure the client instead of deleting the client when a RADIUS-initiated disconnect is received, for all clients:

- Specify the RADIUS-initiated disconnect trigger.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure trigger]
user@host# set radius-disconnect
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure trigger]
user@host# set radius-disconnect
```

To override the global configuration for a particular group of clients, include the statement at the `[edit system services dhcp-local-server group group-name reconfigure trigger]` hierarchy level or the `[edit system services dhcpv6 dhcp-local-server group group-name reconfigure trigger]` hierarchy level.

- Related Documentation**
- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 133
  - `radius-disconnect` on page 1139
  - `trigger` on page 1243

## Configuring a Token for DHCP Local Server Authentication

---

You can configure the local server to include a constant, unencoded token in the DHCP forcerenew message as part of the authentication option it sends to clients. The client compares the received token with a token already configured on the client. If the tokens do not match, the DHCP client discards the forcerenew message. Use of the token provides rudimentary protection against inadvertently instantiated DHCP servers.

(Optional) To configure the DHCP local server to include a token in the forcerenew message sent to the client, for all clients:

- Specify the token.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set token 8ysIU9E32k8r
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set token 8ysIU9E32k8r
```

To override the global configuration for a particular group of clients, include the statement at the `[edit system services dhcp-local-server group group-name reconfigure]` hierarchy level or the `[edit system services dhcpv6 dhcp-local-server group group-name reconfigure]` hierarchy level.

- Related Documentation**
- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 133
  - **token** on page 1210

## Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings

You can request that the DHCP local server initiate reconfiguration of all of clients or only specified clients.

To request reconfiguration of all clients:

- Specify the **all** option.

For DHCPv4:

```
user@host> request dhcp server reconfigure all
```

For DHCPv6:

```
user@host> request dhcpv6 server reconfigure all
```

You can use any of the following methods to request reconfiguration of specific clients:

- Specify the IP address of the DHCP client.

For DHCPv4:

```
user@host> request dhcp server reconfigure 192.168.27.3
```

For DHCPv6:

```
user@host> request dhcpv6 server reconfigure 2001:bd8:1111:2222::
```

- Specify the client ID of a DHCPv6 client.

```
user@host> request dhcpv6 server reconfigure
LL_TIME0x1-0x2e159c0-00:10:94:00:00:02
```

- Specify the session ID of a DHCPv6 client.

```
user@host> request dhcpv6 server reconfigure 5
```

- Specify the MAC address of a DHCPv4 client.

```
user@host> request dhcp server reconfigure 12:23:34:45:56:67
```

- Specify an interface; reconfiguration is attempted for all clients on this interface.

`user@host> request dhcp server reconfigure interface fe-0/0/0.100`

- Specify a logical system; reconfiguration is attempted for all clients or the specified clients in this logical system.

`user@host> request dhcp server reconfigure all logical-system ls-bldg5`

- Specify a routing instance; reconfiguration is attempted for all clients or the specified clients in this routing instance.

`user@host> request dhcp server reconfigure all routing-instance ri-boston`

**Related Documentation**

- Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 133
- `request dhcp server reconfigure`

---

## 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 Documentation**

- [Junos OS System Basics and Services Command Reference](#)

---

## Verifying and Managing DHCPv6 Local Server Configuration

**Purpose** View or clear information about client address bindings and statistics for the DHCPv6 local server.

**Action** • To display the address bindings in the client table on the DHCPv6 local server:

`user@host> show dhcpv6 server binding`

- To display DHCPv6 local server statistics:

`user@host> show dhcpv6 server statistics`

- To clear all DHCPv6 local server statistics:

`user@host> clear dhcpv6 server binding`



- To clear all DHCPv6 local server statistics:

```
user@host> clear dhcpv6 server statistics
```

**Related  
Documentation**

- [Junos OS System Basics and Services Command Reference](#)

---

## Graceful Routing Engine Switchover

The extended DHCP local server and the DHCP relay agent applications both maintain the state of active DHCP client leases in the session database. The extended DHCP application can recover this state if the DHCP process fails or is manually restarted, thus preventing the loss of active DHCP clients in either of these circumstances. However, the state of active DHCP client leases is lost if a power failure occurs or if the kernel stops operating (for example, when the router is reloaded) on a single Routing Engine.

The extended DHCP local server and the DHCP relay agent support graceful Routing Engine switchover on all routing platforms that contain dual Routing Engines. To support graceful Routing Engine switchover, the extended DHCP application 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 local server or 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 application when the router is configured to support graceful Routing Engine switchover.

For more information about using graceful Routing Engine switchover, see the [Junos OS High Availability Configuration Guide](#).

**Related  
Documentation**

- Extended DHCP Local Server Overview on page 98
- Extended DHCP Relay Agent Overview on page 154
- Subscriber Management Unified ISSU Support on page 6

---

## 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.

You can configure DHCP trace operations at the global level or at the interface level. If you configure interface-level trace operations, you can specify tracing for a range of interfaces or an individual interface.

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

- Important events for both global and per-interface tracing are logged in a file located in the `/var/log` directory. By default, the router uses the filename, `jdhcpd`. You can specify a different filename, but you cannot change the directory in which trace files are located.
- When the file `jdhcpd` reaches 128 kilobytes (KB), it is renamed `jdhcpd.0`, then `jdhcpd.1`, and finally `jdhcpd.2`, until there are three trace files. Then the oldest trace file (`jdhcpd.2`) is overwritten.

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

- By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To specify that you want to configure global DHCP tracing operations.

- For DHCP local server:

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

- For DHCP relay:

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

For information about configuring per-interface tracing options, see “Tracing Extended DHCP Operations for Specific Interfaces” on page 144.

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

- Configuring the Extended DHCP Log Filename on page 140
- Configuring the Number and Size of Extended DHCP Log Files on page 141
- Configuring Access to the Extended DHCP Log File on page 141
- Configuring a Regular Expression for Extended DHCP Lines to Be Logged on page 142
- Configuring the Extended DHCP Tracing Flags on page 142
- Tracing Extended DHCP Operations for Specific Interfaces on page 144

## 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 filename
```

## 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 finally **filename.2**, until there are three trace files. Then the oldest trace file (**filename.2**) is overwritten.

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

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 and the **interface-traceoptions** statement.

```
[edit system services dhcp-local-server traceoptions]
user@host# set file filename files number size maximum-file-size
```

## 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 and the **interface-traceoptions** statement.

```
[edit system services dhcp-local-server traceoptions]
user@host# set file filename 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 and the **interface-traceoptions** statement.

```
[edit system services dhcp-local-server traceoptions]
user@host# set file filename 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 to be matched.

To configure regular expressions to be matched, specify 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 filename match regular-expression
```

## 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. All flags are available for global tracing operations. The Interface-Specific Tracing column indicates the subset of flags that you can use for per-interface tracing.

Flag	Description	Interface-Specific Tracing
<b>all</b>	Trace all events	No
<b>auth</b>	Trace authentication events	No
<b>database</b>	Trace database events	No
<b>dhcpv6-general</b>	Trace miscellaneous DHCPv6 events	No
<b>dhcpv6-io</b>	Trace I/O operations for DHCPv6	No
<b>dhcpv6-packet</b>	Trace DHCPv6 packet decoding operations	Yes
<b>dhcpv6-packet-option</b>	Trace DHCPv6 option decoding operations	Yes
<b>dhcpv6-rpd</b>	Trace routing protocol process events for DHCPv6	No
<b>dhcpv6-session-db</b>	Trace session database operations for DHCPv6	No
<b>dhcpv6-state</b>	Trace changes in state for DHCPv6 operations	Yes
<b>fwd</b>	Trace firewall process events	No
<b>general</b>	Trace miscellaneous events	No

Flag	Description	Interface-Specific Tracing
<b>ha</b>	Trace high availability-related events	No
<b>interface</b>	Trace interface operations	No
<b>io</b>	Trace I/O operations	No
<b>packet</b>	Trace packet decoding operations	Yes
<b>packet-option</b>	Trace DHCP option decoding operations	Yes
<b>performance</b>	Trace performance measurement operations	No
<b>profile</b>	Trace profile operations	No
<b>rpd</b>	Trace routing protocol process events	No
<b>rtsock</b>	Trace routing socket operations	No
<b>session-db</b>	Trace session database events	No
<b>state</b>	Trace changes in state	Yes
<b>statistics</b>	Trace baseline statistics	No
<b>ui</b>	Trace user interface operations	No

To configure the flags for the events to be logged, specify the flags. DHCP local server and DHCP relay agent both support the **flag** option for the **traceoptions** statement and the **interface-traceoptions** statement.

- For global tracing operations

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

- For per-interface tracing operations

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

For additional information on configuring per-interface tracing options, see “Tracing Extended DHCP Operations for Specific Interfaces” on page 144.

## Tracing Extended DHCP Operations for Specific Interfaces

In addition to the global DHCP tracing operations, subscriber management enables you to trace extended DHCP operations for a specific interface or for a range of interfaces.

Configuring per-interface tracing is a two-step procedure. In the first step, you specify the tracing options that you want to use, such as file information and flags. In the second step, you enable the tracing operation on the specific interfaces.

To configure per-interface tracing operations:

1. Specify the tracing options you want to use.



**NOTE:** Per-interface tracing uses the same default tracing behavior as the global extended DHCP tracing operation. The default behavior is described in “Tracing Extended DHCP Operations” on page 139.

- a. Specify that you want to configure per-interface tracing options.

- For DHCP local server and DHCPv6 local server:

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

- For DHCP relay agent:

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

- b. (Optional) Specify the tracing file options.

- Configure the name for the file used for the trace output.

See “Configuring the Extended DHCP Log Filename” on page 140.

- Configure the number and size of the log files.

See “Configuring the Number and Size of Extended DHCP Log Files” on page 141.

- Configure access to the log file.

See “Configuring Access to the Extended DHCP Log File” on page 141.

- Configure a regular expression to filter logging events.

See “Configuring a Regular Expression for Extended DHCP Lines to Be Logged” on page 142.

- c. (Optional) Specify tracing flag options.

See “Configuring the Extended DHCP Tracing Flags” on page 142.

2. Enable tracing on an interface or interface range.

The following examples show a DHCP local server configuration. You can also use the **trace** statement at the **[edit forwarding-options dhcp-relay]** hierarchy level and at the **[edit system services dhcp-local-server dhcpv6]** hierarchy level.

- Enable tracing on a specific interface.

```
[edit system services dhcp-local-server]
user@host# set group group-name interface interface-name trace
```

- Enable tracing on a range of interfaces.

```
[edit system services dhcp-local-server]
user@host# set group group-name interface interface-name upto interface
interface-name trace
```





## CHAPTER 8

# DHCP Local Server Examples

- Example: Minimum Extended DHCP Local Server Configuration on page 147
- Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 147
- Example: Extended DHCPv6 Local Server Configuration on page 148

### Example: Minimum Extended DHCP Local Server Configuration

---

This example shows the minimum configuration you need to use for 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**.

**Related Documentation**

- Extended DHCP Local Server Overview on page 98

### Example: Extended DHCP Local Server Configuration with Optional Pool Matching

---

This example shows an extended DHCP local server configuration that includes optional IPv4 address-assignment pool matching and interface groups. For pool matching, this configuration specifies that the DHCP local server first check the response from an external authentication authority (for example, RADIUS) and use the Framed-IPv6-Pool attribute to determine the address-assignment pool to use for the client address. If no external authority match is found, the DHCP local server then uses ip-address-first matching together with the option 82 information to match the named address range for client IPv4 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 {
  external-authority
  ip-address-first;
  option-82;
}
}
```

**Related  
Documentation**

- [Extended DHCP Local Server Overview on page 98](#)
- [Address-Assignment Pools Overview on page 67](#)

---

## Example: Extended DHCPv6 Local Server Configuration

This example shows a sample extended DHCPv6 local server configuration. The second part of the example shows a sample RADIUS authentication configuration—authentication must be configured for DHCPv6 local server operations.

```
[edit system services]
dhcp-local-server {
  dhcpv6 {
    authentication {
      password v679M8vt;
      username-include {
        user-prefix wallybrown;
        domain-name isp55.com;
      }
    }
    group group_two {
      authentication {
        password P$55qw4$$;
        username-include {
          user-prefix south5;
          domain-name isp55.com;
        }
      }
      interface ge-1/0/3.0;
    }
  }
}
```

The following is a sample RADIUS authentication configuration.

```
[edit access]
radius-server {
  192.168.1.250 {
    port 1812;
    secret &tIUeI*7688+;
```

```
    }  
  }  
  profile isp-bos-metro-fiber-basic {  
    accounting-order radius;  
    authentication-order radius;  
    radius {  
      authentication-server 192.168.1.250;  
      accounting-server 192.168.1.250;  
    }  
    accounting {  
      order radius;  
      accounting-stop-on-failure;  
      accounting-stop-on-access-deny;  
      update-interval 10;  
      statistics time;  
    }  
  }  
}
```

**Related Documentation**

- [DHCPv6 Local Server Overview on page 102](#)



## PART 4

# DHCP Relay Agent for Subscriber Access

- DHCP Relay Agent Overview on page 153
- Configuring DHCP Relay Agent on page 161
- Configuring Dynamic Access and Access-Internal Routes for DHCP Subscriber Management on page 205
- DHCP Relay Agent Examples on page 209



## CHAPTER 9

# DHCP Relay Agent Overview

- Extended DHCP Relay Agent Overview on page 154
- DHCP Relay Proxy Overview on page 156
- Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview on page 158

## 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 OS Feature Guides](#).



**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 OS Routing Policy 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 822 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 154

## 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*.

#### Related Documentation

- Access and Access-Internal Routes for Subscriber Management on page 205
- Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview on page 104
- Using External AAA Authentication Services with DHCP on page 110
- DHCP Relay Proxy Overview on page 156
- Graceful Routing Engine Switchover on page 139
- Subscriber Management Unified ISSU Support on page 6
- Verifying and Managing DHCP Relay Configuration on page 198
- Tracing Extended DHCP Operations on page 139
- Example: Minimum DHCP Relay Agent Configuration on page 209
- Example: DHCP Relay Agent Configuration with Multiple Clients and Servers on page 209

- Example: Using Option 60 Strings to Forward DHCP Client Traffic on page 213
- Example: Using Option 60 Strings to Drop DHCP Client Traffic on page 214

## DHCP Relay Proxy Overview

---

DHCP relay proxy mode is an enhancement to extended DHCP relay. DHCP relay proxy supports all DHCP relay features while providing additional features and benefits.

Normally, extended DHCP relay operates as a helper application for DHCP operations. Except for the ability to add DHCP relay agent options and the gateway address (giaddr) to DHCP packets, DHCP relay is transparent to DHCP clients and DHCP servers, and simply forwards messages between DHCP clients and servers.

When you configure DHCP relay to operate in proxy mode, the relay is no longer transparent. In proxy mode, DHCP relay conceals DHCP server details from DHCP clients, which interact with a DHCP relay in proxy mode as though it is the DHCP server. For DHCP servers there is no change, because proxy mode has no effect on how the DHCP server interacts with the DHCP relay.

DHCP relay proxy provides the following benefits:

- DHCP server isolation and DoS protection—DHCP clients are unable to detect the DHCP servers, learn DHCP server addresses, or determine the number of servers that are providing DHCP support. Server isolation also provides denial-of-service (DoS) protection for the DHCP servers.
- Multiple lease offer selection—DHCP relay proxy receives lease offers from multiple DHCP servers and selects a single offer to send to the DHCP client, thereby reducing traffic in the network. Currently, the DHCP relay proxy selects the first offer received.
- Support for both numbered and unnumbered Ethernet interfaces—For DHCP clients connected through Ethernet interfaces, when the DHCP client obtains an address, the DHCP relay proxy adds an access internal host route specifying that interface as the outbound interface. The route is automatically removed when the lease time expires or when the client releases the address.
- Logical system support—DHCP relay proxy can be configured in a logical system, whereas a non-proxy mode DHCP relay cannot.



**NOTE:** Extended DHCP relay proxy is not supported for the J Series Services Routers DHCP server. Also, you cannot configure both DHCP relay proxy and extended DHCP local server on the same interface.

---

## Interaction Among DHCP Relay Proxy, DHCP Client, and DHCP Servers

The DHCP relay agent is configured on the router, which operates between the DHCP client and one or more DHCP servers.

The following steps provide a high-level description of how DHCP relay proxy interacts with DHCP clients and DHCP servers.

1. The DHCP client sends a discover packet to locate a DHCP server in the network from which to obtain configuration parameters for the subscriber.
2. The DHCP relay proxy receives the discover packet from the DHCP client and forwards copies of the packet to each supporting DHCP server. The DHCP relay proxy then creates a client table entry to keep track of the client state.
3. In response to the discover packet, each DHCP server sends an offer packet to the client, which the DHCP relay proxy receives. The DHCP relay proxy does the following:
  - a. Selects the first offer received as the offer to sent to the client
  - b. Replaces the DHCP server address with the address of the DHCP relay proxy
  - c. Forwards the offer to the DHCP client.
4. The DHCP client receives the offer from the DHCP relay proxy.
5. The DHCP client sends a request packet that indicates the DHCP server from which to obtain configuration information—the request packet specifies the address of the DHCP relay proxy.
6. The DHCP relay proxy receives the request packet and forwards copies, which include the address of selected server, to all supporting DHCP servers.
7. The DHCP server requested by the client sends an acknowledgement (ACK) packet that contains the client configuration parameters.
8. The DHCP relay proxy receives the ACK packet, replaces the DHCP server address with its own address, and forwards the packet 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 proxy installs a host route and Address Resolution Protocol (ARP) entry for the DHCP client.
11. After the initial DHCP lease is established, the DHCP relay proxy receives all lease renewals and lease releases from the DHCP client and forwards them to the DHCP server.

**Related  
Documentation**

- [Extended DHCP Relay Agent Overview on page 154](#)
- [Enabling DHCP Relay Proxy Mode on page 196](#)

## 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** statement 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. The **aggregate-clients** statement provides the option of either merging (chaining) or replacing software components for each client.

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.

When you specify the **merge** option, the router aggregates 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.

When you specify the **replace** option, the entire logical interface is replaced whenever a new client logs in to the network using the same VLAN logical interface. For example, if a customer subscribes to voice, video, and data services on the network, when a voice client logs in, instead of applying a specific voice filter for only that service, the entire voice, video, and data filter chain is applied.



**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 IP demux interfaces are used to represent subscribers. To conserve interfaces, make sure the primary profile that you specify does not create a demux interface, but provides the initial policies for the primary interface subscriber.

### Related Documentation

- [Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125](#)



## CHAPTER 10

# Configuring DHCP Relay Agent

- DHCP Duplicate Client Differentiation Using Client Subinterface Overview on page 162
- Guidelines for Configuring Support for DHCP Duplicate Clients on page 163
- Configuring DHCP Duplicate Client Support on page 163
- Using External AAA Authentication Services with DHCP on page 164
- Grouping Interfaces with Common DHCP Configurations on page 165
- Guidelines for Configuring Interface Ranges on page 166
- Group-Specific DHCP Relay Options on page 167
- Overriding the Default DHCP Relay Configuration Settings on page 168
- Overwriting giaddr Information on page 170
- Replacing the DHCP Relay Request and Release Packet Source Address on page 170
- Overriding Option 82 Information on page 170
- Using Layer 2 Unicast Transmission for DHCP Packets on page 171
- Trusting Option 82 Information on page 172
- Disabling ARP Table Population on page 172
- Specifying the Maximum Number of DHCP Clients Per Interface on page 173
- DHCP Snooping Support on page 174
- Configuring DHCP Snooping for DHCP Relay Agent on page 175
- Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent on page 176
- Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent on page 178
- DHCP Auto Logout Overview on page 180
- DHCP Relay Agent Option 82 Value for Auto Logout on page 182
- Automatically Logging Out DHCP Clients on page 183
- Sending Release Messages When Clients Are Deleted on page 184
- Subscriber Binding Retention During Interface Delete Events on page 185
- Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 185
- Verifying and Managing the DHCP Maintain Subscribers Feature on page 186

- Disabling DHCP Relay on page 187
- Disabling Automatic Binding of Stray DHCP Requests on page 187
- Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 189
- Using Matching Option 60 Strings to Process DHCP Client Traffic on page 189
- Using Nonmatching Option 60 Strings to Process DHCP Client Traffic on page 192
- Displaying a Count of Discarded DHCP Packets with Option 60 Information on page 192
- Enabling and Disabling Insertion of Option 82 Information on page 192
- Configuring Server Groups on page 195
- Configuring Active Server Groups on page 196
- Enabling DHCP Relay Proxy Mode on page 196
- Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 197
- Verifying and Managing DHCP Relay Configuration on page 198
- Tracing Extended DHCP Operations on page 199

## DHCP Duplicate Client Differentiation Using Client Subinterface Overview

---

In some network environments, client IDs and MAC addresses might not be unique, resulting in duplicate clients. For example, two network adapters might be manufactured with the same hardware address, resulting in a duplicate MAC address among the DHCP clients attached to the router. A duplicate DHCP client occurs when a client attempts to get a lease, and that client has the same client ID or the same MAC address as an existing DHCP client.

When DHCP server receives a request from a new client that has a duplicate ID or MAC address, DHCP server terminates the address lease for the existing client and returns the address to its original address pool. DHCP server then assigns a new address and lease to the new client.

By default, both DHCP local server and DHCP relay use the subnet information to differentiate between duplicate clients. However, in some cases, this level of differentiation is not adequate. For example, when multiple subinterfaces share the same underlying loopback interface with the same preferred source address, the interfaces appear to be on the same subnet. In this situation, the default configuration prevents duplicate clients.

You can provide greater differentiation between duplicate clients by configuring DHCP to consider the client subinterface when duplicate clients occur. In this optional configuration, DHCP uniquely identifies:

- The subnet on which the client resides
- The subinterface on which the client resides
- The client within the subnet

### Related Documentation

- Configuring DHCP Duplicate Client Support on page 109



- Guidelines for Configuring Support for DHCP Duplicate Clients on page 109

## Guidelines for Configuring Support for DHCP Duplicate Clients

This topic describes the guidelines for configuring DHCP to include the client subinterface in order to distinguish between duplicate clients (clients with the same MAC address or client ID) in a subscriber access environment.

When configuring DHCP duplicate client support, consider the following guidelines:

- The optional DHCP duplicate client support feature is used for DHCPv4 clients. For DHCPv6, client identification is independent of MAC address.
- For DHCP relay agent configuration:
  - DHCP relay must be configured to insert option 82, regardless of whether or not the incoming packet has option 82.
  - Option 82 must include the Agent Circuit ID suboption (suboption 1).
  - Option 82 must be the interface name, not the interface description.
  - DHCP server must echo option 82 in the server's reply. This is required because of the following:
    - The giaddr inserted by DHCP relay is the same for duplicate clients on different subinterfaces. The DHCP local server uses option 82 when allocating the IP address.
    - DHCP relay uses the echoed option 82 to learn the client subinterface and to construct the client key.
- For the Layer 3 wholesale model:
  - The wholesaler and retailer logical system/routing instances must have the same **duplicate-clients-on-interface** statement configuration.
  - For DHCP relay, the wholesaler and the retailer routing contexts must both be configured with the Agent Circuit ID suboption (suboption 1) in option 82.

### Related Documentation

- DHCP Duplicate Client Differentiation Using Client Subinterface Overview on page 108
- Configuring DHCP Duplicate Client Support on page 109

## Configuring DHCP Duplicate Client Support

You can optionally configure DHCP local server and DHCP relay to include a client subinterface when distinguishing between two clients that have the same MAC address or client ID. The configuration is a global setting for each logical system/routing instance.

To configure DHCP local server to include the client subinterface:

1. Specify that you want to configure DHCP local server.

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

2. Configure the optional duplicate client support.

```
[edit system services dhcp-local-server]
user@host# set duplicate-clients-on-interface
```

To configure DHCP relay agent to include the client subinterface:

1. Specify that you want to configure DHCP relay agent.

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

2. Configure the optional duplicate client support.

```
[edit system services dhcp-relay]
user@host# set duplicate-clients-on-interface
```

**Related  
Documentation**

- DHCP Duplicate Client Differentiation Using Client Subinterface Overview on page 108
- Guidelines for Configuring Support for DHCP Duplicate Clients on page 109

---

## Using External AAA Authentication Services with DHCP

---

The extended DHCP local server, including DHCPv6 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 responds as though it were 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
```
  - For DHCPv6 local server:
 

```
[edit system services dhcp-local-server dhcpv6]
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 127.
3. (Optional) Configure optional features to create a unique username.
 

See “Creating Unique Usernames for DHCP Clients” on page 128.

#### Related Documentation

- Extended DHCP Local Server Overview on page 98
- Extended DHCP Relay Agent Overview on page 154
- DHCPv6 Local Server Overview on page 102

## 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, including the DHCPv6 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 the DHCPv6 local server and DHCP relay agent.
 

```
[edit system services dhcp-local-server]
user@host# edit group boston
```
2. Create the group and assign a name.
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# set interface fe-1/0/1.1 upto fe-1/0/1.102
user@host# set interface fe-1/0/1.6 exclude
user@host# set interface fe-1/0/1.70 upto fe-1/0/1.80 exclude
```

#### Related Documentation

- Extended DHCP Local Server Overview on page 98
- Extended DHCP Relay Agent Overview on page 154
- DHCPv6 Local Server Overview on page 102
- Group-Specific DHCP Local Server Options on page 115
- Group-Specific DHCP Relay Options on page 167
- Guidelines for Configuring Interface Ranges on page 113

---

## Guidelines for Configuring Interface Ranges

This topic describes guidelines to consider when configuring interface ranges for named interface groups for DHCP local server and DHCP relay. The guidelines refer to the following configuration statement:

```
user@host# set interface interface-name upto upto-interface-name
```

- The start subunit, **interface *interface-name***, serves as the key for the stanza. The remaining configuration settings are considered attributes.
- If the subunit is not included, an implicit **.0** subunit is enforced. The implicit subunit is applied to all interfaces when autoconfiguration is enabled. For example, **interface ge-2/2/2** is treated as **interface ge-2/2/2.0**.
- Ranged entries contain the **upto** option, and the configuration applies to all interfaces within the specified range. The start of a ranged entry must be less than the end of the range. Discrete entries apply to a single interface, except in the case of autoconfiguration, in which a **0** (zero) subunit acts as a wildcard.
- Interface stanzas defined within the same router context are dependent and can constrain each other—both DHCP local server and DHCP relay are considered. Interface stanzas defined across different router contexts are independent and do not constrain one another.

- Each interface stanza, whether discrete or ranged, has a unique start subunit across a given router context. For example, the following configuration is not allowed within the same group because **ge-1/0/0.10** is the start subunit for both.

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.10
```

- Two groups cannot share interface space. For example, the following configuration is not allowed because the three stanzas share the same space and interfere with one another—interface **ge-1/0/0.26** is common to all three.

```
dhcp-relay group diamond interface ge-1/0/0.10 upto ge-1/0/0.30
dhcp-local-server group ruby interface ge-1/0/0.26
dhcp-relay group sapphire interface ge-1/0/0.25 upto ge-1/0/0.35
```

- Two ranges cannot overlap, either within a group or across groups. Overlapping occurs when two interface ranges share common subunit space but neither range is a proper subset of the other. The following ranges overlap:

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.20 upto ge-1/0/0.40
```

- A range can contain multiple nested ranges. A nested range is a proper subset of another range. When ranges are nested, the smallest matching range applies.

In the following example, the three ranges nest properly:

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.12 upto ge-1/0/0.15 exclude
interface ge-1/0/0.25 upto ge-1/0/0.29 exclude
```

- Discrete interfaces take precedence over ranges. In the following example, interface **ge-1/0/0.20** takes precedence and enforces an interface client limit of 5.

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.15 upto ge-1/0/0.25 exclude
interface ge-1/0/0.20 overrides interface-client-limit 5
```

#### Related Documentation

- Grouping Interfaces with Common DHCP Configurations on page 112

## 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 196.
- 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 Settings” on page 168.
- **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 189.
- **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 192.

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  
Documentation**

- Grouping Interfaces with Common DHCP Configurations on page 112

---

## Overriding the Default DHCP Relay Configuration Settings

---

Subscriber management enables you to override certain default DHCP relay agent configuration settings. You can override the settings at the global level, for a named group of interfaces, or for a specific interface within a named group.

- 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 relay configuration options for a named group of interfaces, include the statements at the **[edit forwarding-options dhcp-relay group group-name]** hierarchy level.
- To override DHCP relay configuration options for a specific interface within a named group of interfaces, include the statements at the **[edit forwarding-options dhcp-relay group group-name interface]** hierarchy level.

To override default DHCP relay agent configuration settings:

1. Specify that you want to configure override options.

Global override:

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

Group-level override:

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

Per-interface override:

```
[edit forwarding-options dhcp-relay]
user@host# edit group boston overrides interface fe-1/0/1.2
```

2. (Optional) Enable DHCP relay proxy mode.  
See “Enabling DHCP Relay Proxy Mode” on page 196.
3. (Optional) Overwrite the giaddr in DHCP packets that the DHCP relay agent forwards.  
See “Overwriting giaddr Information” on page 170.
4. (Optional) Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).  
See “Replacing the DHCP Relay Request and Release Packet Source Address” on page 170.
5. (Optional) Override the DHCP relay agent information option (option 82) in DHCP packets.  
See “Overriding Option 82 Information” on page 170.
6. (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 171.
7. (Optional) Trust DHCP client packets that have a giaddr of 0 and that contain option 82 information.  
See “Trusting Option 82 Information” on page 172.
8. (Optional) Override the ARP table population in distrusted environments.  
See “Disabling ARP Table Population” on page 117.
9. (Optional) Override the maximum number of DHCP clients allowed per interface.  
See “Specifying the Maximum Number of DHCP Clients Per Interface” on page 116.
10. (Optional) Configure client auto logout.  
See “DHCP Auto Logout Overview” on page 120.
11. Enable or disable support for DHCP snooped clients on interfaces.  
See “Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent” on page 176.
12. (Optional) Send release messages to the DHCP server when clients are deleted.  
See “Sending Release Messages When Clients Are Deleted” on page 184.
13. (Optional) Disable the DHCP relay agent on specific interfaces.  
See “Disabling DHCP Relay” on page 187.
14. (Optional) Disable automatic binding of stray DHCP requests.  
See “Disabling Automatic Binding of Stray DHCP Requests” on page 187.

- Related Documentation**
- Group-Specific DHCP Relay Options on page 167
  - Deleting DHCP Local Server and DHCP Relay Override Settings on page 122

---

## 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
```

- Related Documentation**
- Extended DHCP Relay Agent Overview on page 154
  - Overriding the Default DHCP Relay Configuration Settings on page 168

---

## Replacing the DHCP Relay Request and Release Packet Source Address

You can configure the DHCP relay agent to replace request and release packets with the gateway IP address (giaddr) before forwarding the packet to the DHCP server.

To replace the source address with giaddr:

1. Specify that you want to configure override options.

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

2. Specify that you want to replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).

```
[edit forwarding-options dhcp-relay overrides]  
user@host# set replace-ip-source-with giaddr
```

- Related Documentation**
- Extended DHCP Relay Agent Overview on page 154
  - Overriding the Default DHCP Relay Configuration Settings on page 168

---

## 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
```

**Related  
Documentation**

- Extended DHCP Relay Agent Overview on page 154
- Overriding the Default DHCP Relay Configuration Settings on page 168

## 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
```

**Related  
Documentation**

- Extended DHCP Relay Agent Overview on page 154
- Overriding the Default DHCP Relay Configuration Settings on page 168

## 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
```

### Related Documentation

- Extended DHCP Relay Agent Overview on page 154
- Overriding the Default DHCP Relay Configuration Settings on page 168

## 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 24: 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 25: 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
```

**Related Documentation**

- [Overriding Default DHCP Local Server Configuration Settings on page 115](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 122](#)
- [Extended DHCP Local Server Overview on page 98](#)
- [DHCPv6 Local Server Overview on page 102](#)
- [Extended DHCP Relay Agent Overview on page 154](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 122](#)

**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 through 500,000. When the number of clients on the interface reaches the specified limit, no additional DHCP Discover PDUs or DHCPv6 Solicit PDUs are accepted. When the number of clients subsequently drops below the limit, new clients are again accepted.



**NOTE:** The maximum number of DHCP (and DHCPv6) 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 DHCPv6 local server:

```
[edit system services dhcp-local-server dhcpv6]
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, DHCPv6 local server, and DHCP relay agent all support the **interface-client-limit** statement.)

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

#### Related Documentation

- Overriding Default DHCP Local Server Configuration Settings on page 115
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 122
- Extended DHCP Local Server Overview on page 98
- Extended DHCP Relay Agent Overview on page 154

---

## DHCP Snooping Support

DHCP snooping provides DHCP security on the router by filtering incoming messages. When DHCP snooping is enabled, the router differentiates between trusted and untrusted interfaces, and forwards messages from trusted sources while rejecting the untrusted messages.



**NOTE:** In Junos OS Release 10.0 and earlier, DHCP snooping is enabled by default. In Junos OS Release 10.1 and later, DHCP snooping is disabled by default.

You can configure DHCP snooping support for the following:

- DHCP relay agent—Override the router's default snooping configuration and specify that DHCP snooping is enabled or disabled globally, for a named group of interfaces, or for a specific interface within a named group.

In a separate procedure, you can set a global configuration to specify whether DHCP relay agent forwards or drops snooped packets for all interfaces, only configured interfaces, or only nonconfigured interfaces. The router also uses the global DHCP relay agent snooping configuration to determine whether to forward or drop snooped BOOTREPLY packets.

- DHCP local server—Configure whether DHCP local server forwards or drops snooped packets for all interfaces, only configured interfaces, or only nonconfigured interfaces.

#### Related Documentation

- Configuring DHCP Snooping for DHCP Relay Agent on page 175
- Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server on page 119
- Example: Configuring DHCP Snooping Support for DHCP Relay Agent on page 211

## Configuring DHCP Snooping for DHCP Relay Agent

DHCP relay agent uses a two-part configuration to determine how to handle DHCP snooped packets. First, you enable or disable snooping support for DHCP relay agent and, optionally, override the default snooping configuration. Then you configure the forwarding action for snooped clients, which specifies whether DHCP relay agent forwards or drops snooped traffic.

To configure DHCP snooping for DHCP relay agent:

1. Enable or disable DHCP snooping. You can configure DHCP snooping globally, for a named group of interfaces, or for a specific interface.

See “Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent” on page 176.

2. Configure snooped packets forwarding support.

See “Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent” on page 178.

#### Related Documentation

- DHCP Snooping Support on page 174
- Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent on page 176

- Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent on page 178
- Example: Configuring DHCP Snooping Support for DHCP Relay Agent on page 211

## Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent

---

DHCP relay agent uses a two-part configuration to determine how to handle DHCP snooped packets. This topic describes the first procedure, in which you configure DHCP relay to either enable or disable support for snooped packets. The second procedure is described in “Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent” on page 178, and configures the **forward-snooped-clients** statement, which determines whether the snooped packets are forwarded or dropped, depending on the type of interface.



**NOTE:** The router has a default global setting that specifies whether DHCP snooping support is enabled or disabled for DHCP relay. In Junos OS Release 10.0 and earlier, DHCP snooping is enabled by default. In Junos OS Release 10.1 and later, DHCP snooping is disabled by default.

You can override the default global DHCP snooping configuration and explicitly enable or disable DHCP snooping support. You can configure the explicit snooping support globally, for a group of interfaces, or for a specific interface in a group.

- To enable DHCP snooping support, include the **allow-snooped-clients** option in the **overrides** statement.
- To disable DHCP snooping support, include the **no-allow-snooped-clients** option in the **overrides** statement.

To enable or disable DHCP snooping support globally:

1. Specify that you want to configure DHCP relay agent.

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

2. Specify that you want to override the default configuration.

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

3. Enable or disable DHCP snooping support.

- To enable DHCP snooping:

```
[edit forwarding-options dhcp-relay overrides]
user@host# set allow-snooped-clients
```

- To disable DHCP snooping:

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

For example, to enable global DHCP snooping support :

```
forwarding-options {
  dhcp-relay {
    overrides {
      allow-snooped-clients;
    }
  }
}
```

To enable or disable DHCP snooping support for a group of interfaces:

1. Specify that you want to configure DHCP relay agent.

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

2. Specify the named group.

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

3. Specify that you want to override the default configuration.

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

4. Enable or disable DHCP snooping support.

- To enable DHCP snooping:

```
[edit forwarding-options dhcp-relay group group-name overrides]
user@host# set allow-snooped-clients
```

- To disable DHCP snooping:

```
[edit forwarding-options dhcp-relay group group-name overrides]
user@host# set no-allow-snooped-clients
```

For example, to enable DHCP snooping support on all interfaces in group **boston**:

```
forwarding-options {
  dhcp-relay {
    group boston {
      overrides {
        allow-snooped-clients;
      }
    }
  }
}
```

To enable or disable DHCP snooping support on a specific interface:

1. Specify that you want to configure DHCP relay agent.

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

2. Specify the named group containing the interface.

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

```
user@host# edit group group-name
```

3. Specify the interface for which you want to configure DHCP snooping.

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

```
user@host# edit interface interface-name
```

4. Specify that you want to override the default configuration on the interface.

```
[edit forwarding-options dhcp-relay group group-name interface interface-name]
```

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

5. Enable or disable DHCP snooping support.

- To enable DHCP snooping:

```
[edit forwarding-options dhcp-relay group group-name interface interface-name  
overrides]
```

```
user@host# set allow-snooped-clients
```

- To disable DHCP snooping:

```
[edit forwarding-options dhcp-relay group group-name interface interface-name  
overrides]
```

```
user@host# set no-allow-snooped-clients
```

For example, to disable DHCP snooping support on interface **ge-2/1/8.0**, which is in group **boston**:

```
forwarding-options {  
  dhcp-relay {  
    group boston {  
      interface ge-2/1/8.0 {  
        overrides {  
          no-allow-snooped-clients;  
        }  
      }  
    }  
  }  
}
```

#### Related Documentation

- Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent on page 178
- DHCP Snooping Support on page 174
- Overriding the Default DHCP Relay Configuration Settings on page 168

---

## Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent

You can configure how DHCP relay agent handles DHCP snooped packets. Depending on the configuration, DHCP relay agent either forwards or drops the snooped packets it receives.

DHCP relay uses a two-part configuration to determine how to handle DHCP snooped packets. This topic describes how you use the **forward-snooped-clients** statement to manage whether DHCP relay agent forwards or drops snooped packets, depending on



the type of interface on which the packets are snooped. In the other part of the DHCP relay agent snooping configuration, which is described in “Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent” on page 176, you enable or disable the DHCP relay snooping feature.

Table 26 on page 179 shows the action the router takes on snooped packets when DHCP snooping is enabled by the **allow-snooped-clients** statement. Table 27 on page 179 shows the action the router takes on snooped packets when DHCP snooping is disabled by the **no-allow-snooped-clients** statement.

The router also uses the configuration of the DHCP relay agent forwarding support to determine how to handle snooped BOOTREPLY packets. Table 28 on page 180 shows the action the router takes for the snooped BOOTREPLY packets.



**NOTE:** Configured interfaces have been configured with the **group** statement in the **[edit forwarding-options dhcp-relay]** hierarchy. Non-configured interfaces are in the logical system/routing instance but have not been configured by the **group** statement.

**Table 26: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Enabled**

forward-snooped-clients Configuration	Action on Configured Interfaces	Action on Non-Configured Interfaces
<b>forward-snooped-clients</b> not configured	snooped packets result in subscriber creation	dropped
<b>all-interfaces</b>	forwarded	forwarded
<b>configured-interfaces</b>	forwarded	dropped
<b>non-configured-interfaces</b>	snooped packets result in subscriber creation	forwarded

**Table 27: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Disabled**

forward-snooped-clients Configuration	Action on Configured Interfaces	Action on Non-Configured Interfaces
<b>forward-snooped-clients</b> not configured	dropped	dropped
<b>all-interfaces</b>	dropped	forwarded
<b>configured-interfaces</b>	dropped	dropped
<b>non-configured-interfaces</b>	dropped	forwarded

Table 28: Actions for Snooped BOOTREPLY Packets

forward-snooped-clients Configuration	Action
<b>forward-snooped-clients</b> not configured	snooped <b>BOOTREPLY</b> packets dropped if client is not found
<b>forward-snooped-clients</b> all configurations	snooped <b>BOOTREPLY</b> packets forwarded if client is not found

To configure DHCP snooped packet forwarding and BOOTREPLY snooped packet forwarding for DHCP relay agent:

1. Specify that you want to configure DHCP relay agent.

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

2. Enable DHCP snooped packet forwarding.

```
[edit forwarding-options dhcp-relay]
user@host# edit forward-snooped-clients
```

3. Specify the interfaces that are supported for snooped packet forwarding.

```
[edit forwarding-options dhcp-relay forward-snooped-clients]
user@host# set (all-interfaces | configured-interfaces | non-configured-interfaces)
```

For example, to configure DHCP relay agent to forward DHCP snooped packets on only configured interfaces:

```
[edit]
forwarding-options {
  dhcp-relay {
    forward-snooped-clients configured-interfaces;
  }
}
```

#### Related Documentation

- DHCP Snooping Support on page 174
- Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent on page 176

## 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 181
- How DHCP Identifies and Releases Clients on page 181
- Option 60 and Option 82 Requirements on page 182

## 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 discover 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 182.

### Related Documentation

- Automatically Logging Out DHCP Clients on page 121
- DHCP Relay Agent Option 82 Value for Auto Logout on page 182

## DHCP Relay Agent Option 82 Value for Auto Logout

Table 29 on page 182 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 29: DHCP Relay Agent Option 82 Value for Auto Logout**

DHCP Relay Agent Configuration Settings				giaddr in non-snooped packet	Action Taken
DHCP Relay Configured with Option 82	Discover Packet Contains Option 82	Override “trust-option-82”	Override “always-write-option-82”		
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

Table 29: DHCP Relay Agent Option 82 Value for Auto Logout (*continued*)

DHCP Relay Agent Configuration Settings				giaddr in non-snooped packet	Action Taken
DHCP Relay Configured with Option 82	Discover Packet Contains Option 82	Override "trust-option-82"	Override "always-write-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 Documentation**

- DHCP Auto Logout Overview on page 120
- Automatically Logging Out DHCP Clients on page 121

## 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# set client-discover-match
```

- For DHCP relay:

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

- DHCP Auto Logout Overview on page 120
- DHCP Relay Agent Option 82 Value for Auto Logout on page 182
- Deleting DHCP Local Server and DHCP Relay Override Settings on page 122
- Extended DHCP Local Server Overview on page 98
- Extended DHCP Relay Agent Overview on page 154

---

## Sending Release Messages When Clients Are Deleted

By default, when DHCP relay and relay proxy delete a client, they do not send a release message to the DHCP server. You can override the default behavior and configure DHCP relay and relay proxy to send a release message whenever they delete a client. The release message sent by DHCP relay and relay proxy includes option 82 information.

---



**NOTE:** In Junos OS Release 10.1 and earlier, DHCP relay sends a release message to the DHCP server when the **client-discover-match** statement is included as a DHCP relay override. In Junos OS Release 10.2 and later, you must include the **send-release-on-delete** statement to configure DHCP relay and relay proxy to send the release message when the **client-discover-match** statement is included.

---

To send a release message:

1. Specify that you want to configure overrides.

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

- Specify that you want DHCP relay and relay proxy to send a release message when clients are deleted.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set send-release-on-delete
```

**Related  
Documentation**

- Extended DHCP Relay Agent Overview on page 154
- Overriding the Default DHCP Relay Configuration Settings on page 168

## Subscriber Binding Retention During Interface Delete Events

You can configure the router to maintain DHCP subscribers when an event occurs that normally results in the router deleting the subscriber. For example, by default, the router logs out DHCP subscribers when an interface delete event occurs, such as a DPC reboot or failure. However, if you configure the router to maintain subscribers, the router identifies each subscriber that was on the deleted interface, and resumes normal packet processing for the subscriber when the interface is restored.



**NOTE:** Subscribers are logged off as usual when their lease expires, even if the router is configured to maintain subscribers and the subscriber is on a deleted interface that has not yet been restored.

You configure the router to maintain subscribers on a global basis— the configuration applies to DHCP local server, DHCPv6 local server, and DHCP relay clients in all logical routers and routing instances. When you enable the maintain subscribers feature, the router applies the feature to existing subscribers as well as subscribers who later connect.

If the maintain subscribers feature is enabled on the router, you can explicitly delete a subscriber binding and log out the subscriber by either specifying a lease expiration timeout or using one of the following commands, as appropriate:

- clear dhcp server binding**
- clear dhcpv6 server binding**
- clear dhcp relay binding**

**Related  
Documentation**

- Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 124
- Verifying and Managing the DHCP Maintain Subscribers Feature on page 125

## Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events

You can specify a configuration in which the router does not log out a subscriber when the subscriber's interface is deleted.

To configure the router to maintain DHCP subscribers when the subscriber interface is deleted:

1. Specify that you want to configure subscriber management.

```
[edit system services]
user@host# edit subscriber-management
```

2. Configure the router to support the maintain-subscriber feature.

```
[edit system services subscriber-management]
user@host# edit maintain-subscriber
```

3. Configure the router to enable the maintain-subscriber feature when an interface-delete event occurs.

```
[edit system services subscriber-management maintain-subscriber]
user@host# set interface-delete
```

- Related Documentation**
- Subscriber Binding Retention During Interface Delete Events on page 123
  - Verifying and Managing the DHCP Maintain Subscribers Feature on page 125

---

## Verifying and Managing the DHCP Maintain Subscribers Feature

---

**Purpose** Display information related to the DHCP maintain-subscribers feature and explicitly log out maintained clients.

- Action**
- To display DHCP local server binding information for the DHCP maintain subscribers feature:  

```
user@host>show dhcp server binding detail
```
  - To display DHCPv6 local server binding information for the DHCP maintain subscribers feature:  

```
user@host>show dhcpv6 server binding detail
```
  - To display DHCP relay binding information for the DHCP maintain subscribers feature:  

```
user@host>show dhcp relay binding detail
```
  - To explicitly log out a DHCP local server subscriber when the maintain subscriber feature is enabled:  

```
user@host>clear dhcp server binding binding-type
```
  - To explicitly log out a DHCPv6 local server subscriber when the maintain subscriber feature is enabled:  

```
user@host>clear dhcpv6 server binding binding-type
```
  - To explicitly log out a DHCP relay subscriber when the maintain subscriber feature is enabled:  

```
user@host>clear dhcp relay binding binding-type
```



- Related Documentation**
- Subscriber Binding Retention During Interface Delete Events on page 123
  - Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 124

## 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
```

- Related Documentation**
- Extended DHCP Relay Agent Overview on page 154
  - Deleting DHCP Local Server and DHCP Relay Override Settings on page 122

## Disabling Automatic Binding of Stray DHCP Requests

DHCP requests that are received but have no entry in the database are known as stray requests. By default, DHCP relay and DHCP relay proxy attempt to bind the requesting client by creating a database entry and forwarding the request to the DHCP server. If the server responds with an ACK, the client is bound and the ACK is forwarded to the client. If the server responds with a NAK, the database entry is deleted and the NAK is forwarded to the client. This behavior occurs regardless of whether authentication is configured.

You can override the default configuration at the global level, for a named group of interfaces, or for a specific interface within a named group. Overriding the default causes DHCP relay and DHCP relay proxy to drop all stray requests instead of attempting to bind the clients.



**NOTE:** In Junos OS Release 10.4 and later, automatic binding of stray requests is enabled by default.

In Junos OS Release 10.3 and earlier releases, automatic binding of stray requests is disabled by default. In those releases, DHCP relay drops stray requests and forwards a NAK to the client when authentication is configured. Otherwise, DHCP relay attempts to bind the requesting client. In those releases, DHCP relay proxy always drops stray requests and forwards a NAK to the client, regardless of the authentication configuration.

- To disable automatic binding behavior, include the **no-bind-on-request** statement when you configure DHCP overrides at the global, group, or interface level.

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

The following two examples show a configuration that disables automatic binding of stray requests for a group of interfaces and a configuration that disables automatic binding on a specific interface.

To disable automatic binding of stray requests on a group of interfaces:

1. Specify the named group.

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

2. Specify that you want to configure overrides.

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

3. Disable automatic binding for the group.

```
[edit forwarding-options dhcp-relay group boston overrides]
user@host# set no-bind-on-request
```

To disable automatic binding of stray requests on a specific interface:

1. Specify the named group of which the interface is a member.

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

2. Specify the interface on which you want to disable automatic binding.

```
[edit forwarding-options dhcp-relay group boston]
user@host# edit interface fe-1/0/1.2
```

3. Specify that you want to configure overrides.

```
[edit forwarding-options dhcp-relay group boston interface fe-1/0/1.2]
user@host# edit overrides
```

4. Disable automatic binding on the interface.

```
[edit forwarding-options dhcp-relay group boston interface fe-1/0/1.2 overrides]
user@host# set no-bind-on-request
```

**Related  
Documentation**

- Extended DHCP Relay Agent Overview on page 154
- Overriding the Default DHCP Relay Configuration Settings on page 168

## 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 189.

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 192.

4. (Optional) Display a count of the number of discarded packets with option 60 information.

See “Displaying a Count of Discarded DHCP Packets with Option 60 Information” on page 192.

### Related Documentation

- Using Matching Option 60 Strings to Process DHCP Client Traffic on page 189
- Using Nonmatching Option 60 Strings to Process DHCP Client Traffic on page 192
- Displaying a Count of Discarded DHCP Packets with Option 60 Information on page 192

## 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 195.

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. 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. 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 “Extended DHCP Local Server Overview” on page 98.

- To drop (discard) the packets:

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

#### Related Documentation

- Example: Using Option 60 Strings to Forward DHCP Client Traffic on page 213
- Example: Using Option 60 Strings to Drop DHCP Client Traffic on page 214

## 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 nonmatching packets:

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

### Related Documentation

- Example: Using Option 60 Strings to Forward DHCP Client Traffic on page 213
- Example: Using Option 60 Strings to Drop DHCP Client Traffic on page 214

## 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**

### Related Documentation

- *Junos OS 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. You can configure option 82 support globally or for a named group of interfaces.

To restore the default behavior (option 82 information is not inserted into DHCP packets), you use the **delete relay-option-82** statement.

To configure support for the DHCP relay agent information option 82, you use the **relay-option-82** statement.

The following sections describe the option 82 operations you can configure:

- Configuring Agent Circuit ID Information on page 193
- Configuring an Option 82 Prefix on page 193
- Using a Textual Description in Option 82 on page 195

## 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 suboption.

```
[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 information.

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

## Using a Textual Description in Option 82

By default, when DHCP option 82 is inserted into client packets, the Agent Circuit ID suboption includes the interface identifier. You can optionally configure that the Agent Circuit ID suboption include the textual description that is configured for the interface instead of the interface identifier. You can use the textual description for either the logical interface or the device interface.

You can include the textual interface description in the Agent Circuit ID suboption for static interfaces. The textual description is configured using the **description** statement at the **[edit interfaces *interface-name*]** hierarchy level. If you specify that the textual description is used and no description is configured for the interface, DHCP relay defaults to using the interface identifier.

To configure the DHCP relay option 82 suboption to include the textual interface description:

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 information.

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

3. Specify that the textual description is included in the option 82 information. In this example, the option 82 information includes the description used for the device interface.

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

## 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.

---

## Enabling DHCP Relay Proxy Mode

You can enable DHCP relay proxy mode on all interfaces or a group of interfaces.

To enable DHCP relay proxy mode:

1. Specify that you want to configure override options.

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

2. Enable DHCP relay proxy mode.

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

### Related Documentation

- DHCP Relay Proxy Overview on page 156
- Overriding the Default DHCP Relay Configuration Settings on page 168

## 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 197
- Attaching a Dynamic Profile to a Group of DHCP Subscriber Interfaces on page 198

### 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 **aggregate-clients** option does not apply to demux subscriber interfaces. 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 merge
```

- 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

Before you begin:

- Configure the interface group.

See “Grouping Interfaces with Common DHCP Configurations” on page 112.

To attach a dynamic profile to a group of interfaces:

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 **aggregate-clients** option does not apply to demux subscriber interfaces. 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 merge
```

- To use the primary dynamic profile:

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

### Related Documentation

- Dynamic Profiles Overview on page 369
- Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview on page 104
- Example: Configuring Dynamic Subscriber Interfaces on IP Demux Interfaces on page 453

---

## 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 Documentation

- [Junos OS 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.

You can configure DHCP trace operations at the global level or at the interface level. If you configure interface-level trace operations, you can specify tracing for a range of interfaces or an individual interface.

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

- Important events for both global and per-interface tracing are logged in a file located in the `/var/log` directory. By default, the router uses the filename, `jdhcpd`. You can specify a different filename, but you cannot change the directory in which trace files are located.
- When the file `jdhcpd` reaches 128 kilobytes (KB), it is renamed `jdhcpd.0`, then `jdhcpd.1`, and finally `jdhcpd.2`, until there are three trace files. Then the oldest trace file (`jdhcpd.2`) is overwritten.

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

- By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To specify that you want to configure global DHCP tracing operations.

- For DHCP local server:

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

- For DHCP relay:

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

For information about configuring per-interface tracing options, see “Tracing Extended DHCP Operations for Specific Interfaces” on page 144.

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

- Configuring the Extended DHCP Log Filename on page 200
- Configuring the Number and Size of Extended DHCP Log Files on page 200
- Configuring Access to the Extended DHCP Log File on page 201
- Configuring a Regular Expression for Extended DHCP Lines to Be Logged on page 201
- Configuring the Extended DHCP Tracing Flags on page 201
- Tracing Extended DHCP Operations for Specific Interfaces on page 203

## 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 filename
```

## 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 finally **filename.2**, until there are three trace files. Then the oldest trace file (**filename.2**) is overwritten.

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

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 and the **interface-traceoptions** statement.

```
[edit system services dhcp-local-server traceoptions]
user@host# set file filename files number size maximum-file-size
```

## 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 and the **interface-traceoptions** statement.

```
[edit system services dhcp-local-server traceoptions]
user@host# set file filename 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 and the **interface-traceoptions** statement.

```
[edit system services dhcp-local-server traceoptions]
user@host# set file filename 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 to be matched.

To configure regular expressions to be matched, specify 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 filename match regular-expression
```

## 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. All flags are available for global tracing operations. The Interface-Specific Tracing column indicates the subset of flags that you can use for per-interface tracing.

Flag	Description	Interface-Specific Tracing
<b>all</b>	Trace all events	No
<b>auth</b>	Trace authentication events	No
<b>database</b>	Trace database events	No
<b>dhcpv6-general</b>	Trace miscellaneous DHCPv6 events	No
<b>dhcpv6-io</b>	Trace I/O operations for DHCPv6	No

Flag	Description	Interface-Specific Tracing
<b>dhcpv6-packet</b>	Trace DHCPv6 packet decoding operations	Yes
<b>dhcpv6-packet-option</b>	Trace DHCPv6 option decoding operations	Yes
<b>dhcpv6-rpd</b>	Trace routing protocol process events for DHCPv6	No
<b>dhcpv6-session-db</b>	Trace session database operations for DHCPv6	No
<b>dhcpv6-state</b>	Trace changes in state for DHCPv6 operations	Yes
<b>fwd</b>	Trace firewall process events	No
<b>general</b>	Trace miscellaneous events	No
<b>ha</b>	Trace high availability-related events	No
<b>interface</b>	Trace interface operations	No
<b>io</b>	Trace I/O operations	No
<b>packet</b>	Trace packet decoding operations	Yes
<b>packet-option</b>	Trace DHCP option decoding operations	Yes
<b>performance</b>	Trace performance measurement operations	No
<b>profile</b>	Trace profile operations	No
<b>rpd</b>	Trace routing protocol process events	No
<b>rtsock</b>	Trace routing socket operations	No
<b>session-db</b>	Trace session database events	No
<b>state</b>	Trace changes in state	Yes
<b>statistics</b>	Trace baseline statistics	No
<b>ui</b>	Trace user interface operations	No



To configure the flags for the events to be logged, specify the flags. DHCP local server and DHCP relay agent both support the **flag** option for the **traceoptions** statement and the **interface-traceoptions** statement.

- For global tracing operations

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

- For per-interface tracing operations

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

For additional information on configuring per-interface tracing options, see “Tracing Extended DHCP Operations for Specific Interfaces” on page 144.

## Tracing Extended DHCP Operations for Specific Interfaces

In addition to the global DHCP tracing operations, subscriber management enables you to trace extended DHCP operations for a specific interface or for a range of interfaces.

Configuring per-interface tracing is a two-step procedure. In the first step, you specify the tracing options that you want to use, such as file information and flags. In the second step, you enable the tracing operation on the specific interfaces.

To configure per-interface tracing operations:

1. Specify the tracing options you want to use.



**NOTE:** Per-interface tracing uses the same default tracing behavior as the global extended DHCP tracing operation. The default behavior is described in “Tracing Extended DHCP Operations” on page 139.

- a. Specify that you want to configure per-interface tracing options.

- For DHCP local server and DHCPv6 local server:

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

- For DHCP relay agent:

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

- b. (Optional) Specify the tracing file options.

- Configure the name for the file used for the trace output.

See “Configuring the Extended DHCP Log Filename” on page 140.

- Configure the number and size of the log files.

See “Configuring the Number and Size of Extended DHCP Log Files” on page 141.

- Configure access to the log file.

See “Configuring Access to the Extended DHCP Log File” on page 141.

- Configure a regular expression to filter logging events.

See “Configuring a Regular Expression for Extended DHCP Lines to Be Logged” on page 142.

- c. (Optional) Specify tracing flag options.

See “Configuring the Extended DHCP Tracing Flags” on page 142.

2. Enable tracing on an interface or interface range.

The following examples show a DHCP local server configuration. You can also use the **trace** statement at the **[edit forwarding-options dhcp-relay]** hierarchy level and at the **[edit system services dhcp-local-server dhcpv6]** hierarchy level.

- Enable tracing on a specific interface.

```
[edit system services dhcp-local-server]
user@host# set group group-name interface interface-name trace
```

- Enable tracing on a range of interfaces.

```
[edit system services dhcp-local-server]
user@host# set group group-name interface interface-name upto interface
interface-name trace
```

## CHAPTER 11

# Configuring Dynamic Access and Access-Internal Routes for DHCP Subscriber Management

- Access and Access-Internal Routes for Subscriber Management on page 205
- Configuring Dynamic Access Routes for Subscriber Management on page 206
- Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management on page 207
- Verifying the Configuration of Access and Access-Internal Routes for Subscriber Management on page 208

## Access and Access-Internal Routes for Subscriber Management

---

The DHCP and PPP applications 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.

You can dynamically configure IPv4 access routes using values specified in Framed-Route attribute [22]. Configuring support for access-internal variables is optional, but it ensures that if the next-hop value is missing in the Framed-Routes attribute [22], values from the access-internal variables are used instead.

You can dynamically configure IPv6 access routes using values specified in Framed-IPv6-Route attribute [99].

### Related Documentation

- Configuring Dynamic Access Routes for Subscriber Management on page 206
- Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management on page 207
- Configuring Dynamic Access-Internal Routes for PPP Subscriber Management on page 222
- RADIUS IETF Attributes Supported by the AAA Service Framework on page 39

## Configuring Dynamic Access Routes for Subscriber Management

---

You can dynamically configure access routes for DHCP and PPP subscribers based on the values specified in the following RADIUS attributes:

- For IPv4 access routes, use the variable, **\$junos-framed-route-ip-address-prefix**. The route prefix variable is dynamically replaced with the value in Framed-Route RADIUS attribute [22].
- For IPv6 access routes, use the variable, **\$junos-framed-route-ipv6-address-prefix**. The variable is dynamically replaced with the value in Framed-IPv6-Route RADIUS attribute [99].

To dynamically configure access routes:

1. Configure the route prefix for the access route as a variable.

For IPv4:

```
[edit dynamic-profiles profile-name routing-options]
user@host# edit access route $junos-framed-route-ip-address-prefix
```

For IPv6:

```
[edit dynamic-profiles profile-name routing-options]
user@host# edit access route $junos-framed-route-ipv6-address-prefix
```

2. Configure the next-hop address as a variable.

For IPv4:

```
[edit dynamic-profiles profile-name routing-options access route
"$junos-framed-route-ip-address-prefix"]
user@host# set next-hop $junos-framed-route-nexthop
```

For IPv6:

```
[edit dynamic-profiles profile-name routing-options access route
"$junos-framed-route-ipv6-address-prefix"]
user@host# set next-hop $junos-framed-route-ipv6-nexthop
```

3. Configure the metric as a variable (IPv4 only).

```
[edit dynamic-profiles profile-name routing-options access route
"$junos-framed-route-ip-address-prefix"]
user@host# set metric $junos-framed-route-cost
```

4. Configure the preference as a variable (IPv4 only).

```
[edit dynamic-profiles profile-name routing-options access route
"$junos-framed-route-ip-address-prefix"]
user@host# set preference $junos-framed-route-distance
```

5. Configure the tag as a variable (IPv4 only).

```
[edit dynamic-profiles profile-name routing-options access route
"$junos-framed-route-ip-address-prefix"]
user@host# set tag $junos-framed-route-tag
```

**Related Documentation**

- Access and Access-Internal Routes for Subscriber Management on page 205
- RADIUS IETF Attributes Supported by the AAA Service Framework on page 39
- Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management on page 207
- Configuring Dynamic Access-Internal Routes for PPP Subscriber Management on page 222
- Verifying the Configuration of Access and Access-Internal Routes for Subscriber Management on page 208

## Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management

You can dynamically configure access-internal routes. Configuring support for access-internal variables is optional, but it ensures that if the next-hop value is missing in the Framed-Routes Attribute [22], values from the access-internal variables are used instead.

DHCP subscriber interfaces require the qualified-next-hop to identify the interface and the MAC address.

To dynamically configure access-internal routes:

1. Specify that you want to configure the access-internal route.

```
user@host# edit dynamic-profiles profile-name routing-options
```

2. Configure the IP address and the qualified next-hop address as variables.

```
[edit dynamic-profiles profile-name routing-options]
```

```
user@host# edit access-internal route $junos-subscriber-ip-address qualified-next-hop $junos-interface-name
```



**NOTE:** Prior to Junos OS Release 10.0, the variable used for qualified-next-hop was `$junos-underlying-interface`. It is now `$junos-interface-name`.

3. Configure the MAC address for the qualified next-hop as a variable.

```
[edit dynamic-profiles profile-name routing-options access-internal route $junos-subscriber-ip-address qualified-next-hop $junos-underlying-interface]
user@host# set mac-address $junos-subscriber-mac-address
```

**Related Documentation**

- Access and Access-Internal Routes for Subscriber Management on page 205
- Configuring Dynamic Access Routes for Subscriber Management on page 206
- Verifying the Configuration of Access and Access-Internal Routes for Subscriber Management on page 208

## Verifying the Configuration of Access and Access-Internal Routes for Subscriber Management

---

<b>Purpose</b>	View configuration information for access routes and access-internal routes on DHCP and PPP subscribers.
<b>Action</b>	<ul style="list-style-type: none"><li>• To display extensive information about access routes and access-internal routes: user@host&gt;show route extensive</li><li>• To display the configuration for access routes: user@host&gt;show route protocol access</li><li>• To display the configuration for access-internal routes: user@host&gt; show route protocol access-internal</li></ul>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Dynamic Access Routes for Subscriber Management on page 206</li><li>• Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management on page 207</li><li>• Configuring Dynamic Access-Internal Routes for PPP Subscriber Management on page 222</li></ul>

## CHAPTER 12

# DHCP Relay Agent Examples

- Example: Minimum DHCP Relay Agent Configuration on page 209
- Example: DHCP Relay Agent Configuration with Multiple Clients and Servers on page 209
- Example: Configuring DHCP Snooping Support for DHCP Relay Agent on page 211
- Example: Using Option 60 Strings to Forward DHCP Client Traffic on page 213
- Example: Using Option 60 Strings to Drop DHCP Client Traffic on page 214

### Example: Minimum DHCP Relay Agent Configuration

---

This 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.

#### Related Documentation

- Extended DHCP Relay Agent Overview on page 154

### Example: DHCP Relay Agent Configuration with Multiple Clients and Servers

---

This example shows an extended DHCP relay agent configuration for a network that includes multiple DHCP clients and DHCP servers. Additional details follow 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.

- Related Documentation**
- Extended DHCP Relay Agent Overview on page 154

## Example: Configuring DHCP Snooping Support for DHCP Relay Agent

This example shows how to configure DHCP snooping support for DHCP relay agent.

- Requirements on page 211
- Overview on page 211
- Configuration on page 211

### Requirements

- Configure DHCP relay agent. See “Extended DHCP Relay Agent Overview” on page 154.

### Overview

In this example, you configure DHCP snooping support for DHCP relay agent by completing the following operations:

- Override the default DHCP snooping configuration and enable DHCP snooping support for the interfaces in group **frankfurt**.
- Configure DHCP relay agent to forward snooped packets to only configured interfaces.



**NOTE:** By default, DHCP snooping is enabled globally in Junos OS Release 10.0 and earlier and disabled globally in Junos OS Release 10.1 and later.

### Configuration

#### Step-by-Step Procedure

To configure DHCP relay support for DHCP snooping:

1. Specify that you want to configure DHCP relay agent.  

```
[edit]
user@host# edit forwarding-options dhcp-relay
```
2. Specify the named group of interfaces on which DHCP snooping is supported.  

```
[edit forwarding-options dhcp-relay]
user@host# edit group frankfurt
```
3. Specify the interfaces that you want to include in the group. DHCP relay agent considers these as the configured interfaces when determining whether to forward or drop traffic.  

```
[edit forwarding-options dhcp-relay group frankfurt]
user@host# set interface fe-1/0/1.3 upto fe-1/0/1.9
```

4. Specify that you want to override the default configuration for the group.  

```
[edit forwarding-options dhcp-relay group frankfurt]
user@host# edit overrides
```
5. Enable DHCP snooping support for the group.  

```
[edit forwarding-options dhcp-relay group frankfurt overrides]
user@host# set allow-snooped-clients
```
6. Return to the **[edit forwarding-options dhcp-relay]** hierarchy level to configure the forwarding action and specify that DHCP relay agent forward snooped packets on only configured interfaces:  

```
[edit forwarding-options dhcp-relay group frankfurt overrides]
user@host# up 2
```
7. Enable DHCP snooped packet forwarding for DHCP relay agent.  

```
[edit forwarding-options dhcp-relay]
user@host# edit forward-snooped-clients
```
8. Specify that snooped packets are forwarded on only configured interfaces (the interfaces in group **frankfurt**).  

```
[edit forwarding-options dhcp-relay forward-snooped-clients]
user@host# set configured-interfaces
```

**Results** From configuration mode, confirm your configuration by entering the **show forwarding-options** command. If the output does not display the intended configuration, repeat the instructions in this example to correct it. The following output also shows a range of configured interfaces in group **frankfurt**.

```
[edit]
regress@montag# show forwarding-options
dhcp-relay {
  forward-snooped-clients configured-interfaces;
  group frankfurt {
    overrides {
      allow-snooped-clients;
    }
    interface fe-1/0/1.3 {
      upto fe-1/0/1.9;
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

- Related Documentation**
- DHCP Snooping Support on page 174
  - Configuring DHCP Snooping for DHCP Relay Agent on page 175

## Example: Using Option 60 Strings to Forward DHCP Client Traffic

This example 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.

**Related  
Documentation**

- Extended DHCP Relay Agent Overview on page 154
- Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 189
- **server-group** on page 1180

---

## Example: Using Option 60 Strings to Drop DHCP Client Traffic

---

This example 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**.

**Related  
Documentation**

- Extended DHCP Relay Agent Overview on page 154
- Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 189

## PART 5

# PPP for Subscriber Access

- [Dynamic Profiles for PPP Overview on page 217](#)
- [Configuring PPP for Subscriber Access on page 219](#)
- [Configuring Subscriber Services for MLPPP Interfaces on page 225](#)



# Dynamic Profiles for PPP Overview

- Dynamic Profiles for PPP Subscriber Interfaces Overview on page 217

## Dynamic Profiles for PPP Subscriber Interfaces Overview

---

Subscriber management PPP support enables you to create and attach dynamic profiles for PPP subscriber interfaces. When the PPP subscriber logs in, the router instantiates the specified dynamic profile and then applies the attributes defined in the profile to the interface.

Dynamic profiles are used for both static and dynamic PPP interfaces. For static PPP interfaces, you use the CLI to attach dynamic profiles, which specify PPP options. For dynamic PPP interfaces, the dynamic profile creates the interface, including the PPP options.



**NOTE:** Dynamically created interfaces are supported only on PPPoE interfaces.

Unlike traditional PPP support, subscriber management does not allow bi-directional PPP authentication—authentication is performed only by the router, never by the remote peer. The router's AAA process manages authentication and address assignment for subscriber management. When you configure PPP options for a dynamic profile, you can configure either CHAP or PAP authentication, but you do not configure any additional options under either the CHAP or PAP stanza. Also, other PPP options, which are either commonly used or mandatory for a traditional PPP interface configuration, are not supported in subscriber management dynamic profiles.

### Related Documentation

- Configuring Dynamic Authentication for PPP Subscribers on page 219
- Attaching Dynamic Profiles to Static PPP Subscriber Interfaces on page 223
- Verifying and Managing PPP Configuration for Subscriber Management on page 223
- Example: Minimum PPPoE Dynamic Profile on page 403





# Configuring PPP for Subscriber Access

- Configuring Dynamic Authentication for PPP Subscribers on page 219
- Access and Access-Internal Routes for Subscriber Management on page 220
- Configuring Dynamic Access Routes for Subscriber Management on page 221
- Configuring Dynamic Access-Internal Routes for PPP Subscriber Management on page 222
- Attaching Dynamic Profiles to Static PPP Subscriber Interfaces on page 223
- Verifying and Managing PPP Configuration for Subscriber Management on page 223
- Verifying the Configuration of Access and Access-Internal Routes for Subscriber Management on page 223

## Configuring Dynamic Authentication for PPP Subscribers

---

You can configure a dynamic profile that includes PPP authentication that enables PPP clients to dynamically access the network. You can specify either CHAP or PAP authentication.

For dynamic interfaces, the router supports unidirectional authentication only—the router always functions as the authenticator. When you configure PPP authentication in a dynamic profile, the **pap** and **chap** statements do not support any additional configuration options, including the **passive** statement.



**NOTE:** Dynamic profiles for PPP subscribers are supported only on PPPoE interfaces.

To configure authentication in a dynamic profile for PPP subscriber interfaces:

1. Name the dynamic profile.

[edit]

user@host# **edit dynamic-profiles vod-profile-25**

2. Configure the interfaces and unit for the dynamic profile. Use **pp0** for the interface type and the Junos predefined variable for the unit.

[edit dynamic-profiles vod-profile-25]

user@host# **edit interfaces pp0 unit \$junos-interface-unit**

3. Configure PPP options.

```
[edit dynamic-profiles vod-profile-25 interfaces pp0 unit "$junos-interface-unit"]
user@host# edit ppp-options
```

4. Specify the authentication protocol used in the dynamic profile. You can configure either CHAP or PAP. There are no additional options for either authentication protocol.

```
[edit dynamic-profiles vod-profile-25 interfaces pp0 unit "$junos-interface-unit"
  ppp-options]
user@host# set chap
```

**Related Documentation**

- Dynamic Profiles for PPP Subscriber Interfaces Overview on page 217
- Attaching Dynamic Profiles to Static PPP Subscriber Interfaces on page 223
- Dynamic Profiles Overview on page 369
- Configuring a Basic Dynamic Profile on page 391
- Example: Minimum PPPoE Dynamic Profile on page 403
- Verifying and Managing PPP Configuration for Subscriber Management on page 223

---

## Access and Access-Internal Routes for Subscriber Management

---

The DHCP and PPP applications 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.

You can dynamically configure IPv4 access routes using values specified in Framed-Route attribute [22]. Configuring support for access-internal variables is optional, but it ensures that if the next-hop value is missing in the Framed-Routes attribute [22], values from the access-internal variables are used instead.

You can dynamically configure IPv6 access routes using values specified in Framed-IPv6-Route attribute [99].

**Related Documentation**

- Configuring Dynamic Access Routes for Subscriber Management on page 206
- Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management on page 207
- Configuring Dynamic Access-Internal Routes for PPP Subscriber Management on page 222
- RADIUS IETF Attributes Supported by the AAA Service Framework on page 39

## Configuring Dynamic Access Routes for Subscriber Management

You can dynamically configure access routes for DHCP and PPP subscribers based on the values specified in the following RADIUS attributes:

- For IPv4 access routes, use the variable, **\$junos-framed-route-ip-address-prefix**. The route prefix variable is dynamically replaced with the value in Framed-Route RADIUS attribute [22].
- For IPv6 access routes, use the variable, **\$junos-framed-route-ipv6-address-prefix**. The variable is dynamically replaced with the value in Framed-IPv6-Route RADIUS attribute [99].

To dynamically configure access routes:

1. Configure the route prefix for the access route as a variable.

For IPv4:

```
[edit dynamic-profiles profile-name routing-options]
user@host# edit access route $junos-framed-route-ip-address-prefix
```

For IPv6:

```
[edit dynamic-profiles profile-name routing-options]
user@host# edit access route $junos-framed-route-ipv6-address-prefix
```

2. Configure the next-hop address as a variable.

For IPv4:

```
[edit dynamic-profiles profile-name routing-options access route
"$junos-framed-route-ip-address-prefix"]
user@host# set next-hop $junos-framed-route-nexthop
```

For IPv6:

```
[edit dynamic-profiles profile-name routing-options access route
"$junos-framed-route-ipv6-address-prefix"]
user@host# set next-hop $junos-framed-route-ipv6-nexthop
```

3. Configure the metric as a variable (IPv4 only).

```
[edit dynamic-profiles profile-name routing-options access route
"$junos-framed-route-ip-address-prefix"]
user@host# set metric $junos-framed-route-cost
```

4. Configure the preference as a variable (IPv4 only).

```
[edit dynamic-profiles profile-name routing-options access route
"$junos-framed-route-ip-address-prefix"]
user@host# set preference $junos-framed-route-distance
```

5. Configure the tag as a variable (IPv4 only).

```
[edit dynamic-profiles profile-name routing-options access route
"$junos-framed-route-ip-address-prefix"]
user@host# set tag $junos-framed-route-tag
```

**Related Documentation**

- Access and Access-Internal Routes for Subscriber Management on page 205
- RADIUS IETF Attributes Supported by the AAA Service Framework on page 39
- Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management on page 207
- Configuring Dynamic Access-Internal Routes for PPP Subscriber Management on page 222
- Verifying the Configuration of Access and Access-Internal Routes for Subscriber Management on page 208

## Configuring Dynamic Access-Internal Routes for PPP Subscriber Management

You can dynamically configure access-internal routes for PPP subscribers. Configuring support for access-internal variables is optional, but it ensures that if the next-hop value is missing in the Framed-Routes Attribute [22], values from the access-internal variables are used instead.

For PPP subscriber interfaces, you do not need to specify the MAC address for access-internal routes.

To dynamically configure access-internal routes for PPP:

1. Specify that you want to configure the access-internal route.

```
user@host# edit dynamic-profiles profile-name routing-options
```

2. Specify the IP address as a variable.

```
[edit dynamic-profiles profile-name routing-options]  
user@host# edit access-internal route $junos-subscriber-ip-address
```

3. Specify the qualified-next-hop as a variable.

```
[edit dynamic-profiles profile-name routing-options access-internal route  
$junos-subscriber-ip-address]  
user@host# set qualified-next-hop $junos-interface-name
```

**Related Documentation**

- Access and Access-Internal Routes for Subscriber Management on page 205
- Configuring Dynamic Access Routes for Subscriber Management on page 206
- Verifying the Configuration of Access and Access-Internal Routes for Subscriber Management on page 208

## Attaching Dynamic Profiles to Static PPP Subscriber Interfaces

You can attach a dynamic profile to a static PPP subscriber interface. When a PPP subscriber logs in, the specified dynamic profile is instantiated and the services defined in the profile are applied to the interface.

To attach a dynamic profile to a static PPP subscriber interface:

1. Specify that you want to configure PPP options.

```
[edit interfaces pp0 unit 0]
user@host# edit ppp-options
```

2. Specify the dynamic profile you want to associate with the interface.

```
[edit interfaces pp0 unit 0 ppp-options]
user@host# set dynamic-profile vod-profile-50
```

### Related Documentation

- Dynamic Profiles for PPP Subscriber Interfaces Overview on page 217
- Configuring Dynamic Authentication for PPP Subscribers on page 219
- Dynamic Profiles Overview on page 369
- Configuring a Basic Dynamic Profile on page 391
- Example: Minimum PPPoE Dynamic Profile on page 403
- Verifying and Managing PPP Configuration for Subscriber Management on page 223

## Verifying and Managing PPP Configuration for Subscriber Management

**Purpose** View or clear information about PPP configuration for subscriber management.

**Action** • To display information about PPP interfaces:

```
user@host> show ppp interface
```

- To display PPP statistics information:

```
user@host> show ppp statistics
```

- To display PPP session summary information:

```
user@host> show ppp summary
```

### Related Documentation

- Dynamic Profiles for PPP Subscriber Interfaces Overview on page 217
- *Junos OS System Basics and Services Command Reference*

## Verifying the Configuration of Access and Access-Internal Routes for Subscriber Management

**Purpose** View configuration information for access routes and access-internal routes on DHCP and PPP subscribers.

- Action**
- To display extensive information about access routes and access-internal routes:

`user@host>show route extensive`

- To display the configuration for access routes:

`user@host>show route protocol access`

- To display the configuration for access-internal routes:

`user@host> show route protocol access-internal`

**Related  
Documentation**

- Configuring Dynamic Access Routes for Subscriber Management on page 206
- Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management on page 207
- Configuring Dynamic Access-Internal Routes for PPP Subscriber Management on page 222

# Configuring Subscriber Services for MLPPP Interfaces

- Dynamic PPP Subscriber Services for Static MLPPP Interfaces on page 225
- Hardware Requirements for PPP Subscriber Services on Non-Ethernet Interfaces on page 226
- Configuring PPP Subscriber Services for MLPPP Bundles on page 226
- Enabling PPP Subscriber Services for Static Non-Ethernet Interfaces on page 226
- Attaching Dynamic Profiles to MLPPP Bundles on page 227

## Dynamic PPP Subscriber Services for Static MLPPP Interfaces

---

Dynamic subscriber services are supported for MLPPP bundle interfaces, with certain interface and hardware restrictions. See “Hardware Requirements for PPP Subscriber Services on Non-Ethernet Interfaces” on page 226. Multiclass MLPPP (MCML) enables the relative prioritization of up to eight classes of traffic over an MLPPP bundle, but only on link services intelligent queuing (IQ) (LSQ) interfaces.

RADIUS previously supported only authentication for MLPPP. Address management, service deactivation, and dynamic selection of subscriber properties based on RADIUS user ID are now also supported.

RADIUS can dynamically allocate IPv4 addresses for MLPPP connections. When the first subscriber logs in, an address is allocated. The same address is allocated to all links in a bundle. Any other address provided for any of the links is ignored. The IP address is released for re-allocation when the last member link in a bundle logs out. Similar to the address allocation, the services configured for the first subscriber to log in are configured for all subsequent subscribers in the bundle.

The Acct-Multi-Session-Id [50] attribute enables RADIUS to link multiple related sessions into a single log file. RADIUS uses the session database (SDB) bundle session ID for the value of Acct-Multi-Session-Id. This bundle ID enables RADIUS to initiate a disconnect for an entire bundle. By tracking the member link sessions, RADIUS is also able to disconnect the individual member links in a bundle.

The Acct-Link-Count [51] attribute records the number of links present in a multilink session at the time the accounting record is generated.

- Related Documentation**
- Hardware Requirements for PPP Subscriber Services on Non-Ethernet Interfaces on page 226
  - Configuring PPP Subscriber Services for MLPPP Bundles on page 226

---

## Hardware Requirements for PPP Subscriber Services on Non-Ethernet Interfaces

PPP subscriber services are supported for MLPPP bundle interfaces. These services require the following hardware:

- M120 router or M320 router
- Channelized DS3/E3 Enhanced IP PIC (PB-4CHDS3-E3-IQE-BNC) to support MLPPP subscriber access
- An Adaptive Services PIC or Multiservices PIC to support subscriber services on LSQ MLPPP bundle interfaces

Subscriber services are not supported for single-link PPP interfaces with this hardware.

---

## Configuring PPP Subscriber Services for MLPPP Bundles

You can configure PPP subscriber services for static LSQ MLPPP bundle interfaces.

To configure PPP subscriber services for static LSQ MLPPP bundle interfaces:

1. Enable PPP subscriber services for the interfaces.  
See “Enabling PPP Subscriber Services for Static Non-Ethernet Interfaces” on page 226.
2. Attach a dynamic profile to the MLPPP bundle interface.  
See “Attaching Dynamic Profiles to MLPPP Bundles” on page 227.

- Related Documentation**
- Hardware Requirements for PPP Subscriber Services on Non-Ethernet Interfaces on page 226
  - Example: Minimum MLPPP Dynamic Profile on page 402
  - Example: Configuring CoS on Static LSQ MLPPP Bundle Interfaces on page 467

---

## Enabling PPP Subscriber Services for Static Non-Ethernet Interfaces

You can enable PPP subscriber services for certain non-Ethernet interface types on particular associated PICs. Supported interfaces are listed in “Hardware Requirements for PPP Subscriber Services on Non-Ethernet Interfaces” on page 226.

To enable PPP subscriber services on supported non-Ethernet interfaces:

- Configure PPP subscriber services.  

```
[edit chassis]  
user@host# set ppp-subscriber-services enable
```



To disable PPP subscriber services on supported non-Ethernet interfaces:

- Disable PPP subscriber services.

```
[edit chassis]
user@host# set ppp-subscriber-services disable
```

- Related Documentation**
- For hardware requirements, see Hardware Requirements for PPP Subscriber Services on Non-Ethernet Interfaces on page 226
  - Configuring PPP Subscriber Services for MLPPP Bundles on page 226

## Attaching Dynamic Profiles to MLPPP Bundles

You can attach a dynamic profile to a static MLPPP bundle interface. When a PPP subscriber logs in on a member link, the specified dynamic profile is instantiated and the services defined in the profile are applied to the LSQ bundle interface.

To attach a dynamic profile to a static LSQ MLPPP bundle interface:

1. Specify that you want to configure PPP options.

```
[edit interfaces lsq-3/3/0 unit 0]
user@host# edit ppp-options
```

2. Specify the dynamic profile you want to associate with the interface.

```
[edit interfaces lsq-3/3/0 unit 0 ppp-options]
user@host# set dynamic-profile vod-profile-50
```

- Related Documentation**
- Hardware Requirements for PPP Subscriber Services on Non-Ethernet Interfaces on page 226
  - Configuring PPP Subscriber Services for MLPPP Bundles on page 226
  - Dynamic Profiles for PPP Subscriber Interfaces Overview on page 217
  - Dynamic Profiles Overview on page 369
  - Configuring a Basic Dynamic Profile on page 391
  - Configuring PPP Subscriber Services for MLPPP Bundles on page 226
  - Example: Minimum MLPPP Dynamic Profile on page 402
  - Example: Configuring CoS on Static LSQ MLPPP Bundle Interfaces on page 467



## PART 6

# L2TP for Subscriber Access

- L2TP for Subscriber Access Overview on page 231
- Configuring L2TP for Subscriber Access on page 241



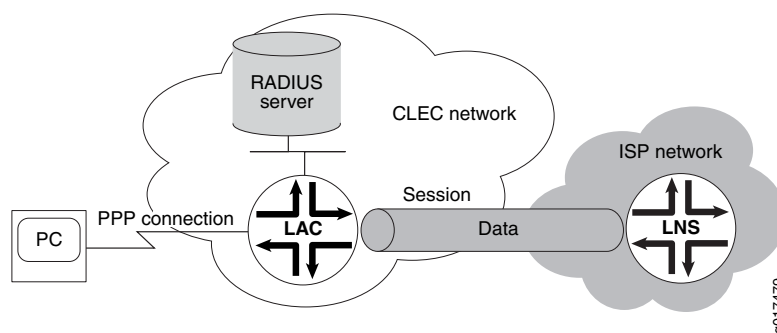
# L2TP for Subscriber Access Overview

- L2TP for Subscriber Access Overview on page 231
- L2TP Terminology on page 233
- L2TP Implementation on page 233
- LAC Tunnel Selection Overview on page 235
- L2TP Failover and Peer Resynchronization on page 238
- L2TP LAC and Graceful Routing Engine Switchover on page 239

## L2TP for Subscriber Access Overview

The Layer 2 Tunneling Protocol (L2TP) is a client-server protocol that allows the Point-to-Point Protocol (PPP) to be tunneled across a network. L2TP encapsulates Layer 2 packets, such as PPP, for transmission across a network. An L2TP access concentrator (LAC), configured on an access device, receives packets from a remote client and forwards them to an L2TP network server (LNS) on a remote network. Figure 4 on page 231 shows a simple L2TP topology.

**Figure 4: Simple L2TP Topology**

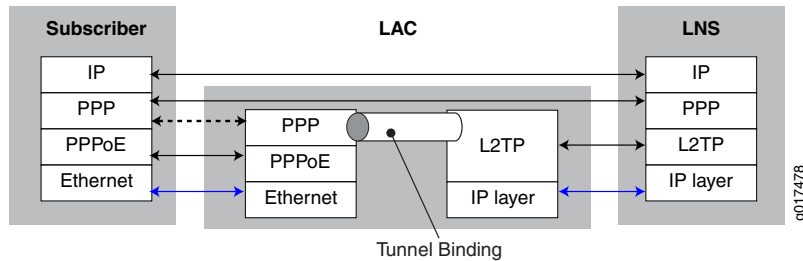


L2TP separates the termination of access technologies, such as cable or xDSL, from the termination of PPP and subsequent access to a network. This separation enables public ISPs to outsource their access technologies to competitive local exchange carriers (CLECs). L2TP provides ISPs the capability to supply VPN service; private enterprises can reduce or avoid investment in access technologies for remote workers.

You can configure your router to act as an LAC in PPP pass-through mode in which the LAC receives packets from a remote client and then forwards them at Layer 2 directly to

the LNS. The PPP session is terminated on the LNS. This LAC implementation supports only Point-to-Point Protocol over Ethernet (PPPoE) subscribers over dynamic or static logical interfaces. Figure 5 on page 232 shows the protocol layer stacking for an L2TP pass-through connection.

**Figure 5: Protocol Stacking for L2TP Subscribers in Pass-Through Mode**



**NOTE:** On MX Series routers, only the LAC function is supported in this release. The LNS function is supported on certain M Series routers. For more information about the L2TP implementation on M Series routers, see the [Junos OS Services Interfaces Configuration Guide](#).

The router creates tunnels dynamically based on AAA authentication parameters and transmits L2TP packets to the LNS by means of the IP/User Datagram Protocol (UDP). Traffic travels in an L2TP *session*; a tunnel is an aggregation of one or more sessions. You can also provision a domain map that is used by AAA to determine whether to tunnel or terminate the PPPoE subscriber.

The characteristics of the tunnel can originate either from a tunnel profile that you configure or from RADIUS tunnel attributes and vendor-specific attributes (VSAs). You can include a tunnel profile in a domain map, which applies the tunnel profile before RADIUS authentication takes place. You can use RADIUS standard attributes and VSAs to override any or all characteristics configured by the tunnel profile in a domain map. Alternatively, RADIUS can itself apply a tunnel profile when the RADIUS Tunnel-Group VSA [26-64] is specified in the RADIUS login.

The LAC supports RADIUS-initiated mirroring, which creates secure policies based on certain RADIUS VSAs, and uses RADIUS attributes to identify a subscriber whose traffic is to be mirrored.

#### Related Documentation

- RADIUS IETF Attributes Supported by the AAA Service Framework on page 39
- Juniper Networks VSAs Supported by the AAA Service Framework on page 45
- Configuring a Tunnel Profile for Subscriber Access on page 242
- Domain Mapping Overview on page 80
- Subscriber Secure Policy and L2TP LAC Subscribers on page 627

## L2TP Terminology

Table 30 on page 233 describes the basic terms for L2TP.

**Table 30: L2TP Terms**

Term	Description
AVP	Attribute value pair (AVP)—Combination of a unique attribute—represented by an integer—and a value containing the actual value identified by the attribute.
Call	A connection (or attempted connection) between a remote system and the LAC.
LAC	L2TP access concentrator (LAC)—A node that acts as one side of an L2TP tunnel endpoint and is a peer to the LNS. The LAC sits between an LNS and a remote system and forwards packets to and from each.
LNS	L2TP network server (LNS)—A node that acts as one side of an L2TP tunnel endpoint and is a peer to the LAC. The LNS is the logical termination point of a PPP connection that is being tunneled from the remote system by the LAC.
Peer	In the L2TP context, refers to either the LAC or LNS. The LAC's peer is an LNS, and vice versa.
Proxy authentication	Authentication data from the PPP client that is sent from the LNS as part of a proxy LCP. Data might include attributes such as authentication type, authentication name, and authentication challenge.
Proxy LCP	Link Control Protocol (LCP)—Negotiation that is performed by the LAC on behalf of the LNS. The proxy is sent by the LAC to the LNS containing attributes such as the last configuration attributes sent and received from the client.
Remote system	An end system or router attached to a remote access network, which is either the initiator or recipient of a call.
Session	A logical connection created between the LAC and the LNS when an end-to-end PPP connection is established between a remote system and the LNS.  <b>NOTE:</b> There is a one-to-one relationship between established L2TP sessions and their associated PPP connections.
Tunnel	A connection between an LAC-LNS pair consisting of a control connection and 0 or more L2TP sessions.

## L2TP Implementation

L2TP is implemented on four levels:

- Source—The local router acting as an LAC
- Destination—The remote router acting as an LNS

- Tunnel—A direct path between the LAC and the LNS
- Session—A PPP connection in a tunnel.

When the router has established destinations, tunnels, and sessions, you can control the L2TP traffic. Making a change to a destination affects all tunnels and sessions to that destination; making a change to a tunnel affects all sessions in that tunnel. For example, closing a destination closes all tunnels and sessions to that destination.

## Sequence of Events on the LAC

The router acting as the LAC creates destinations, tunnels, and sessions dynamically, as follows:

1. The client initiates a PPP connection with the router.
2. The router and the client exchange Link Control Protocol (LCP) packets. The LAC negotiates on behalf of the LNS; this is known as proxy LCP.
3. The LAC authenticates the client on behalf of the LNS; this is known as proxy authentication. By using either a local database related to the domain name or RADIUS authentication, the router determines either to terminate or to tunnel the PPP connection.
4. If the router discovers that it should tunnel the session, it does the following:
  - a. Sets up a new destination or selects an existing destination.
  - b. Sets up a new tunnel or selects an existing tunnel.

When a shared secret is configured in either the tunnel profile or the RADIUS attribute Tunnel-Password [69]—depending on which method is used to configure the tunnel—the secret is used to authenticate the tunnel during the establishment phase. The LAC includes the Challenge AVP in the SCCRP message sent to the LNS. The LNS returns the Challenge Response AVP in the SCCRP message. If the response from the LNS does not match the value expected by the LAC, then tunnel authentication fails and the tunnel is not established.

- c. Opens a new session.
5. The router forwards the results of the LCP negotiations and authentication to the LNS.

A PPP connection now exists between the client and the LNS.



**NOTE:** The router discards received packets if the size of the variable-length, optional offset pad field in the L2TP header is too large. The router always supports packets that have an offset pad field of up to 16 bytes, and may support larger offset pad fields, depending on other information in the header. This restriction is a possible, although unlikely, cause of excessive discarding of L2TP packets.

---



## Sequence of Events on the LNS



**NOTE:** The MX Series router does not support LNS in the current release.

A typical router acting as an LNS might be set up as follows:

1. An LAC initiates a tunnel with the router.
2. The router verifies that a tunnel with this LAC is valid: destination configured, hostname and tunnel password correct.
3. The router completes the tunnel setup with the LAC.
4. The LAC sets up a session with the router.
5. The router creates a dynamic PPP interface on top of the session.
6. If they are enabled and present, the router takes the proxy LCP and the proxy authentication data and passes them to PPP.
7. PPP processes the proxy LCP, if it is present, and, if acceptable, places LCP on the router in opened state without renegotiation of LCP.



**NOTE:** If the proxy LCP is not present or not acceptable, the router negotiates LCP with the peer.

8. PPP processes the proxy authentication data, if present, and passes the data to AAA for verification. (If the data is not present, PPP requests the data from the peer.)
9. The router passes the authentication results to the peer.

## LAC Tunnel Selection Overview

L2TP enables you to specify:

- Up to 31 destinations for a domain.
- Up to eight levels of preference. Preference indicates the order in which the router attempts to connect to the destinations specified for a domain. Zero (0) is the highest level of preference.
- Up to 31 destinations for a single preference level.

When the LAC determines that a PPP session should be tunneled, it selects a tunnel from a set of tunnels associated with either the PPP user or the PPP user's domain. The router provides the following methods for selecting tunnels:

- Tunnel selection failover between preference levels (the default behavior)
- Tunnel selection failover within a preference level

- Maximum sessions per tunnel
- Weighted load balancing

## Tunnel Selection Failover Between Preference Levels

When a user tries to log in to a domain, in the default method, the router attempts to connect to a destination in that domain by means of the associated tunnel with the highest preference level. If more than one destination is considered reachable by a tunnel in the preference level, the router randomly selects a destination and attempts to contact it through its associated tunnel at that level. If the router is unsuccessful, it marks the destination as unreachable and does not try to connect to that destination for five minutes. The router then moves to the next lower preference level and repeats the process.

For example, suppose that there are three destinations for a domain and a tunnel has been defined for each destination: A, B, and C. All destinations are considered reachable, and the preference levels for the tunnels are assigned as follows:

- A at preference 0
- B at preference 1
- C at preference 2

When a PPP user tries to connect to the domain, the router initially attempts to reach a destination by a tunnel at preference level 0. In this example, that is destination A. If this connection attempt fails, the router excludes destination A for five minutes and goes to the next level (preference 1) to reach a destination for the domain. At level 1, it attempts to connect to destination B. If the second connection attempt also fails, the router excludes destination B in addition to the already excluded destination A. The router goes to the next level (preference 2), and attempts to connect to destination C, the only destination in the domain that is still available. If that attempt also fails, the router has attempted to connect to every tunnel available for the domain. When the exclusion period for destination A expires, the router can attempt again to connect to destination A, and so on.

Although the five-minute timer typically prevents an unreachable destination from being tried until the timer expires, the timer is ignored in some circumstances. For example, If all destinations at a preference level are marked as unreachable when a user tries to log in to a domain, the router chooses and attempts to connect to the destination that failed first and therefore has the shortest time remaining until the timer expires. The key is to understand that the router always chooses a single destination at each level of preference, even if all destinations have recently failed.

If more than one destination for the domain is present at a preference level, the router randomly selects among them. If the router fails to connect to a destination at all preference levels with destinations for the domain, it cycles back to the highest level that still has a destination not excluded by an attempt.

For example, suppose that again there are three destinations for a domain and a tunnel has been defined for each destination: A, B, and C. All destinations are considered reachable, but the tunnels are distributed among the preference levels as follows:

- A and B at preference 0
- C at preference 1

If a PPP user tries to connect to the domain, the router randomly selects between A and B at level 0. Suppose it selects B, but the connection attempt fails. The router excludes destination B for five minutes and goes to the next level (preference 1) to reach a destination for the domain. At level 1, it attempts to connect to destination C. If the second connection attempt also fails, the router excludes destination C in addition to the already excluded destination B. The router cycles back to preference level 0. If destination B is still excluded, it attempts to connect to destination A. If the exclusion period for destination B has expired, then the router once again randomly selects between A and B to attempt a connection.

### Tunnel Selection Failover Within a Preference Level

When tunnel selection failover within a preference level is configured, if the router tries to connect to a destination and is unsuccessful, it selects a new destination at the same preference level. If all destinations at a preference level are marked as unreachable, the router does not attempt to connect to a destination at that level. It drops to the next lower preference level to select a destination.

If all destinations at all preference levels are marked as unreachable, the router chooses the destination that failed first and tries to make a connection. If the connection fails, the router rejects the PPP user session without attempting to contact the remote router.

For example, suppose that there are four destinations for a domain and a tunnel has been defined for each destination: A, B, C, and D. All destinations are considered reachable, and the preference levels for the tunnels are assigned as follows:

- A and B at preference 0
- C and D at preference 1

When the router attempts to connect to the domain, suppose it randomly selects tunnel B from preference 0. If it fails to connect to the destination, the router excludes tunnel B for five minutes and attempts to connect to a destination with tunnel A. If this attempt also fails, the router drops to preference level 1. Then suppose the router randomly selects tunnel C. If it also fails to connect to a destination with tunnel C, the router excludes tunnel C for five minutes and attempts to connect with tunnel D. If this connection attempt fails, then the router attempts to use tunnel B again, the original selection. If that attempt fails, the user session is rejected.

### Tunnel Selection and Maximum Sessions per Tunnel

When the maximum number of sessions allowed per tunnel is configured, the router takes that setting into consideration during the tunnel selection process. The maximum number of sessions per tunnel can be configured through a RADIUS Tunnel-Max-Sessions VSA [26-64] or by including the **max-sessions** statement in a tunnel profile.

If a randomly selected tunnel has a current session count equal to its maximum session count, the router does not attempt to connect to a destination with that tunnel. Instead, it selects an alternate tunnel from the set of reachable tunnels at the same preference level. If no additional reachable tunnels exist at the current preference level, the router drops to the next lower preference level to make the selection. This process is consistent, regardless of which fail-over scheme is currently running on the router.

If the maximum number of sessions is not configured for a tunnel, then that tunnel has no upper limit on the number of sessions it can support. By default, the maximum sessions value is 0 (zero), which allows unlimited sessions in the tunnel.

## Tunnel Selection with Weighted Load Balancing

The maximum sessions value for a tunnel is used for weighted load balancing to select among multiple tunnels with the same preference level.

The weight of a tunnel is determined by the tunnel's maximum session limit and the maximum session limits of the other tunnels at the same preference level. The tunnel with the largest maximum session value has the largest weight. The tunnel with the next largest maximum session value has the next largest weight, and so on. The tunnel with the smallest maximum session value has the smallest weight.

### Related Documentation

- [Configuring the L2TP LAC Tunnel Selection Parameters on page 244](#)

---

## L2TP Failover and Peer Resynchronization

L2TP failover enables a failed L2TP endpoint to resynchronize with its nonfailed peer during recovery and restart of the L2TP protocol on the failed endpoint. L2TP failover is enabled by default.

The failover and L2TP peer resynchronization process does all of the following:

- Prevents the nonfailed endpoint from prematurely terminating a tunnel while the failed endpoint is recovering.
- Reestablishes the sequence numbers required for the operation of the L2TP control protocol.
- Resolves inconsistencies in the tunnel and session databases of the failed endpoint and the nonfailed endpoint.

The router supports both the L2TP failover protocol method (described in *RFC 4951, Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP) "failover"*) and the L2TP silent failover method. The differences between these two methods are as follows:

- With the L2TP failover protocol method, both endpoints must support the method or recovery always fails. The L2TP failover protocol method also requires a nonfailed endpoint to wait an additional recovery time period while the failed endpoint is recovering to prevent the nonfailed endpoint from prematurely disconnecting the tunnel. The additional recovery period delays the detection of tunnel keepalive failures.

- Silent failover operates entirely within the failed endpoint and does not require nonfailed endpoint support—this improves interoperability between peers. Silent failover does not require additional recovery time by the nonfailed endpoint, which also eliminates the potential for degraded responsiveness to the loss of tunnel connectivity.

The default resynchronization method in Junos OS is *failover-protocol-fall-back-to-silent-failover*. The recovery method used depends on the results of the failover capability negotiation that takes place between L2TP peers when they establish a tunnel, which works as follows:

- L2TP on the LAC by default attempts to negotiate the L2TP failover protocol first. When L2TP determines that the remote peer supports the L2TP failover protocol, then the L2TP failover protocol method is used.
- When L2TP determines that the remote peer does not support the L2TP failover protocol, then the L2TP silent failover method is used. Falling back on this secondary method prevents the failover from forcing a disconnection of the tunnel to the peer and all its sessions.

You can change the default behavior by including the **disable-failover-protocol** statement at the **[edit services l2tp]** hierarchy level. This statement forces the LAC to operate only in silent failover mode. This configuration can be useful when routers that act as the LNS either are configured for silent failover or incorrectly negotiate use of the failover protocol even though they do not support it. However, when you issue this statement and the LNS supports only failover protocol, then the LAC cannot negotiate failover protocol, and recovery (failover protocol recovery initiated by the LNS) always fails.

#### Related Documentation

- L2TP LAC and Graceful Routing Engine Switchover on page 239
- L2TP for Subscriber Access Overview on page 231

## L2TP LAC and Graceful Routing Engine Switchover

Graceful Routing Engine Switchover (GRES) is supported on routers acting as the L2TP LAC. In the event that L2TP (the `l2tp-universal-edge` process) restarts or that the router fails over from the active routing engine (RE) to the standby RE, L2TP graceful Routing Engine switchover ensures that the LAC does the following:

- Recovers destinations, tunnels, and sessions that were already established at the time of the restart of failover.
- Sends L2TP keepalives for established tunnels to the LNS.
- Deletes all the tunnels and sessions that are not in Established state.
- Rejects tunnel subscriber requests that had been initiated but not established at the time of recovery.

- Deletes existing sessions and tunnels that were disconnected during the restart or switchover without notifying the LNS. This occurs when the LAC does not have enough information at warm start to connect to the LNS for the session or tunnel.
- Restarts timers for the full timeout period for recovered L2TP destinations, tunnels, and sessions.



**NOTE:** Graceful Routing Engine switchover is supported only by L2TP LAC on MX Series routers. It is not supported by L2TP LNS on M Series routers.

---

**Related  
Documentation**

- L2TP Failover and Peer Resynchronization on page 238
- L2TP for Subscriber Access Overview on page 231

## Configuring L2TP for Subscriber Access

- Configuring an L2TP LAC on page 241
- Configuring a Tunnel Profile for Subscriber Access on page 242
- Configuring the L2TP LAC Tunnel Selection Parameters on page 244
- Configuring LAC Tunnel Selection Failover Within a Preference Level on page 244
- Configuring Weighted Load Balancing for LAC Tunnel Sessions on page 245
- Preventing the LAC from Sending Calling Number AVP 22 to the LNS on page 246
- Preventing the LAC From Negotiating L2TP Failover Protocol on page 246
- Tracing L2TP Operations for Subscriber Access on page 247
- Configuring the L2TP Trace Log Filename on page 247
- Configuring the Number and Size of L2TP Log Files on page 248
- Configuring Access to the L2TP Log File on page 248
- Configuring a Regular Expression for L2TP LAC to Be Logged on page 249
- Configuring the L2TP Tracing Flags on page 249
- Verifying and Managing L2TP for Subscriber Access on page 250

### Configuring an L2TP LAC

---

To configure an L2TP LAC:

1. Configure a tunnel profile to apply to subscribers.  
See “Configuring a Tunnel Profile for Subscriber Access” on page 242.
2. (Optional) Configure the method used for selecting among multiple tunnels.
  - See “Configuring the L2TP LAC Tunnel Selection Parameters” on page 244.
  - See “Configuring Weighted Load Balancing for LAC Tunnel Sessions” on page 245.
  - See “Configuring LAC Tunnel Selection Failover Within a Preference Level” on page 244.
3. (Optional) Configure the LAC to not send Calling Number AVP 22 to the LNS.  
See “Preventing the LAC from Sending Calling Number AVP 22 to the LNS” on page 246.
4. (Optional) Configure trace options for troubleshooting the configuration.

See “Tracing L2TP Operations for Subscriber Access” on page 247

5. (Optional) Disable negotiation of the L2TP failover protocol to force use of only the silent failover resynchronization mechanism.

See “Preventing the LAC From Negotiating L2TP Failover Protocol” on page 246

---

## Configuring a Tunnel Profile for Subscriber Access

---

The tunnel profile specifies a set of attributes to characterize the tunnel. The profile can be applied by a domain map or automatically when the tunnel is created.



**NOTE:** RADIUS attributes and VSAs can override the values you configure in a domain map. In the absence of a domain map, RADIUS can supply all the characteristics of a tunnel. The steps in the following procedure list the corresponding standard RADIUS attribute or VSA that you can configure on your RADIUS server to modify or configure the tunnel profile.

To configure a tunnel definition for a tunnel profile:

1. Specify the tunnel profile for which you are defining a tunnel. (Tunnel-Group [26-64])

```
[edit access]
user@host# set tunnel-profile profile-name
```

2. Specify an identification number for the L2TP control connection for the tunnel.

```
[edit access tunnel-profile profile-name]
user@host# set tunnel tunnel-id
```

3. Configure the IP address of the local L2TP tunnel endpoint, the LAC. (Tunnel-Client-Endpoint [66])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set source-gateway address client-ip-address
```

4. Configure the IP address of the remote L2TP tunnel endpoint, the LNS. (Tunnel-Server-Endpoint [67])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set remote-gateway address server-ip-address
```

5. (Optional) Configure the preference level for the tunnel. (Tunnel-Preference [83])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set preference number
```

6. (Optional) Configure the hostname of the local client (LAC). (Tunnel-Client-Auth-Id [90])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set source-gateway gateway-name client-name
```

7. (Optional) Configure the hostname of the remote server (LNS). (Tunnel-Server-Auth-Id [91])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
```



```
user@host# set remote-gateway gateway-name server-name
```

8. (Optional) Specify the medium (network) type for the tunnel. (Tunnel-Medium-Type [65])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set medium type
```

9. (Optional) Specify the protocol type for the tunnel. (Tunnel-Type [64])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set type tunnel-type
```

10. (Optional) Configure the assignment ID for the tunnel. (Tunnel-Assignment-Id [82])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set identification name
```

11. (Optional) Configure the maximum number of sessions allowed in the tunnel. (Tunnel-Max-Sessions [26-33])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set max-sessions number
```

12. (Optional) Configure the password for remote server authentication. (Standard RADIUS attribute Tunnel-Password [69] or VSA Tunnel-Password [26-9])

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set secret password
```

13. (Optional) Configure the logical system to use for the tunnel.

If you configure a logical system, you must also configure a routing instance.

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set logical-system logical-system-name
```

14. (Optional) Configure the routing instance to use for the tunnel. (Tunnel-Virtual-Router [26-8])

If you configure a routing instance, configuring a logical system is optional.

```
[edit access tunnel-profile profile-name tunnel tunnel-id]
user@host# set routing-instance routing-instance-name
```

The following example shows a complete configuration for a tunnel profile:

```
tunnel-profile marketing {
  tunnel 1 {
    preference 5;
    remote-gateway {
      address 172.16.98.4;
      gateway-name work;
    }
    source-gateway {
      address 192.168.4.10;
      gateway-name local;
    }
    secret mk5Sn$3k%V;
    logical-system bos-metro-5;
    routing-instance rox-12-32;
  }
}
```

```
        medium ipv4;  
        type l2tp;  
        identification tunnel_to_work;  
        max-sessions 32;  
    }  
}
```

**Related Documentation**

- Domain Mapping Overview on page 80

---

## Configuring the L2TP LAC Tunnel Selection Parameters

When the LAC determines that a PPP session should be tunneled, it selects a tunnel from the set of tunnels associated with either the PPP user or the PPP user's domain. You can configure how a tunnel is selected and whether certain information is sent by the LAC to the LNS.

To configure tunnel selection parameters:

1. (Optional) Configure how a tunnel is selected when a connection attempt fails.  
See "Configuring LAC Tunnel Selection Failover Within a Preference Level" on page 244.
2. (Optional) Configure how sessions are load-balanced among tunnels.  
See "Configuring Weighted Load Balancing for LAC Tunnel Sessions" on page 245.

**Related Documentation**

- LAC Tunnel Selection Overview on page 235

---

## Configuring LAC Tunnel Selection Failover Within a Preference Level

You can configure how LAC tunnel selection continues in the event of a failure to connect. By default, when the router is unable to connect to a destination at a given preference level, it attempts to connect at the next lower level. You can specify that the router instead attempt to connect to another destination at the same level as the failed attempt.

If all destinations at a preference level are marked as unreachable, the router does not attempt to connect to a destination at that level. It drops to the next lower preference level to select a destination.

If all destinations at all preference levels are marked as unreachable, the router chooses the destination that failed first and tries to make a connection. If the connection fails, the router rejects the PPP user session without attempting to contact the remote router.

For example, suppose there are four tunnels for a domain: A, B, C, and D. All tunnels are considered reachable, and the preference levels are assigned as follows:

- A and B at preference 0
- C and D at preference 1

When the router attempts to connect to the domain, suppose it randomly selects tunnel B from preference 0. If it fails to connect to tunnel B, the router excludes tunnel B for five

minutes and attempts to connect to tunnel A. If this attempt also fails, the router drops to preference 1. Then suppose the router selects tunnel C. If it also fails to connect to tunnel C, the router excludes tunnel C for five minutes and attempts to connect to tunnel D.

You configure the preference level used for this tunnel selection method in the tunnel profile or the RADIUS Tunnel-Preference [83] attribute.

To enable tunnel selection failover within a preference level:

- Specify failover within preference.

```
[edit services l2tp]  
user@host# set fail-over-within-preference
```

**Related  
Documentation**

- LAC Tunnel Selection Overview on page 235
- Configuring the L2TP LAC Tunnel Selection Parameters on page 244
- Configuring a Tunnel Profile for Subscriber Access on page 242
- Configuring How RADIUS Attributes Are Used for Subscriber Access on page 31

---

## Configuring Weighted Load Balancing for LAC Tunnel Sessions

You can configure how L2TP LAC sessions are distributed across tunnels. You can specify that the router uses the maximum sessions per tunnel to choose among multiple tunnels that share the same preference level.

The weight of a tunnel is proportional to its maximum session limit and the maximum session limits of the other tunnels at the same preference level. The tunnel with the largest maximum session value has the highest weight. The tunnel with the next larger maximum session value has the next higher weight, and so on. The tunnel with the smallest maximum session value has the lowest weight.

When you configure weighted load balancing, the tunnel with the highest weight in the preference level is selected until the maximum number of sessions for the tunnel is reached. Then the router selects the tunnel with the next higher weight to establish connections until that tunnel's maximum session limit is reached, and so on.

To configure weighted load balancing:

- Specify load balancing.

```
[edit services l2tp]  
user@host# set weighted-load-balancing
```

**Related  
Documentation**

- LAC Tunnel Selection Overview on page 235
- Configuring the L2TP LAC Tunnel Selection Parameters on page 244

## Preventing the LAC from Sending Calling Number AVP 22 to the LNS

---

Calling Number AVP 22 typically identifies the interface that is connected to the customer in the access network. When RADIUS includes the Calling-Station-Id in the Access-Accept message, that value is used for the Calling Number AVP. Otherwise, the underlying interface (for example, the S-VLAN IFL) on which the PPPoE session is established is used for the Calling Number AVP value.

By default, the LAC includes this AVP in the incoming-call request (ICRQ) packets that it sends to the LNS. However, you may wish to hide your network access interface information. To do so, you can configure the tunnel so that the LAC does not send the Calling Number AVP to the LNS.

To disable sending the Calling Number AVP:

- Configure disabling.

```
[edit services l2tp]  
user@host# set disable-calling-number-avp
```

**Related Documentation**

- LAC Tunnel Selection Overview on page 235

## Preventing the LAC From Negotiating L2TP Failover Protocol

---

The L2TP LAC implementation on MX Series routers supports L2TP failover and peer resynchronization with a failed remote endpoint. The LAC supports both the L2TP failover protocol method and the L2TP silent failover method. By default, L2TP on the LAC attempts to negotiate the L2TP failover protocol with the LNS. When negotiation determines that the LNS supports this method, then the LAC uses L2TP failover protocol if the LNS fails. When the LNS does not support L2TP failover protocol, then the LAC uses silent failover in the event of an LNS failure. The ability to fall back on silent failover prevents the failover from forcing a disconnection of the tunnel to the peer and all the associated sessions.

You can disable the default behavior to force the LAC to operate only in silent failover mode. This configuration can be useful when routers that act as the LNS either are configured for silent failover or incorrectly negotiate use of the failover protocol even though they do not support it. However, when you issue this statement and the LNS supports only failover protocol, then the LAC cannot negotiate failover protocol, and recovery (failover protocol recovery initiated by the LNS) always fails.

To disable negotiation of the L2TP failover protocol:

- Configure disabling.

```
[edit services l2tp]  
user@host# set disable-failover-protocol
```

**Related Documentation**

- Configuring an L2TP LAC on page 241

## Tracing L2TP Operations for Subscriber Access

---

The Junos OS trace feature tracks L2TP operations and records events 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 **jl2tpd** located in the **/var/log** directory. You cannot change the directory (**/var/log**) in which trace files are located.
2. When the file **jl2tpd** reaches 128 kilobytes (KB), it is renamed **jl2tpd.0**, then **jl2tpd.1**, and finally **jl2tpd.2**, until there are three trace files. Then the oldest trace file (**jl2tpd.2**) is overwritten.

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

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To configure L2TP tracing operations:

1. (Optional) Configure a trace log filename.  
See “Configuring the L2TP Trace Log Filename” on page 247.
2. (Optional) Configure the number and size of trace logs.  
See “Configuring the Number and Size of L2TP Log Files” on page 248.
3. (Optional) Configure user access to trace logs.  
See “Configuring Access to the L2TP Log File” on page 248.
4. (Optional) Configure a regular expression to filter the information to be included in the trace log.  
See “Configuring a Regular Expression for L2TP LAC to Be Logged” on page 249.
5. (Optional) Configure flags to specify which events are logged.  
See “Configuring the L2TP Tracing Flags” on page 249.

## Configuring the L2TP Trace Log Filename

---

By default, the name of the file that records trace output for L2TP is **jl2tpd**. You can specify a different name with the **file** option.

To configure the filename for L2TP tracing operations:

- Specify the name of the file used for the trace output.

```
[edit services l2tp traceoptions]
user@host# set file l2tp_logfile_1
```

**Related  
Documentation**

- Configuring an L2TP LAC on page 241
- Tracing L2TP Operations for Subscriber Access on page 247
- **traceoptions on page 1225**

---

## Configuring the Number and Size of L2TP Log Files

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

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

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.

```
[edit protocols l2tp traceoptions]
user@host# set file l2tp_1_logfile_1 files 20 size 2097152
```

**Related  
Documentation**

- Configuring an L2TP LAC on page 241
- Tracing L2TP Operations for Subscriber Access on page 247
- **traceoptions on page 1225**

---

## Configuring Access to the L2TP Log File

By default, only the user who configures the tracing operation can access the log files. 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 l2tp traceoptions]
user@host# set file l2tp_1_logfile_1 world-readable
```

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

- Configure the log file to be no-world-readable.  

```
[edit services l2tp traceoptions]
user@host# set file l2tp_1_logfile_1 no-world-readable
```

#### Related Documentation

- Configuring an L2TP LAC on page 241
- Tracing L2TP Operations for Subscriber Access on page 247
- **traceoptions on page 1225**

## Configuring a Regular Expression for L2TP LAC 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 to be matched.

To configure regular expressions to be matched:

- Configure the regular expression.  

```
[edit services l2tp traceoptions]
user@host# set file l2tp_1_logfile_1 match regex
```

#### Related Documentation

- Configuring an L2TP LAC on page 241
- Tracing L2TP Operations for Subscriber Access on page 247
- **traceoptions on page 1225**

## Configuring the L2TP 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
<b>all</b>	Trace all operations
<b>configuration</b>	Trace configuration events
<b>events</b>	Trace interface events
<b>general</b>	Trace general events
<b>gres</b>	Trace GRES events
<b>init</b>	Trace daemon initialization

Flag	Description
<code>ipc-rx</code>	Trace IPC receive events
<code>ipc-tx</code>	Trace IPC transmit events
<code>memory</code>	Trace memory management code
<code>message</code>	Trace message processing events
<code>packet-error</code>	Trace packet error events
<code>parse</code>	Trace parsing events
<code>protocol</code>	Trace L2TP events
<code>receive-packets</code>	Trace received L2TP packets
<code>routing-processes</code>	Trace routing process interactions
<code>routing-socket</code>	Trace routing socket events
<code>session-db</code>	Trace session database interactions
<code>states</code>	Trace state machine events
<code>timer</code>	Trace timer events
<code>transmit-packets</code>	Trace transmitted L2TP packets
<code>tunnel</code>	Trace tunnel events

To configure the flags for the events to be logged:

- Configure the flags.  

```
[edit services l2tp traceoptions]
user@host# set flag flag
```

#### Related Documentation

- Configuring an L2TP LAC on page 241
- Tracing L2TP Operations for Subscriber Access on page 247
- `traceoptions` on page 1225

## Verifying and Managing L2TP for Subscriber Access

**Purpose** View or clear information about L2TP tunnels and sessions.

**Action** • To display the L2TP destinations:



user@host> show services l2tp destination

- To clear L2TP destinations:

user@host> clear services l2tp destination

- To display the L2TP sessions:

user@host> show services l2tp session

- To clear L2TP sessions:

user@host> clear services l2tp session

- To clear session statistics:

user@host> clear services l2tp session statistics

- To display a summary of L2TP tunnels, sessions, errors, and control and data packets:

user@host> show services l2tp summary

- To display the L2TP tunnels:

user@host> show services l2tp tunnel

- To clear L2TP tunnels:

user@host> clear services l2tp tunnel

- To clear L2TP tunnel statistics:

user@host> clear services l2tp tunnel statistics

**Related  
Documentation**

- [\*Junos OS System Basics and Services Command Reference.\*](#)



## PART 7

# Diameter Base Protocol and Applications for Subscriber Access

- Diameter Base Protocol Overview on page 255
- Configuring Diameter Base Protocol on page 259
- JSRC and Juniper Networks Session Resource Control (SRC) Overview on page 271
- Configuring JSRC for Subscriber Access on page 279
- Subscribers on Static Interfaces on page 283
- Configuring Subscribers over Static Interfaces on page 287
- Static Subscribers for Subscriber Access Examples on page 301
- PTSP and Juniper Networks Session and Resource Control (SRC) on page 303
- Configuring the PTSP Application on page 311
- Configuring Packet-Triggered Subscriber Services on page 317
- Gx-Plus Overview on page 329
- Configuring Gx-Plus on page 339



# Diameter Base Protocol Overview

- Diameter Base Protocol Overview on page 255

## Diameter Base Protocol Overview

---

The Diameter protocol is defined in *RFC 3588, Diameter Base Protocol*, and provides an alternative to RADIUS that is more flexible and extensible. The Diameter base protocol provides basic services to one or more applications (also called functions) that each runs in a different Diameter instance. The individual application provides the extended AAA functionality. Applications that use Diameter include Gx-Plus, JSRC, and PTSP.

Diameter peers communicate over a reliable TCP transport layer connection by exchanging Diameter messages that convey status, requests, and acknowledgments by means of standard Diameter AVPs and application-specific AVPs. The Diameter transport layer configuration is based on Diameter network elements (DNEs); multiple DNEs per Diameter instance are supported. Currently only the predefined *master* Diameter instance is supported, but you can configure alternative values for many of the master Diameter instance values.

Each DNE consists of a prioritized list of peers and a set of routes that define how traffic is forwarded. Each route associates a destination with a function, a function partition, and a metric. When an application sends a message to a routed destination, all routes within the Diameter instance are examined for a match. When the best route to the destination has been selected, the message is forwarded by means of the DNE that includes that route.

Multiple routes to the same destination can exist within a given DNE and in different DNEs. In the case of multiple routes that match a request for forwarding, the best route is selected as follows:

1. The route with the lowest metric is selected.
2. In the event of a tie, the route with the highest specification score is selected.
3. In the event of another tie, then the names of the DNEs are compared in lexicographical order. The route in the DNE with the lowest value is selected. For example, dne-austin has a lower value than dne-boston.
4. If the routes are tied within the same DNE, then the route names are compared in lexicographical order. The route with the lowest value is selected.

The specification score of a route is 0 by default. Points are added to the score as follows:

- If the destination realm matches the request, add 1.
- If the destination host matches the request, add 2.
- If the function matches the request, add 3.
- If the function partition matches the request, add 4.

When the state of any DNE changes, the route lookup for all destinations is reevaluated. All outstanding messages to routed destinations are rerouted as needed, or discarded.

To configure a Diameter network element, include the **network-element** statement at the **[edit diameter]** hierarchy level. Include the **route** statement at the **[edit diameter network-element element-name forwarding]** hierarchy level.

To configure a route for the DNE, include the **destination** (optional), **function** (optional), and **metric** statements at the **[edit diameter network-element element-name forwarding route dne-route-name]** hierarchy level.

Specify the Diameter peers associated with the DNE by including one or more **peer** statements at the **[edit diameter network-element element-name]** hierarchy level.

Set the priority for each peer with the **priority** statement at the **[edit diameter network-element element-name peer peer-name]** hierarchy level.

Diameter requires you to configure information about the origin node; this is the endpoint node that originates Diameter for the Diameter instance. Include the **host** and **realm** statements at the **[edit diameter]** hierarchy level to configure the Diameter origin.

You can optionally configure one or more **transports** to specify the source (local) address of the transport layer connection. To configure a Diameter transport, include the **transport** statement at the **[edit diameter]** hierarchy level. Then include the **address** statement at the **[edit diameter transport transport-name]** hierarchy level.

You can optionally specify a logical system and routing instance for the connection by including the **logical-system** and **routing-instance** statements at the **[edit diameter transport transport-name]** hierarchy level. By default, Diameter uses the *default* logical system and *master* routing instance. The logical system and routing instance for the transport connection must match that for the peer, or a configuration error is reported.

Each Diameter peer is specified by a name. Peer attributes include address and the destination TCP port used by active connections to this peer. To configure a Diameter peer, include the **peer** statement at the **[edit diameter]** hierarchy level, and then include the **address** and **connect-actively** statements at the **[edit diameter peer peer-name]** hierarchy level.

To configure the active connection, include the **port** and **transport** statements at the **[edit diameter peer peer-name connect-actively]** hierarchy level. The assigned transport identifies the transport layer source address used to establish active connections to the peers. **transport** statements.

**Related  
Documentation**

- [Configuring Diameter on page 259](#)
- [Gx-Plus for Provisioning Subscribers Overview on page 329](#)
- [Juniper Networks Session and Resource Control \(SRC\) and JSRC Overview on page 271](#)
- [Juniper Networks Session and Resource Control \(SRC\) and PTSP Overview on page 304](#)





# Configuring Diameter Base Protocol

- Configuring Diameter on page 259
- Configuring the Origin Attributes of the Diameter Instance on page 260
- Configuring Diameter Peers on page 260
- Configuring Diameter Network Elements on page 261
- Configuring the Diameter Transport on page 262
- Tracing Diameter Base Protocol Processes for Subscriber Access on page 262
- Configuring the Diameter Base Protocol Trace Log Filename on page 263
- Configuring the Number and Size of Diameter Base Protocol Log Files on page 264
- Configuring Access to the Diameter Base Protocol Log File on page 264
- Configuring a Regular Expression for Diameter Base Protocol Lines to Be Logged on page 265
- Configuring the Diameter Base Protocol Tracing Flags on page 265
- Verifying Diameter Node, Instance, and Route Information on page 266
- Verifying and Managing Diameter Function Information on page 267
- Verifying and Managing Diameter Peer Information on page 268
- Verifying Diameter Network Element Information on page 269
- Troubleshooting Diameter Network Configuration on page 269
- Troubleshooting Diameter Network Connectivity on page 270

## Configuring Diameter

---

You configure Diameter by specifying the endpoint origin, the remote peers, the transport layer connection, and network elements that associate routes with peers. Only the master Diameter instance is currently supported. You can configure alternative values for the master instance only in the context of the master routing instance

To configure Diameter base protocol:

1. Configure the origin realm and origin host of the Diameter master instance.  
See “Configuring the Origin Attributes of the Diameter Instance” on page 260
2. Configure the Diameter peers.

See “Configuring Diameter Peers” on page 260

3. (Optional) Configure the Diameter transport layer elements.

See “Configuring the Diameter Transport” on page 262

4. (Optional) Configure the Diameter network elements.

See “Configuring Diameter Network Elements” on page 261

5. (Optional) Configure trace options for troubleshooting the configuration.

See “Tracing Diameter Base Protocol Processes for Subscriber Access” on page 262.

---

## Configuring the Origin Attributes of the Diameter Instance

---

You can configure the identifying characteristics of the endpoint node that originates Diameter messages for the Diameter instance. The hostname is supplied as the value for the Origin-Host AVP by the Diameter instance. The realm is supplied as the value for the Origin-Realm AVP by the Diameter instance.

To configure the origin attributes for a Diameter instance:

1. Specify the name of the host that originates the Diameter message.

```
[edit diameter origin]
user@host# set host host14
```

2. Specify the realm of the host that originates the Diameter message.

```
[edit diameter origin]
user@host# set realm example.com
```

- Related Documentation**
- Configuring Diameter on page 259
  - origin on page 1091

---

## Configuring Diameter Peers

---

You can configure the peers to which Diameter sends messages. By default, logical system *default* and routing instance *master* are used. Port 3868 is used for active connections to peers by default.

To configure a remote peer for a Diameter instance:

1. Specify the name of the Diameter peer.

```
[edit diameter]
user@host# set peer p3
```

2. Specify the address of the Diameter peer.

```
[edit diameter peer p3]
user@host# set address 192.168.23.10
```

3. (Optional) Specify a routing instance, a logical system, or a logical system and routing instance for the Diameter peer.

```
[edit diameter peer p3]
user@host# set routing-instance ri8
```

```
[edit diameter peer p3]
user@host# set logical-system ls10
```

```
[edit diameter peer p3]
user@host# set logical-system ls10 routing-instance ri8
```

4. (Optional) Specify the port that Diameter uses for active connections to the peer.

```
[edit diameter peer p3]
user@host# set connect-actively port 49152
```

5. Specify the transport that Diameter uses for active connections to the peer.

```
[edit diameter peer p3]
user@host# set connect-actively transport t6
```

#### Related Documentation

- Configuring Diameter on page 259

## Configuring Diameter Network Elements

A Diameter network element (DNE) consists of associated functions, a list of prioritized peers, and a set of forwarding rules. The forwarding rules define individual routes through a set of associated destinations, functions, and metrics.

Before you configure Diameter network elements, perform the following task:

- Define the Diameter peers. See “Configuring Diameter Peers” on page 260.

To configure a Diameter network element:

1. Specify the name of the network element.

```
[edit diameter]
user@host# set network-element dne25
```

2. (Optional) Associate one or more functions with the network element. All functions are associated by default.

```
[edit diameter network-element dne25]
user@host# set function jsrsc
```

3. Associate a Diameter peer with the network element and set the priority for the peer.

```
[edit diameter network-element dne25]
user@host# set peer peer1 priority 1
```

4. Specify a route that is reachable through the network element based on the forwarding rules that you define.

```
[edit diameter network-element dne25]
user@host# set forwarding route dne-route2
```

5. Specify a metric for the route.

```
[edit diameter network-element dne25 forwarding route dne-route2]
user@host# set metric 15
```

6. (Optional) Associate the route with a destination host and realm.

```
[edit diameter network-element dne25 forwarding route dne-route2]  
user@host# set destination host host5 realm example.com
```

7. (Optional) Specify a function (application) associated with the route.

```
[edit diameter network-element dne25 forwarding route dne-route2]  
user@host# set function jsr
```

**Related Documentation**

- [Configuring Diameter on page 259](#)

---

## Configuring the Diameter Transport

You can configure one or more transports for a Diameter instance to set the IP address for the local connection, and optionally configure a logical system or routing instance context. By default, the logical system *default* and the routing instance *master* are used. The logical system and routing instance for the transport connection must match that for the peer, or a configuration error is reported. Multiple peers can share the same transport.

To configure a transport for a Diameter instance:

1. Configure the transport name.

```
[edit diameter]  
user@host# set transport t1
```

2. Configure the local IP address for the Diameter local transport connection.

```
[edit diameter transport t1]  
user@host# set address 10.9.20.0
```

3. (Optional) Configure a logical system and optionally a routing instance for the transport.

```
[edit diameter transport t1]  
user@host# set logical-system ls5
```

4. (Optional) Configure a routing instance for the transport.

```
[edit diameter transport t1]  
user@host# set routing-instance ri10
```

**Related Documentation**

- [Configuring Diameter on page 259](#)

---

## Tracing Diameter Base Protocol Processes for Subscriber Access

The Junos OS trace feature tracks Diameter base protocol operations and records events 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 **jdiameterd** located in the **/var/log** directory. You cannot change the directory (**/var/log**) in which trace files are located.
2. When the file **jdiameterd** reaches 128 kilobytes (KB), it is renamed **jdiameterd.0**, then **jdiameterd.1**, and finally **jdiameterd.2**, until there are three trace files. Then the oldest trace file (**jdiameterd2**) is overwritten.

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

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To configure Diameter base protocol tracing operations:

1. (Optional) Configure a trace log filename.  
See “Configuring the Diameter Base Protocol Trace Log Filename” on page 263.
2. (Optional) Configure the number and size of trace logs.  
See “Configuring the Number and Size of Diameter Base Protocol Log Files” on page 264.
3. (Optional) Configure user access to trace logs.  
See “Configuring Access to the Diameter Base Protocol Log File” on page 264.
4. (Optional) Configure a regular expression to filter the information to be included in the trace log.  
See “Configuring a Regular Expression for Diameter Base Protocol Lines to Be Logged” on page 265.
5. (Optional) Configure flags to specify which events are logged.  
See “Configuring the Diameter Base Protocol Tracing Flags” on page 265.

## Related Documentation

### Configuring the Diameter Base Protocol Trace Log Filename

By default, the name of the file that records trace output for Diameter base protocol is **jdiameterd**. You can specify a different name with the **file** option.

To configure the filename for Diameter base protocol tracing operations:

- Specify the name of the file used for the trace output.  
[edit system processes diameter-service traceoptions]  
user@host# set file diam\_logfile\_1

- Related Documentation**
- [Configuring Diameter on page 259](#)
  - [Tracing Diameter Base Protocol Processes for Subscriber Access on page 262](#)
  - [traceoptions on page 1223](#)

---

## Configuring the Number and Size of Diameter Base Protocol Log Files

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

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

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. (Diameter base protocol supports the **files** and **size** options for the **traceoptions** statement.)

```
[edit system processes diameter-service traceoptions]  
user@host# set file diam_1_logfile_1 files 20 size 2097152
```

- Related Documentation**
- [Configuring Diameter on page 259](#)
  - [Tracing Diameter Base Protocol Processes for Subscriber Access on page 262](#)
  - [traceoptions on page 1223](#)

---

## Configuring Access to the Diameter Base Protocol Log File

By default, only the user who configures the tracing operation can access the log files. 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 system processes diameter-service traceoptions]  
user@host# set file diam_1_logfile_1 world-readable
```

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

- Configure the log file to be no-world-readable.  

```
[edit system processes diameter-service traceoptions]
user@host# set file diam_1_logfile_1 no-world-readable
```

#### Related Documentation

- Configuring Diameter on page 259
- Tracing Diameter Base Protocol Processes for Subscriber Access on page 262
- **traceoptions on page 1223**

## Configuring a Regular Expression for Diameter Base Protocol 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 to be matched.

To configure regular expressions to be matched:

- Configure the regular expression.  

```
[edit system processes diameter-service traceoptions]
user@host# set file diam_1_logfile_1 match regex
```

#### Related Documentation

- Configuring Diameter on page 259
- Tracing Diameter Base Protocol Processes for Subscriber Access on page 262
- **traceoptions on page 1223**

## Configuring the Diameter Base Protocol 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
<b>all</b>	Trace all events
<b>application</b>	Trace Diameter application interface events
<b>configuration</b>	Trace configuration events
<b>daemon</b>	Trace daemon level events
<b>diameter-instance</b>	Trace Diameter instance events
<b>dne</b>	Trace Diameter DNE events

Flag	Description
<b>framework</b>	Trace Diameter framework events
<b>memory-management</b>	Trace memory management events
<b>messages</b>	Trace Diameter messages
<b>node</b>	Trace Diameter node events
<b>peer</b>	Trace Diameter peer events

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit system processes diameter-service traceoptions]
user@host# set flag dne
```

#### Related Documentation

- Configuring Diameter on page 259
- Tracing Diameter Base Protocol Processes for Subscriber Access on page 262
- **traceoptions on page 1223**

## Verifying Diameter Node, Instance, and Route Information

**Purpose** View Diameter node information:

#### Action

- To display summary information about all Diameter nodes:  

```
user@host> show diameter
```
- To display summary information about all Diameter nodes and add information about Diameter functions, instances, network elements, and peers:  

```
user@host> show diameter brief
```
- To display brief information about all Diameter nodes and add information about Diameter routes:  

```
user@host> show diameter detail
```
- To display summary information about all Diameter instances:  

```
user@host> show diameter instance
```
- To display detailed information about all Diameter instances:  

```
user@host> show diameter instance detail
```
- To display information about a specific Diameter instance, add the instance name to the command:  

```
user@host> show diameter instance master
```

```
user@host> show diameter instance detail master
```



- To display summary information about all Diameter routes:  

```
user@host> show diameter route
```
- To display detailed information about all Diameter routes:  

```
user@host> show diameter route detail
```
- To display information about a specific Diameter route, add the route name to the command:  

```
user@host> show diameter route dne-route2
```

```
user@host> show diameter route detail dne-route2
```

**Related Documentation** • [Junos OS System Basics and Services Command Reference](#)

## Verifying and Managing Diameter Function Information

**Purpose** View or clear Diameter function information:

- Action**
- To display summary information about all functions associated with Diameter:  

```
user@host> show diameter function
```
  - To display detailed information about all functions associated with Diameter:  

```
user@host> show diameter function detail
```
  - To display information about a specific function associated with Diameter, add the function name to the command:  

```
user@host> show diameter function jsrc
```

```
user@host> show diameter function detail ptsp
```
  - To display summary statistics about all functions associated with Diameter:  

```
user@host> show diameter function statistics
```
  - To display detailed statistics about all functions associated with Diameter:  

```
user@host> show diameter function statistics detail
```
  - To display statistics about a specific function associated with Diameter, add the function name to the command:  

```
user@host> show diameter function statistics gx-plus
```

```
user@host> show diameter function statistics detail jsrc
```
  - To delete current statistics for all functions associated with Diameter:  

```
user@host> clear diameter function statistics
```
  - To delete current statistics for a specific function associated with Diameter:  

```
user@host> clear diameter function gx-plus statistics
```

**Related Documentation** • [Junos OS System Basics and Services Command Reference](#)

## Verifying and Managing Diameter Peer Information

---

**Purpose** View or clear Diameter peer information:

- Action**
- To display summary information about all Diameter peers:  
`user@host> show diameter peer`
  - To display detailed information about all Diameter peers:  
`user@host> show diameter peer detail`
  - To display information about a specific Diameter peer, add the peer name to the command:  
`user@host> show diameter peer peer235`  
`user@host> show diameter peer detail peer235`
  - To display summary information about Diameter peer-to-network-element mapping for all peers:  
`user@host> show diameter peer map`
  - To display detailed information about Diameter peer-to-network-element mapping for all peers:  
`user@host> show diameter peer map detail`
  - To display information about Diameter peer-to-network-element mapping for a specified peer, add the peer name to the command:  
`user@host> show diameter peer map peer235`  
`user@host> show diameter peer map detail peer235`
  - To display summary statistics about all Diameter peers:  
`user@host> show diameter peer statistics`
  - To display detailed statistics about all Diameter peers:  
`user@host> show diameter peer statistics detail`
  - To display summary statistics about a specified Diameter peer:  
`user@host> show diameter peer statistics peer235`
  - To display detailed statistics about a specified Diameter peer:  
`user@host> show diameter peer statistics detail peer235`
  - To delete the specified Diameter peer and all of its statistics.  
`user@host>clear diameter peer peer5 connection`
  - To delete the specified Diameter peer and its current statistics:  
`user@host>clear diameter peer peer5 statistics`

**Related Documentation**

- [\*Junos OS System Basics and Services Command Reference\*](#)

## Verifying Diameter Network Element Information

<b>Purpose</b>	View Diameter network element information:
<b>Action</b>	<ul style="list-style-type: none"> <li>To display summary information about Diameter network elements:  <pre>user@host&gt; show diameter network-element</pre> </li> <li>To display detailed information about Diameter network elements:  <pre>user@host&gt; show diameter network-element detail</pre> </li> <li>To display information about Diameter network elements for a specified network element, include the element name in the command:  <pre>user@host&gt; show diameter network-element dne-1</pre> <pre>user@host&gt; show diameter network-element detail dne-1</pre> </li> <li>To display summary information about Diameter network-element-to-peer mapping for all network elements:  <pre>user@host&gt; show diameter network-element map</pre> </li> <li>To display detailed information about Diameter network-element-to-peer mapping for all network elements:  <pre>user@host&gt; show diameter network-element map detail</pre> </li> </ul>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><i>Junos OS System Basics and Services Command Reference</i></li> </ul>

## Troubleshooting Diameter Network Configuration

<b>Problem</b>	<p>A misconfiguration of the network can prevent Diameter from functioning properly. Configuration options for the Diameter base protocol are simple in the current release, simplifying discovery of a misconfiguration.</p> <p>The output of the <b>show diameter peer</b> command indicates a peer is in the no-activation state. In this case issue the <b>show diameter peer map</b> and <b>show diameter network-element map</b> commands to determine which network elements use the peer. The output of these commands can indicate why the peer is not activated. For example, all the associated network elements might have higher-priority peers in the open state.</p> <p>The failed-to-forward counters are increasing in the output of the <b>show diameter function statistics detail</b> command. this can indicate that the routes to the peer are incorrectly configured. Check the network connectivity, then use the <b>show diameter routes</b> command to determine whether application traffic is being correctly forwarded.</p>
<b>Cause</b>	Typical misconfigurations appear in the routes, peers, and network element configurations.
<b>Solution</b>	Use the appropriate statements to correct the misconfiguration.

- Related Documentation**
- show diameter function statistics
  - show diameter network-element map
  - show diameter peer
  - show diameter peer map
  - show diameter route

---

## Troubleshooting Diameter Network Connectivity

---

**Problem** In some circumstances, problems can arise with network connectivity to Diameter peers. The problem may originate with the peer or the peer host.

The output of the **show diameter peer** command indicates a peer is in the suspended, rejected, or bad-peer state.

**Cause** The suspended state indicates that the peer is not responding or has some other malfunction, or the network path to the peer does not exist.

The rejected state indicates that the network connection has been rejected by the peer.

The bad-peer state indicates that the network connection has been rejected by the router on which the peer resides.

**Solution** Determine how persistent the problem is by issuing the **show diameter peer statistics peer-name brief** command to check the connectivity statistics.

- Related Documentation**
- show diameter peer
  - show diameter peer statistics

## CHAPTER 20

# JSRC and Juniper Networks Session Resource Control (SRC) Overview

- Juniper Networks Session and Resource Control (SRC) and JSRC Overview on page 271
- Diameter Messages Exchanged by JSRC and the SAE on page 272
- Understanding Diameter AVPs for JSRC on page 273
- Understanding JSRC-SAE Interactions on page 276

### Juniper Networks Session and Resource Control (SRC) and JSRC Overview

The Juniper Networks Session and Resource Control (SRC) environment provides a central administrative point for managing subscribers and their services. The SRC software runs on Juniper Networks C Series Controllers. The SRC software uses the Diameter protocol for communications between the local SRC peer on a Juniper Networks routing platform and the remote SRC peer on a C Series Controller. The local SRC peer is known as JSRC and is part of the AAA application. The remote SRC peer is the service activation engine (SAE); the SAE acts as the controlling agent in the SRC environment. JSRC and the SAE jointly provide the remote control enforcement functionality (RCEF).

JSRC has the following responsibilities:

- Request address authorization from the SAE.
- Request service activations from the SAE.
- Activate and deactivate services as specified by the SAE. JSRC can activate multiple policies with the same service (dynamic profile) name.
- Log out subscribers as specified by the SAE.
- Update the SAE with status of new service activations and deactivations.
- Synchronize subscriber state and service information with the SAE.
- Notify the SAE when subscribers log out.

The SRC software enables the SAE to activate and deactivate subscriber services (described by SRC policies) and log out subscribers. The SAE can control only those resources that have been provisioned through SAE. Therefore, the SAE receives information about only those subscribers for whom JSRC has requested provisioning from the SAE. For example, when a subscriber logs in, but the configuration did not require

the session activation path to include SAE provisioning, the SAE does not receive information about this subscriber and cannot control the subscriber session.

Similarly, the SAE can control only the subscriber services that it has activated. When a service is not activated from the SAE—a RADIUS-activated service, for example—the SAE receives no information about the service and has no control over it.



**NOTE:** More than one Diameter-based application (function) can run on a router simultaneously.

## Hardware Requirements for JSRC for Subscriber Access

JSRC is supported on Juniper Networks MX Series 3D Universal Edge Routers. JSRC currently supports subscriber sessions on static and dynamic interfaces.

### Related Documentation

- Configuring JSRC on page 279
- Diameter Messages Exchanged by JSRC and the SAE on page 272
- Understanding JSRC-SAE Interactions on page 276

## Diameter Messages Exchanged by JSRC and the SAE

JSRC is a Juniper Networks Diameter application registered with the IANA (<http://www.iana.org>) as Juniper Policy-Control-JSRC, with an ID of 16777244. JSRC and the SAE communicate by exchanging the Diameter messages described in Table 31 on page 272.

**Table 31: Diameter Messages Used by JSRC and the SAE**

Diameter Message	Code	Description
AA-Request (AAR)	265	Request from JSRC to the SAE at subscriber login or during SAE-JSRC synchronization. The request can be one of three types: address-authorization, provisioning-request, or synchronization.
AA-Answer (AAA)	265	Response from the SAE to the JSRC AA-Request message.
Abort-Session-Request (ASR)	274	Request from the SAE to JSRC to log out a provisioned subscriber.
Abort-Session-Answer (ASA)	274	Response from JSRC to the SAE ASR message. If the application sends the logout request to AAA, the ASA message includes a success notification (ACK). If the logout failed, the ASA message includes a failure notification (NAK).
Push-Profile-Request (PPR)	288	Request from the SAE to JSRC to activate or deactivate services after a subscriber logs in.

Table 31: Diameter Messages Used by JSRC and the SAE (*continued*)

Diameter Message	Code	Description
Push-Profile-Answer (PPA)	288	Response from JSRC to the SAE PPR message. Includes success or failure notification for each of the service activation or deactivation commands in the request.
Session-Resource-Query (SRQ)	277	Request from JSRC to the SAE or from the SAE to JSRC to initiate synchronization between JSRC and the SAE.
Session-Resource-Reply (SRR)	277	Response to the SRQ message to begin synchronization.
Session-Termination-Request (STR)	275	Notification from JSRC to the SAE that a provisioned subscriber has logged out.
Session-Termination-Answer (STA)	275	Response from the SAE to the JSRC STR message

**Related Documentation**

- Configuring JSRC on page 279
- Juniper Networks Session and Resource Control (SRC) and JSRC Overview on page 271
- Understanding Diameter AVPs for JSRC on page 273
- Understanding JSRC-SAE Interactions on page 276

## Understanding Diameter AVPs for JSRC

Diameter conveys information by including various attribute-value pairs (AVPs) in Diameter messages. Table 32 on page 273 lists the standard Diameter AVPs used in JSRC interactions. Diameter reserves AVP code numbers 0 through 255 for RADIUS functions that are implemented in Diameter.

Table 32: Standard Diameter AVPs

Diameter AVP	Code Number	Description	Type
User-Name	1	Specifies the username. For a subscriber managed by AAA, the value is the subscriber's login name. For a static interface, the value is the interface name, which is used as the subscriber's login name.	UTF8String

Table 32: Standard Diameter AVPs (*continued*)

Diameter AVP	Code Number	Description	Type
Result-Code	268	<p>Indicates whether a request completed successfully. Provides an error code if the request failed.</p> <p>The following classes are recognized by Diameter:</p> <ul style="list-style-type: none"> <li>• 1xxx—Informational</li> <li>• 2xxx—Success</li> <li>• 3xxx—Protocol errors</li> <li>• 4xxx—Transient errors</li> <li>• 5xxx—Permanent failures</li> </ul> <p>Unrecognized classes, which begin with numerals 6–9 or 0, are handled as permanent failures.</p> <p>JSRC supports the following values; all non-success values are treated as permanent failures:</p> <ul style="list-style-type: none"> <li>• 1001—DIAMETER_MULTI_ROUND_AUTH</li> <li>• 2001—DIAMETER_SUCCESS</li> <li>• 5002—DIAMETER_UNKNOWN_SESSION_ID</li> <li>• 5012—DIAMETER_UNABLE_TO_COMPLY</li> </ul>	Unsigned32
Auth-Session-State	277	<p>Indicates whether AAA session state is maintained.</p> <ul style="list-style-type: none"> <li>• 0—STATE_MAINTAINED</li> <li>• 1—NO_STATE_MAINTAINED</li> </ul>	Enumerated
Termination-Cause	295	<p>Indicates the reason why a session was terminated on the access device.</p> <ul style="list-style-type: none"> <li>• 1—DIAMETER_LOGOUT</li> <li>• 2—DIAMETER_SERVICE_NOT_PROVIDED</li> <li>• 3—DIAMETER_BAD_ANSWER</li> <li>• 4—DIAMETER_ADMINISTRATIVE</li> <li>• 5—DIAMETER_LINK_BROKEN</li> <li>• 6—DIAMETER_AUTH_EXPIRED</li> <li>• 7—DIAMETER_USER_MOVED</li> <li>• 8—DIAMETER_SESSION_TIMEOUT</li> </ul>	Enumerated

Juniper Networks AVPs are used in addition to the standard Diameter AVPs. These AVPs have an enterprise number of 2636. Table 33 on page 274 lists the Juniper Networks AVPs used in JSRC interactions.

Table 33: Juniper Networks Diameter AVPs

Diameter AVP	Code Number	Description	Type
Juniper-DHCP-Options	2010	Specifies the client's DHCP options.	OctetString
Juniper-DHCP-GI-Address	2011	Specifies the DHCP relay agent's IP address.	OctetString



Table 33: Juniper Networks Diameter AVPs (*continued*)

Diameter AVP	Code Number	Description	Type
Juniper-Policy-Install	2020	Specifies policies to be activated for the subscriber. Includes Juniper-Policy-Name and Juniper-Policy-Definition.	Grouped
Juniper-Policy-Name	2021	Defines the name of a policy decision.	OctetString
Juniper-Policy-Definition	2022	Defines a policy decision. Includes Juniper-Policy-Name, Juniper-Template-Name, and Juniper-Substitution.	Grouped
Juniper-Template-Name	2023	Profile name defined by the router.	UTF8String
Juniper-Substitution	2024	Defines the substitution attributes. Includes Juniper-Substitution-Name and Juniper-Substitution-Value.	OctetString
Juniper-Substitution-Name	2025	Defines the name of the variable to be replaced.	OctetString
Juniper-Substitution-Value	2026	Defines the value of the variable to be replaced.	OctetString
Juniper-Policy-Remove	2027	Specifies policies to be deactivated for the subscriber. Includes Juniper-Policy-Name.	Grouped
Juniper-Policy-Failed	2035	Specifies the name of the policy activation or deactivation that failed.	OctetString
Juniper-Policy-Success	2038	Specifies the name of the policy activation or deactivation that succeeded.	OctetString
Juniper-Logical-System	2046	Specifies the logical system.	UTF8String
Juniper-Routing-Instance	2047	Specifies the routing instance.	UTF8String
Juniper-Jsrc-Partition	2048	Specifies the logical system and routing instance for the subscriber or request. Includes Juniper-Logical-System and Juniper-Routing-Instance.	Grouped
Juniper-Request-Type	2050	Describes the type of request: <ul style="list-style-type: none"> <li>• 1—ADDRESS_AUTHORIZATION</li> <li>• 2—PROVISIONING_REQUEST</li> <li>• 3—SYNCHRONIZATION</li> </ul>	Enumerated
Juniper-Synchronization-Type	2051	Describes the type of synchronization: <ul style="list-style-type: none"> <li>• 1—FULL-SYNC</li> <li>• 2—FAST-SYNC</li> <li>• 3—NO-STATE-TO-SYNC</li> </ul>	Enumerated

Table 33: Juniper Networks Diameter AVPs (*continued*)

Diameter AVP	Code Number	Description	Type
Juniper-Synchronization	2052	Describes the state of synchronization: <ul style="list-style-type: none"> <li>1—NO-SYNC; this is the default state</li> <li>2—SYNC-IN-PROGRESS</li> <li>3—SYNC-COMPLETE</li> </ul>	Enumerated

- Related Documentation**
- Diameter Messages Exchanged by JSRC and the SAE on page 272
  - Understanding JSRC-SAE Interactions on page 276

## Understanding JSRC-SAE Interactions

This topic describes the sequences of Diameter messages exchanged between JSRC and the SAE as they interact to perform the following tasks for subscriber access:

- Subscriber login
- Service activation
- Service deactivation
- Resynchronization
- SAE-initiated subscriber logout
- Subscriber-initiated logout

### Subscriber Login

JSRC authorization is enabled for DHCP subscribers when you include the **authorization-order jsrc** statement at the **[edit access profile *profile-name*]** hierarchy level. This setting causes AAA to ignore the authentication order setting in the access profile. As a result, AAA does not authenticate the DHCP subscribers. For non-DHCP subscribers, AAA ignores the **authorization-order** statement.

When a DHCP subscriber attempts to log in, DHCP sends an authentication request to AAA. In turn, JSRC sends a Diameter AA-Request message to the SAE. SAE returns a Diameter AA-Answer message that can include the Framed-IP-Address attribute and the Juniper-DHCP-Options AVP (AVP code 2010). JSRC ignores any other optional AVPs included in this AA-Answer message.

JSRC provisioning is enabled for DHCP (and SSC) subscribers when you include the **provisioning-order** statement at the **[edit access profile *profile-name*]** hierarchy level. When the application requests AAA to activate the subscriber's session, JSRC sends an AA-Request message that includes the Juniper-Request-Type AVP (AVP code 2050) with a value that indicates service provisioning is requested from the SAE.

The SAE returns a AA-Answer message that contains an ACK if the request is accepted or a NAK if the request is denied. If the request is accepted, the AA-Answer message

includes the Juniper-Policy-Install AVP (AVP code 2020), which is used to specify the service to attach to the subscriber's interface. When this AVP is included, the SAE sets the Result-Code AVP to 1001 (DIAMETER\_MULTI\_ROUND\_AUTH). This code means that the JSRC must send another AA-Request message to the SAE to report the success or failure of the policy instantiation (service activation) by AAA. JSRC ignores any other optional AVPs included in this AA-Answer message. The SAE returns an AA-Answer message to acknowledge this second AA-Request message.

## Subscriber Service Activation and Deactivation

SAE policies provision subscriber services. After a subscriber is logged in, the SAE can send a PPR message to JSRC to activate or deactivate services. A given PPR can include the Juniper-Policy-Install AVP (AVP code 2020) to activate a service, the Juniper-Policy-Remove AVP (AVP code 2027) to deactivate a service, or both (for different services). A PPR can include no more than three of these AVPs (install, remove, or mixed).

JSRC sends a PPA message to the SAE when it has completed the tasks requested in the PPR. The PPA indicates the success or failure of the actions requested in the PPR.



**NOTE:** If you use RADIUS or the CLI to deactivate a service that the SAE, the SAE becomes unsynchronized with the state of subscribers on the routing engine.

## Subscriber Resynchronization

During resynchronization, JSRC informs the SAE about the services that are active for the provisioned subscribers. Either JSRC or the SAE initiates the resynchronization.

- The SAE initiates resynchronization at startup or when a backup SAE takes over session control due to resource limits or conditions on the primary SAE. The SAE clears its database of all entries in preparation for the synchronization.
- JSRC initiates resynchronization at JSRC startup, such as when AAA starts or restarts.

JSRC can also initiate resynchronization in another circumstance. When an SAE in a multi-SAE environment becomes active, it must send an SRQ to JSRC as its first message. JSRC then locks the Origin-Host AVP of the active SAE. JSRC subsequently triggers resynchronization if it receives a message from any other SAE as indicated by the Origin-Host AVP. Such an incident can occur if communication between the active SAE and a standby SAE is interrupted.

Both entities initiate a resynchronization by sending an SRQ message. The recipient responds with an SRR message. After the SRR is sent, regardless of whether the SAE or JSRC initiates the synchronization, JSRC sends an AA-Request message to the SAE for each provisioned subscriber present in the session database. The AA-Request message includes a Juniper-Policy-Install AVP for the active services. The SAE returns an AA-Answer message with an ACK to acknowledge receipt.

## Subscriber Session Terminated by the SAE

When the SAE terminates a subscriber session, it sends an ASR message to JSRC. JSRC causes AAA to send a logout request to the DHCP (or SSC) client application. When the DHCP client application accepts the logout request, JSRC includes an ACK in the ASR message it sends to the SAE to signify success. If the DHCP client application does not accept the request, then JSRC includes a NAK in the ASR to signify failure. The DHCP client application is responsible for initiating the actual logout sequence with AAA.

## Subscriber Logout

When the DHCP (or SSC) client application sends a subscriber logout notice to AAA, JSRC sends an STR message to notify the SAE that the provisioned subscriber session is being terminated. The SAE returns an STA message to JSRC, and JSRC notifies DHCP that the logout is complete.

### **Related Documentation**

- Configuring JSRC on page 279
- Juniper Networks Session and Resource Control (SRC) and JSRC Overview on page 271
- Diameter Messages Exchanged by JSRC and the SAE on page 272
- Understanding Diameter AVPs for JSRC on page 273

## CHAPTER 21

# Configuring JSRC for Subscriber Access

- Configuring JSRC on page 279
- Configuring the JSRC Partition on page 280
- Assigning a Partition to JSRC on page 281
- Authorizing Subscribers with JSRC on page 281
- Provisioning Subscribers with JSRC on page 282

## Configuring JSRC

---

You can configure the JSRC client application to work with Session and Resource Control (SRC) to centrally manage subscribers and services. JSRC requests address and service authorizations from the remote SRC peer (the SAE), activates and deactivates services as specified by the SAE, logs out subscribers as specified by the SAE, and synchronizes subscriber state and service information with the SAE.

To configure JSRC:

1. Configure the JSRC partition.  
See “Configuring the JSRC Partition” on page 280.
2. Assign the JSRC partition.  
See “Assigning a Partition to JSRC” on page 281.
3. Configure JSRC authorization for subscribers.  
See “Authorizing Subscribers with JSRC” on page 281.
4. Configure JSRC provisioning for subscribers.  
See “Provisioning Subscribers with JSRC” on page 282.
5. Configure JSRC event tracing as part of general authentication service tracing operations.  
See “Tracing General Authentication Service Processes” on page 74.

### Related Documentation

- Juniper Networks Session and Resource Control (SRC) and JSRC Overview on page 271

## Configuring the JSRC Partition

---

JSRC works within a specific logical system: routing instance context, called a partition.



**NOTE:** Currently, only a single partition is supported; you must configure it within the default logical system: routing instance context.

Before you configure the JSRC partition, perform the following task:

- Configure the Diameter instance at the **[edit diameter]** hierarchy level. See “Configuring Diameter” on page 259.

Configuration for the JSRC partition consists of naming the partition and then associating a Diameter instance, the SAE hostname, and the SAE realm with the partition.

To configure the JSRC partition:

1. Create the partition.

```
[edit jsrc]
user@host# set partition partition1
```

2. Specify the Diameter instance for the JSRC partition.



**NOTE:** Currently, only the default Diameter instance, *master*, is supported.

```
[edit jsrc partition partition1]
user@host# set diameter-instance master
```

3. Configure the destination host for the JSRC partition.

```
[edit jsrc partition partition1]
user@host# set destination-host sae1
```

4. Configure the destination realm for the JSRC partition.

```
[edit jsrc partition partition1]
user@host# set destination-realm generic.example.com
```

### Related Documentation

- Configuring JSRC on page 279

## Assigning a Partition to JSRC

---

You must associate a configured JSRC partition with the JSRC instance that you are configuring.

Before you assign a partition to JSRC, perform the following task:

- Configure the JSRC partition. See “Configuring the JSRC Partition” on page 280

To assign the JSRC partition:

- Specify the partition name.

```
[edit jsrc]
user@host# set jsrc-partition partition1
```

### Related Documentation

- Configuring JSRC on page 279

## Authorizing Subscribers with JSRC

---

You can configure AAA to use JSRC in an SRC environment to request authorization from the SAE when AAA is verifying whether a DHCP subscriber can access the router. When JSRC authorization is configured, AAA ignores any configured authentication order settings.

Before you configure JSRC authorization, perform the following tasks:

- Create the subscriber access profile at the **[edit access profile]** hierarchy level.
- Define the subscriber username with the **username-include** statement in the authentication configuration for DHCP local server or DHCP relay.

To configure JSRC authorization:

- Specify **jsrc** as the authorization method in the profile.

```
[edit access profile dhcpsub1]
user@host# set authorization-order jsrc
```

### Related Documentation

- Configuring JSRC on page 279
- Creating Unique Usernames for DHCP Clients on page 128
- **profile** on page 1127

## Provisioning Subscribers with JSRC

---

You can configure AAA to use JSRC in an SRC environment to request provisioning from the SAE to instantiate services for an authenticated subscriber.

Before you configure JSRC provisioning for subscribers, perform the following task:

- Create the subscriber access profile at the **[edit access profile]** hierarchy level.

To configure JSRC provisioning:

- Specify **jsrc** as the provisioning method in the profile.

```
[edit access profile dhcpsub1]  
user@host# set provisioning-order jsrc
```

### Related Documentation

- Configuring JSRC on page 279



# Subscribers on Static Interfaces

- Subscribers on Static Interfaces Overview on page 283

## Subscribers on Static Interfaces Overview

---

You can associate subscribers with statically configured interfaces and provide dynamic service activation and activation for these subscribers. When the static interface comes up, the event is treated as a subscriber login. When the interface goes down, it is treated as a subscriber logout. After the subscribers are present in the session database (SDB), JSRC can report the subscribers to the SAE so that the SRC software can subsequently manage the subscribers.

Alternatively, you can configure the static subscribers to be authenticated and authorized by means of RADIUS. In this case, RADIUS can then activate and deactivate services with change of authorization (CoA) messages. However, this configuration does not prevent the interface from coming up and forwarding traffic. Further, authorization parameters are not imposed on the subscriber interface.

Currently, only Ethernet interfaces support static subscribers. Only one static subscriber can exist over a given interface. An interface cannot appear in more than one group. Static subscribers cannot be created over dynamic interfaces.

Static subscribers are intended to work with JSRC. Include the **provisioning-order jsrc** statement at the **[edit access profile *profile-name*]** hierarchy level to enable JSRC to handle the subscribers at the direction of the SRC software.

If the authentication request fails for a static subscriber, a 60-minute, nonconfigurable timer begins counting down. The request is reissued when the timer expires. This action repeats for as long as the interface is operationally up.

You can force a logout of the static subscriber by issuing the **request services static-subscribers logout interface *interface-name*** command. A static subscriber can also be logged out by AAA or an external policy manager. In both cases, no subsequent logins can take place on the underlying interface until you reset the state by issuing the **request services static-subscribers login interface *interface-name*** command or the router or process reboots.

You can log out an interface group by issuing the **request services static-subscriber logout group *group-name*** command. You can subsequently log in a group of interfaces by issuing the **request services static-subscriber login group *group-name*** command.

No new CLI statements are required to configure the dynamic profile for static subscribers. The dynamic profile can be very simple; it is activated at login and deactivated at logout. If you do not configure a profile, then the *junos-default-profile* is automatically activated.

During a graceful Routing Engine switchover (GRES) event, active static subscribers are recovered, inactive subscribers are cleaned up, and logout continues for subscribers that were in the process of logging out.

Include the **static-subscribers** statement at the **[edit system services]** hierarchy level to configure static subscribers. Include the **traceoptions** statement at the **[edit system processes static-subscribers]** hierarchy level to configure tracing operations for static subscribers.

You can configure the access profile, dynamic profile, and authentication parameters for all static subscribers or for a particular group of static subscribers:

- To configure the access profile that triggers AAA services for the static subscriber for all static subscribers, include the **access-profile** statement at the **[edit system services static-subscribers]** hierarchy level. Alternatively, include this statement at the **[edit system services static-subscribers group *group-name*]** hierarchy level to apply the profile to a specific group and override a top-level configuration.
- To configure the dynamic profile that is instantiated when the static subscriber logs in for all static subscribers, include the **dynamic-profile** statement at the **[edit system services static-subscribers]** hierarchy level. Alternatively, include this statement at the **[edit system services static-subscribers group *group-name*]** hierarchy level to apply the profile to a specific group and override a top-level configuration. Do not specify a dynamic profile that creates a dynamic interface.
- To configure the authentication parameters that trigger an Access-Request message to AAA for all static subscribers, include the **authentication** statement at the **[edit system services static-subscribers]** hierarchy level. Alternatively, include the statement at the **[edit system services static-subscribers group *group-name*]** hierarchy level to configure authentication for a specific group and override a top-level configuration. If you do not configure authentication, then by default the interface name is modified and used as the default username for the subscriber session and the authentication request.

The configurable authentication parameters include the password and details of how the username is formed. Include the **password** statement at the **[edit system services static-subscribers authentication]** hierarchy level to configure the authentication password for all static subscribers. Alternatively, include the statement at the **[edit system services static-subscribers group *group-name* authentication]** hierarchy level to configure authentication for a specific group and override a top-level configuration.

The username that is sent to AAA for authentication must include at least one of the following attributes:

- Domain name
- User prefix
- Interface name
- Logical system name
- Routing instance name

To configure how the username is formed for all static subscribers, include the desired statements at the **[edit system services static-subscribers authentication]** hierarchy level: **domain-name**, **user-prefix**, **logical-system-name**, or **routing-instance-name**. Alternatively, include the desired statements at the **[edit system services static-subscribers group group-name authentication]** hierarchy level to configure the username for a specific group and override a top-level configuration.

If you change the authentication configuration for an existing group or for static subscribers globally, the change has no effect on existing static subscribers. The changes are applied only to any new logins that are attempted after you commit the changes.

A group configuration must specify all the interfaces that you expect to support static subscribers. Include the **interface** statement at the **[edit system services static-subscribers group group-name]** hierarchy level to specify the interfaces. This statement enables you to specify a single interface or a range of interfaces.

You must also statically configure these interfaces before any static subscribers can be supported on them. You must configure the static interfaces in the same logical system and routing instance as the group that includes the interfaces.

If you change the interfaces that are included in an existing interface group, existing static subscribers are automatically logged out and then back in when you commit the changes. However, changes made to the configuration of the interface itself have no effect on the login or logout state of the static subscriber associated with that interface.

By default, multiple subscribers are not supported on top of the same VLAN logical interface. If you want to support this behavior, then you can manage multiple subscribers on a single logical interface in one of two ways. You can either merge attributes such as firewall filters and CoS attributes for the multiple subscribers, or you can replace the current attributes with those of a new subscriber whenever a new subscriber logs into the underlying VLAN logical interface.

- To enable attribute merging for all static interfaces, include the **aggregate-clients merge** statement at the **[edit system services static-subscribers]** hierarchy level. Alternatively, include this statement at the **[edit system services static-subscribers group group-name]** hierarchy level to enable attribute merging for a specific group of static interfaces and override a top-level configuration.
- To enable attribute replacement for all static interfaces, include the **aggregate-clients replace** statement at the **[edit system services static-subscribers]** hierarchy level.

Alternatively, include this statement at the **[edit system services static-subscribers group group-name]** hierarchy level to enable attribute replacement for a specific group of static interfaces and override a top-level configuration.

- Related Documentation**
- [Configuring Subscribers over Static Interfaces on page 288](#)
  - [Juniper Networks Session and Resource Control \(SRC\) and JSRC Overview on page 271](#)
  - [Understanding JSRC-SAE Interactions on page 276](#)

## CHAPTER 23

# Configuring Subscribers over Static Interfaces

- Configuring Subscribers over Static Interfaces on page 288
- Specifying the Static Subscriber Global Access Profile on page 289
- Specifying the Static Subscriber Global Dynamic Profile on page 289
- Enabling Multiple Subscribers on a VLAN Logical Interface for All Static Subscribers on page 290
- Configuring the Static Subscriber Global Authentication Password on page 290
- Configuring the Static Subscriber Global Username on page 291
- Creating a Static Subscriber Group on page 292
- Specifying the Static Subscriber Group Access Profile on page 293
- Specifying the Static Subscriber Group Dynamic Profile on page 293
- Enabling Multiple Subscribers on a VLAN Logical Interface for a Static Subscriber Group on page 294
- Configuring the Static Subscriber Group Authentication Password on page 294
- Configuring the Static Subscriber Group Username on page 295
- Forcing a Static Subscriber to Be Logged Out on page 296
- Resetting the State of an Interface for Static Subscriber Login on page 296
- Forcing a Group of Static Subscribers to Be Logged Out on page 296
- Resetting the State of an Interface Group for Static Subscriber Login on page 296
- Tracing Static Subscriber Operations on page 297
- Configuring the Static Subscribers Trace Log Filename on page 298
- Configuring the Number and Size of Static Subscribers Log Files on page 298
- Configuring Access to the Static Subscribers Log File on page 298
- Configuring a Regular Expression for Static Subscriber Lines to Be Logged on page 299
- Configuring the Static Subscribers Tracing Flags on page 299

## Configuring Subscribers over Static Interfaces

---

This topic describes the procedure for configuring subscribers over static interfaces (static subscribers).

Before you configure subscribers over static interfaces, perform the following tasks:

- Configure the static interfaces on which you want to create and manage subscribers.
- Create an access profile to trigger AAA services for static subscribers.
- Create a dynamic profile that is instantiated when static subscribers log in.

To configure static subscribers:

1. Specify the global access profile that triggers AAA services for static subscribers.  
See “Specifying the Static Subscriber Global Access Profile” on page 289.
2. Specify the global dynamic profile that is instantiated when static subscribers log in.  
See “Specifying the Static Subscriber Global Dynamic Profile” on page 289.
3. Configure global method to handle multiple subscribers on a VLAN Logical Interface.  
See “Enabling Multiple Subscribers on a VLAN Logical Interface for All Static Subscribers” on page 290
4. Configure the global authentication password for static subscribers.  
See “Configuring the Static Subscriber Global Authentication Password” on page 290.
5. Configure the global username for static subscribers.  
See “Configuring the Static Subscriber Global Username” on page 291.
6. Configure a group of subscribers to share values different from the global configuration.  
See “Creating a Static Subscriber Group” on page 292.
7. Specify the access profile for the static subscriber group.  
See “Specifying the Static Subscriber Group Access Profile” on page 293.
8. Specify the dynamic profile for the static subscriber group.  
See “Specifying the Static Subscriber Group Dynamic Profile” on page 293.
9. Configure method to handle multiple subscribers on a VLAN Logical Interface for a static subscriber group.  
See “Enabling Multiple Subscribers on a VLAN Logical Interface for a Static Subscriber Group” on page 294.
10. Configure the authentication password for the static subscriber group.  
See “Configuring the Static Subscriber Group Authentication Password” on page 294.
11. Configure the username for the static subscriber group.  
See “Configuring the Static Subscriber Group Username” on page 295.

12. (Optional) Force a static subscriber to be logged out from an interface.  
See “Forcing a Static Subscriber to Be Logged Out” on page 296.
13. (Optional) Enable an interface to accept static subscriber logins.  
See “Resetting the State of an Interface for Static Subscriber Login” on page 296.
14. (Optional) Force static subscribers to be logged out from a group of interfaces.  
See “Forcing a Group of Static Subscribers to Be Logged Out” on page 296.
15. (Optional) Enable a group of interfaces to accept static subscriber logins.  
See “Resetting the State of an Interface Group for Static Subscriber Login” on page 296.
16. Configure trace options for troubleshooting the configuration.  
See “Tracing Static Subscriber Operations” on page 297.

**Related  
Documentation**

- Subscribers on Static Interfaces Overview on page 283
- [edit system services static-subscribers] Hierarchy Level on page 832

---

## Specifying the Static Subscriber Global Access Profile

You specify a previously created access profile that triggers AAA services for all static subscribers. This value can be overridden for a group of static subscribers when a different profile is configured for that group.

To specify the access profile used for all static subscribers:

- Specify the profile name.  

```
[edit system services static-subscribers]  
user@host# set access-profile access5
```

**Related  
Documentation**

- Configuring Subscribers over Static Interfaces on page 288
- Specifying the Static Subscriber Group Access Profile on page 293
- **profile on page 1127**

---

## Specifying the Static Subscriber Global Dynamic Profile

You specify a previously created dynamic profile that is instantiated when a static subscriber logs in. This profile is used for all static subscribers. This value can be overridden for a group of static subscribers when a different profile is configured for that group.

To specify the dynamic profile used for all static subscribers:

- Specify the profile name.  

```
[edit system services static-subscribers]  
user@host# set dynamic-profile dyn-profile-1
```

- Related Documentation**
- [Configuring Subscribers over Static Interfaces on page 288](#)
  - [Specifying the Static Subscriber Group Dynamic Profile on page 293](#)
  - [dynamic-profiles on page 943](#)

---

## Enabling Multiple Subscribers on a VLAN Logical Interface for All Static Subscribers

For a given interface, only a single static subscriber (or group) is logged in. Although we do not recommend this practice, you might have other kinds of subscribers configured on the same interface, such as a DHCP subscriber managed by the DHCP application. You can use the **aggregate-clients** statement to extend the dynamic profile for all static subscribers to enable multiple subscribers to share the same VLAN logical interface.

You can specify that attributes (such as CoS or firewall) for the multiple subscribers are merged for the logical interface. That is, the profiles for multiple subscribers of different types are instantiated on the interface, but the profile attributes of each are merged together. Alternatively, you can specify that the instantiated profile for the current subscriber is replaced by the profile of a new subscriber that logs in using the same logical interface. This configuration can be overridden for a group of static subscribers when a different configuration is applied for that group.

To enable multiple subscribers to share the same VLAN logical interface for all static subscribers, do one of the following:

- Specify that the multiple subscriber attributes are merged for the logical interface.

```
[edit system services static-subscribers dynamic-profile dyn-profile-1]  
user@host# set aggregate-clients merge
```

- Specify that the entire logical interface is replaced when a new subscriber logs into the network using the same VLAN logical interface.

```
[edit system services static-subscribers dynamic-profile dyn-profile-3]  
user@host# set aggregate-clients replace
```

- Related Documentation**
- [Configuring Subscribers over Static Interfaces on page 288](#)
  - [Specifying the Static Subscriber Group Dynamic Profile on page 293](#)
  - [dynamic-profile on page 942](#)

---

## Configuring the Static Subscriber Global Authentication Password

You configure a password that is included in the Access-Request message sent to AAA to authenticate all static subscribers. This value can be overridden for a group of static subscribers when a different password is configured for that group.

To specify the authentication password used for all static subscribers:

- Specify the password.

```
[edit system services static-subscribers authentication]
```



```
user@host# set password Gj85*3mS
```

#### Related Documentation

- Configuring Subscribers over Static Interfaces on page 288
- Configuring the Static Subscriber Group Authentication Password on page 294
- authentication on page 870

## Configuring the Static Subscriber Global Username

You configure how the username is formed. The username serves as the username for all static subscribers that are created and is included in the Access-Request message sent to AAA to authenticate all static subscribers. This value can be overridden for a group of static subscribers when a different username is configured for that group.

The username must include at least one of the five possible elements. The value of each element is concatenated in a specific order; the resulting string is the username. If you specify their inclusion, the interface name, logical system name, and routing instance name are derived from the configuration context. The elements are ordered as follows:

***user-prefix.interface.logical-system-name.routing-instance-name@domain-name***

To configure the username for all static subscribers:

1. (Optional) Specify a prefix for the username.

```
[edit system services static-subscribers authentication username-include]
user@host# set user-prefix Building5
```

2. (Optional) Specify that the interface name is included in the username.

```
[edit system services static-subscribers authentication username-include]
user@host# set interface
```

3. (Optional) Specify that the logical system name is included in the username.

```
[edit system services static-subscribers authentication username-include]
user@host# set logical-system-name
```

4. Specify that the routing instance name is included in the username.

```
[edit system services static-subscribers authentication username-include]
user@host# set routing-instance-name
```

5. Specify the domain name included in the username.

```
[edit system services static-subscribers authentication username-include]
user@host# set domain-name campus.example.com
```

Configured in the default logical system and master routing instance for interface ge-0/1/1.100, this sample configuration generates the following username:

**Building5.ge-0-1-1-100.default.master.campus.example.com**

#### Related Documentation

- Configuring Subscribers over Static Interfaces on page 288
- Configuring the Static Subscriber Group Username on page 295

- [username-include on page 1270](#)

## Creating a Static Subscriber Group

---

You can override the configuration that is applied globally to static subscribers by creating a static subscriber group that consists of a set of statically configured interfaces. You can then apply a common configuration for the group with values different from the global values for access and dynamic profiles, password, and username.

To configure an interface group for static subscribers:

1. Access the **[edit system services static-subscribers]** hierarchy level.
2. Create the group and assign the name.

```
[edit system services static-subscribers]
user@host# edit group boston
```

3. Specify the names of one or more interfaces on which static subscribers can be created. 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 static-subscribers group boston]
user@host# set interface ge-1/0/1.1
user@host# set interface ge-1/0/1.2
```

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

```
[edit system services static-subscribers group boston]
user@host# set interface ge-1/0/1.3 upto ge-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 static-subscribers group boston]
user@host# set interface ge-1/0/1.1 upto ge-1/0/1.102
user@host# set interface ge-1/0/1.6 exclude
user@host# set interface ge-1/0/1.70 upto ge-1/0/1.80 exclude
```

### Related Documentation

- [Configuring Subscribers over Static Interfaces on page 288](#)
- [Specifying the Static Subscriber Group Access Profile on page 293](#)
- [Specifying the Static Subscriber Group Dynamic Profile on page 293](#)
- [Configuring the Static Subscriber Group Authentication Password on page 294](#)
- [Configuring the Static Subscriber Group Username on page 295](#)

## Specifying the Static Subscriber Group Access Profile

---

You can override the configured global access profile by specifying a different profile for a group of static subscribers. The access profile triggers AAA services for that group of static subscribers.

To specify the access profile used for a group of static subscribers:

- Specify the profile name.

```
[edit system services static-subscribers group boston]  
user@host# set access-profile boston-ac
```

### Related Documentation

- Configuring Subscribers over Static Interfaces on page 288
- **profile on page 1127**

## Specifying the Static Subscriber Group Dynamic Profile

---

You can override the configured global dynamic profile by specifying a different profile for a group of static subscribers. The dynamic profile is instantiated when any static subscriber in the group logs in.

To specify the dynamic profile used for a group of static subscribers:

- Specify the profile name.

```
[edit system services static-subscribers group boston]  
user@host# set dynamic-profile dyn-profile-2
```

### Related Documentation

- Configuring Subscribers over Static Interfaces on page 288
- Specifying the Static Subscriber Global Dynamic Profile on page 289
- **dynamic-profiles on page 943**

## Enabling Multiple Subscribers on a VLAN Logical Interface for a Static Subscriber Group

For a given interface, only a single static subscriber group (or static subscriber) is logged in. Although we do not recommend this practice, you might have other kinds of subscribers configured on the same interface, such as a DHCP subscriber managed by the DHCP application. You can use the **aggregate-clients** statement to extend the dynamic profile for a static subscriber group to enable multiple subscribers to share the same VLAN logical interface.

You can specify that attributes (such as CoS or firewall) for the multiple subscribers are merged for the logical interface. That is, the profiles for multiple subscribers of different types are instantiated on the interface, but the profile attributes of each are merged together. Alternatively, you can specify that the instantiated profile for the current subscriber group is replaced by the profile of a new subscriber that logs in using the same logical interface. This configuration overrides the configuration applied to all static subscribers that are not members of the group.

To enable multiple subscribers to share the same VLAN logical interface for a static subscriber group, do one of the following:

- Specify that the multiple subscriber attributes are merged for the logical interface.

```
[edit system services static-subscribers group boston dynamic-profile dyn-profile-2]  
user@host# set aggregate-clients merge
```

- Specify that the entire logical interface is replaced when a new subscriber logs into the network using the same VLAN logical interface.

```
[edit system services static-subscribers group boston dynamic-profile dyn-profile-4]  
user@host# set aggregate-clients replace
```

### Related Documentation

- Configuring Subscribers over Static Interfaces on page 288
- Specifying the Static Subscriber Group Dynamic Profile on page 293
- **dynamic-profile** on page 942

## Configuring the Static Subscriber Group Authentication Password

You can override the configured global authentication password by specifying a different password for a group of static subscribers. This password is included in the Access-Request message sent to AAA to authenticate all static subscribers in the group.

To specify the authentication password used for a group of static subscribers:

- Specify the password.

```
[edit system services static-subscribers group boston authentication]  
user@host# set password knTS$Sk2
```

### Related Documentation

- Configuring Subscribers over Static Interfaces on page 288

- Configuring the Static Subscriber Global Authentication Password on page 290
- **authentication on page 870**

## Configuring the Static Subscriber Group Username

You can override the configured global username by specifying a different username for a group of static subscribers. The username serves as the username for a group of static subscribers that is created and is included in the Access-Request message sent to AAA to authenticate that group.

The username must include at least one of the five possible elements. The value of each element is concatenated in a specific order; the resulting string is the username. If you specify their inclusion, the interface name, logical system name, and routing instance name are derived from the configuration context. The elements are ordered as follows:

***user-prefix.interface.logical-system-name.routing-instance-name@domain-name***

To configure the username for a group of static subscribers:

1. (Optional) Specify a prefix for the username.

```
[edit system services static-subscribers group boston authentication username-include]
user@host# set user-prefix 2ndFloor
```

2. (Optional) Specify that the interface name is included in the username.

```
[edit system services static-subscribers group boston authentication username-include]
user@host# set interface
```

3. (Optional) Specify that the logical system name is included in the username.

```
[edit system services static-subscribers group boston authentication username-include]
user@host# set logical-system-name
```

4. Specify that the routing instance name is included in the username.

```
[edit system services static-subscribers group boston authentication username-include]
user@host# set routing-instance-name
```

5. Specify the domain name included in the username.

```
[edit system services static-subscribers group boston authentication username-include]
user@host# set domain-name building5.example.com
```

Configured in the default logical system and master routing instance for interface ge-0/1/2.50, this sample configuration generates the following username:

**2ndfloor.ge-0-1-2-50.default.master.building5.example.com**

### Related Documentation

- Configuring Subscribers over Static Interfaces on page 288
- Configuring the Static Subscriber Global Username on page 291
- **username-include on page 1270**

## Forcing a Static Subscriber to Be Logged Out

---

You can force a static subscriber to be logged out on an interface. After you do so, no subscriber can subsequently log in on that interface until the interface state is reset either by a router reset or by entering the **request services static-subscribers login interface** command.

- To forcibly log out a static subscriber on a static interface:

```
user@host> request services static-subscribers logout interface ge-2/0/1.5
```

### Related Documentation

- Resetting the State of an Interface for Static Subscriber Login on page 296

## Resetting the State of an Interface for Static Subscriber Login

---

When a static subscriber has been forcibly logged out on an interface with the **request services static-subscribers logout interface** command, you can reset the state of the interface. This action enables a static subscriber to log in on the interface. If you do not reset the state manually, then no static subscribers can log in on the interface until the state is reset by a router reset.

- To reset the state of a static interface:

```
user@host> request services static-subscribers login interface ge-2/0/1.5
```

### Related Documentation

- Forcing a Static Subscriber to Be Logged Out on page 296

## Forcing a Group of Static Subscribers to Be Logged Out

---

You can force the static subscribers on all interfaces in a group to be logged out. After you do so, no subscriber can subsequently log in on an interface in that group until the interface state is reset either by a router reset or by entering the **request services static-subscribers login group** command.

- To forcibly log out all static subscribers on a static interface group:

```
user@host> request services static-subscribers logout group boston
```

### Related Documentation

- Resetting the State of an Interface Group for Static Subscriber Login on page 296

## Resetting the State of an Interface Group for Static Subscriber Login

---

When static subscribers have been forcibly logged out on an interface group with the **request services static-subscribers logout group** command, you can reset the state of the group. This action enables static subscribers to log in on the interfaces in the group. If you do not reset the state manually, then no static subscribers can log in on any interface in the group until the state is reset by a router reset.

- To reset the state of a static interface group:

```
user@host> request services static-subscribers login group boston
```

**Related  
Documentation**

- Forcing a Group of Static Subscribers to Be Logged Out on page 296

## Tracing Static Subscriber Operations

The Junos OS trace feature tracks static subscriber operations and records events 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 **jsscd** located in the **/var/log** directory. You cannot change the directory (**/var/log**) in which trace files are located.
2. When the file **jsscd** reaches 128 kilobytes (KB), it is renamed **jsscd.0**, then **jsscd.1**, and finally **jsscd.2**, until there are three trace files. Then the oldest trace file (**jsscd.2**) is overwritten.

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

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To configure static subscriber tracing operations:

1. (Optional) Configure a trace log filename.  
See “Configuring the Static Subscribers Trace Log Filename” on page 298.
2. (Optional) Configure the number and size of trace logs.  
See “Configuring the Number and Size of Static Subscribers Log Files” on page 298.
3. (Optional) Configure user access to trace logs.  
See a “Configuring Access to the Static Subscribers Log File” on page 298.
4. (Optional) Configure a regular expression to filter the information to be included in the trace log.  
See “Configuring a Regular Expression for Static Subscriber Lines to Be Logged” on page 299.
5. (Optional) Configure flags to specify which events are logged.  
See “Configuring the Static Subscribers Tracing Flags” on page 299.

Related  
Documentation

## Configuring the Static Subscribers Trace Log Filename

---

By default, the name of the file that records trace output for static subscribers is **jsscd**. You can specify a different name with the **file** option.

To configure the filename for static subscribers tracing operations:

- Specify the name of the file used for the trace output.  

```
[edit system processes static-subscribers traceoptions]  
user@host# set file stat-subs_1
```

Related  
Documentation

- Tracing Static Subscriber Operations on page 297
- traceoptions on page 1234

## Configuring the Number and Size of Static Subscribers Log Files

---

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

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

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.  

```
[edit system processes static-subscribers traceoptions]  
user@host# set file stat-subs_1 _logfile_1 files 20 size 2097152
```

Related  
Documentation

- Tracing Static Subscriber Operations on page 297
- traceoptions on page 1234

## Configuring Access to the Static Subscribers Log File

---

By default, only the user who configures the tracing operation can access the log files. 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 system processes static-subscribers traceoptions]
user@host# set file stat-subs_1 _logfile_1 world-readable
```

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

- Configure the log file to be no-world-readable.

```
[edit system processes static-subscribers traceoptions]
user@host# set file stat-subs_1 _logfile_1 no-world-readable
```

#### Related Documentation

- Tracing Static Subscriber Operations on page 297
- [traceoptions on page 1234](#)

## Configuring a Regular Expression for Static Subscriber 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 to be matched.

To configure regular expressions to be matched:

- Configure the regular expression.

```
[edit system processes static-subscribers traceoptions]
user@host# set file stat-subs_1 _logfile match regex
```

#### Related Documentation

- Tracing Static Subscriber Operations on page 297
- [traceoptions on page 1234](#)

## Configuring the Static Subscribers 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
<b>all</b>	Trace all operations
<b>authentication</b>	Trace authentication events
<b>configuration</b>	Trace configuration events
<b>database</b>	Trace database events

Flag	Description
<b>general</b>	Trace general flow.
<b>gres</b>	Trace GRES events
<b>profile</b>	Trace dynamic profile events
<b>rtsock</b>	Trace routing socket events
<b>statistics</b>	Trace statistics events
<b>subscriber</b>	Trace subscriber events

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit system processes static-subscribers traceoptions]  
user@host# set flag authentication
```

**Related  
Documentation**

- [Tracing Static Subscriber Operations on page 297](#)
- [traceoptions on page 1234](#)

# Static Subscribers for Subscriber Access Examples

- Example: Configuring Static Subscribers for Subscriber Access on page 301

## Example: Configuring Static Subscribers for Subscriber Access

---

This example shows a static subscriber configuration.

1. Configure the access profile to be used for static subscribers.

```
access {  
  profile access5 {  
    provisioning-order jsr;  
    accounting {  
      order radius;  
    }  
    authentication {  
      order radius;  
    }  
  }  
}
```

2. Configure the dynamic profile to be used for static subscribers.

If you do not configure this profile, the default profile, junos-default-profile, is used.

3. Configure the static interfaces on which to layer the static subscribers.
4. Configure the parameters that apply globally to all static subscribers in the configuration context.

```
static-subscribers {  
  access-profile access5;  
  dynamic-profile dyn-profile-1;  
  authentication {  
    password Gj85*3mS;  
    username-include {  
      user-prefix Building5;  
      interface;  
      logical-system-name;  
      routing-instance-name;  
      domain-name example.com;  
    }  
  }  
}
```

```
    }  
  }
```

5. If you want to override the global parameters for certain static subscribers, create a group of static interfaces for those subscribers and configure parameters to apply to that group. Repeat this step for as many groups as you need.

```
static-subscribers {  
  group boston {  
    interface ge-1/0/1.1 upto ge-1/0/1.102  
    interface ge-1/0/1.6 exclude  
    interface ge-1/0/1.70 upto ge-1/0/1.80 exclude  
    access-profile boston-ac;  
    dynamic-profile dyn-profile-2;  
    authentication {  
      password knTS$$k2;  
      username-include {  
        user-prefix 2ndFloor;  
        interface;  
        logical-system-name;  
        routing-instance-name;  
        domain-name example.net;  
      }  
    }  
  }  
}
```

6. Configure tracing options for static subscriber events.

```
static-subscribers {  
  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;  
  }  
}
```

## CHAPTER 25

# PTSP and Juniper Networks Session and Resource Control (SRC)

- PTSP Overview on page 303
- Juniper Networks Session and Resource Control (SRC) and PTSP Overview on page 304
- Packet-Triggered Subscribers Services Overview on page 309

### PTSP Overview

---

The packet-triggered subscribers and policy control (PTSP) feature allows the application of policies to individual source IP addresses flowing through a given interface. A subscriber context is created for each distinct source IP address seen in a given underlying interface. This feature can be used to support dynamic subscribers that are controlled by a subscriber termination device, such as a B-RAS or GGSN device, that is connected to an MX Series 3D Universal Edge Router.

PTSP has the following responsibilities:

- Create a subscriber context for each distinct IPv4 address on a given interface (subscriber context).
- Apply policies to or remove policies from the subscriber context.
- Collect statistics and report for each individual policy for each subscriber context.
- Derive information about subscribers.

You can associate specific subscriber contexts based on IPv4 addresses and provide service activation and deactivation for these subscribers. The Multiservices DPC (MS-DPC) maintains a table of addresses for each subscriber and any corresponding policies. If an address is not found in the subscriber table, then a new subscriber context is created. All policies are defined on a per-subscriber basis. Once the subscribers are present in the subscriber table, PTSP enforces the policies active for the subscriber context. PTSP can report the subscribers to the SAE using the Diameter protocol so that the SRC software can manage the subscribers and services with dynamic policies. You can also configure static policies, but dynamic policies take precedence over static policies. When you download a new dynamic policy, it takes effect only for new flows. All new flows and TCP connections use the new dynamic policy. Existing flows are not affected by the new policy unless they timeout, after which they are considered a new flow.

Statistics collection that is aggregated on a service rule basis is also shared with the SAE using the Diameter application. These statistics are not written to a flat file. Statistics collection that is aggregated on an application or application group basis is written to a flat file. These statistics are not shared with the SAE using the Diameter protocol.

## Hardware Requirements for PTSP for Subscriber Access

PTSP is supported on Juniper Networks MX Series 3D Universal Edge Routers. You must have a Multiservices DPC (MS-DPC) on the MX Series router.

**Related Documentation**

- Configuring PTSP on page 317

## Juniper Networks Session and Resource Control (SRC) and PTSP Overview

The Juniper Networks Session and Resource Control (SRC) environment provides a central administrative point for managing subscribers and their services. The SRC software runs on Juniper Networks C Series Controllers. The SRC software uses the Diameter protocol for communications between the local peer on a Juniper Networks routing platform and the remote SRC peer on a C Series Controller. The local peer is known as PTSP and is part of the AAA application. The remote SRC peer is the service activation engine (SAE); the SAE acts as the controlling agent in the SRC environment.

The SRC software enables the SAE to activate and deactivate subscriber services (described by SRC policies). The SAE installs or removes policies using a service rule policy template called `_svc_rule_`. This policy template indicates which policy is applied to a new subscriber session. Additional policies are bound to new sessions; they do not affect existing sessions. Note that policy name must be unique between PPR requests. You can use the same rule name within a single request, but you cannot use the same name again in a separate request.

Statistics collection that is aggregated on a service rule basis is also shared with the SAE using the Diameter protocol.



**NOTE:** More than one Diameter-based application (function) can run on a router simultaneously.

## Diameter Messages Exchanged by PTSP and the SAE

The PTSP application is a Juniper Networks Diameter application registered with the IANA (<http://www.iana.org>) as Juniper JGx, with an ID of 16777273. PTSP and the SAE communicate by exchanging the Diameter messages described in Table 34 on page 304.

**Table 34: Diameter Messages Used by PTSP and the SAE**

Diameter Message	Code	Description
AA-Request (AAR)	265	Request from PTSP to the SAE at new subscriber login or during SAE-PTSP synchronization. The request can be one of three types: address-authorization, provisioning-request, or synchronization.

**Table 34: Diameter Messages Used by PTSP and the SAE (*continued*)**

Diameter Message	Code	Description
AA-Answer (AAA)	265	Response from the SAE to the PTSP AA-Request message.
Accounting-Request (ACR)	271	Request from the SAE to PTSP or from PTSP to the SAE for statistics.
Accounting-Answer (ACA)	271	Response to the ACR message to provide statistics for each installed policy.
Abort-Session-Request (ASR)	274	Request from the SAE to PTSP to log out a subscriber.
Abort-Session-Answer (ASA)	274	Response from PTSP to the SAE ASR message. Includes success or failure notification for the logout request.
Push-Profile-Request (PPR)	288	Request from the SAE to PTSP to activate or deactivate services for a subscriber.
Push-Profile-Answer (PPA)	288	Response from PTSP to the SAE PPR message. Includes success or failure notification for the service activation or deactivation commands in the request.
Session-Resource-Query (SRQ)	277	Request from PTSP to the SAE or from the SAE to PTSP to initiate synchronization between PTSP and the SAE.
Session-Resource-Reply (SRR)	277	Response to the SRQ message to begin synchronization.
Session-Termination-Request (STR)	275	Notification from PTSP to the SAE that a provisioned subscriber has logged out.
Session-Termination-Answer (STA)	275	Response from the SAE to the PTSP STR message. Includes success or failure notification.

## Understanding Diameter AVPs for PTSP

Diameter conveys information by including various attribute-value pairs (AVPs) in Diameter messages. Table 35 on page 305 lists the standard Diameter AVPs used in PTSP interactions.

**Table 35: Standard Diameter AVPs for PTSP**

Code Number	Diameter AVP	Description	Type
263	Session-Id	Specifies the subscriber session identifier. For a packet-triggered subscriber managed by AAA, the value is assigned by PTSP to uniquely identify the subscriber session.	UTF8String

Table 35: Standard Diameter AVPs for PTSP (*continued*)

Code Number	Diameter AVP	Description	Type
268	Result-Code	<p>Indicates whether a request completed successfully. Provides an error code if the request failed.</p> <p>The following classes are recognized by Diameter:</p> <ul style="list-style-type: none"> <li>• 1xxx—Informational</li> <li>• 2xxx—Success</li> <li>• 3xxx—Protocol errors</li> <li>• 4xxx—Transient errors</li> <li>• 5xxx—Permanent failures</li> </ul> <p>Unrecognized classes, which begin with numerals 6–9 or 0, are handled as permanent failures.</p> <p>PTSP supports the following values; all non-success values are treated as permanent failures:</p> <ul style="list-style-type: none"> <li>• 1001—DIAMETER_MULTI_ROUND_AUTH</li> <li>• 2001—DIAMETER_SUCCESS</li> <li>• 5002—DIAMETER_UNKNOWN_SESSION_ID</li> <li>• 5012—DIAMETER_UNABLE_TO_COMPLY</li> </ul>	Unsigned32
277	Auth-Session-State	<p>Indicates whether AAA session state is maintained.</p> <ul style="list-style-type: none"> <li>• 0—STATE_MAINTAINED</li> <li>• 1—NO_STATE_MAINTAINED</li> </ul>	Enumerated
295	Termination-Cause	<p>Indicates the reason why a session was terminated on the access device.</p> <ul style="list-style-type: none"> <li>• 1—DIAMETER_LOGOUT</li> <li>• 2—DIAMETER_SERVICE_NOT_PROVIDED</li> <li>• 3—DIAMETER_BAD_ANSWER</li> <li>• 4—DIAMETER_ADMINISTRATIVE</li> <li>• 5—DIAMETER_LINK_BROKEN</li> <li>• 6—DIAMETER_AUTH_EXPIRED</li> <li>• 7—DIAMETER_USER_MOVED</li> <li>• 8—DIAMETER_SESSION_TIMEOUT</li> </ul>	Enumerated

Juniper Networks AVPs are used in addition to the standard Diameter AVPs. These AVPs have an enterprise number of 2636. Table 36 on page 306 lists the Juniper Networks AVPs used in PTSP interactions.

Table 36: Juniper Networks Diameter AVPs

Code Number	Diameter AVP	Description	Type
2020	Juniper-Policy-Install	<p>Specifies policies to be activated for the subscriber.</p> <p>Includes Juniper-Policy-Name and Juniper-Policy-Definition.</p>	Grouped



Table 36: Juniper Networks Diameter AVPs (*continued*)

Code Number	Diameter AVP	Description	Type
2021	Juniper-Policy-Name	Defines the name of a policy decision.	OctetString
2022	Juniper-Policy-Definition	Defines a policy decision. Includes Juniper-Policy-Name, Juniper-Template-Name, and Juniper-Substitution.	Grouped
2023	Juniper-Template-Name	Profile name defined by the router. PTSP only supports the <code>_svc_rule_</code> policy template.	UTF8String
2024	Juniper-Substitution	Defines the substitution attributes. Includes Juniper-Substitution-Name and Juniper-Substitution-Value.	OctetString
2025	Juniper-Substitution-Name	Defines the name of the variable to be replaced.	OctetString
2026	Juniper-Substitution-Value	Defines the value of the variable to be replaced.	OctetString
2027	Juniper-Policy-Remove	Specifies policies to be deactivated for the subscriber. Includes Juniper-Policy-Name.	Grouped
2035	Juniper-Policy-Failed	Specifies the name of the policy activation or deactivation that failed.	OctetString
2038	Juniper-Policy-Success	Specifies the name of the policy activation or deactivation that succeeded.	OctetString
2046	Juniper-Logical-System	Specifies the logical system.	UTF8String
2047	Juniper-Routing-Instance	Specifies the routing instance.	UTF8String
2048	Juniper-Jsrc-Partition	Specifies the logical system and routing instance for the subscriber or request. Includes Juniper-Logical-System and Juniper-Routing-Instance.	Grouped
2050	Juniper-Request-Type	Describes the type of request: <ul style="list-style-type: none"> <li>1—ADDRESS_AUTHORIZATION</li> <li>2—PROVISIONING_REQUEST</li> <li>3—SYNCHRONIZATION</li> </ul>	Enumerated
2051	Juniper-Synchronization-Type	Describes the type of synchronization: <ul style="list-style-type: none"> <li>1—FULL-SYNC</li> <li>2—FAST-SYNC</li> <li>3—NO-STATE-TO-SYNC</li> </ul>	Enumerated
2052	Juniper-Synchronization	Describes the state of synchronization: <ul style="list-style-type: none"> <li>1—NO-SYNC; this is the default state</li> <li>2—SYNC-IN-PROGRESS</li> <li>3—SYNC-COMPLETE</li> </ul>	Enumerated

Table 36: Juniper Networks Diameter AVPs (*continued*)

Code Number	Diameter AVP	Description	Type
2053	Juniper-Acct-Record	Statistics data for each policy installed for this subscriber. Includes Juniper-Policy-Name.	Grouped

## Understanding PTSP-SAE Interactions

This topic describes the sequences of Diameter messages exchanged between PTSP and the SAE as they interact to perform the following tasks for subscriber access:

- Subscriber login

When a packet-triggered subscriber logs in, PTSP sends a Diameter AA-Request message to request service provisioning from the SAE that includes the Session-Id attribute for the new subscriber. If the AA-Request fails, then the subscriber is not considered logged in and the subscriber session is not managed by the SAE. Only the static PTSP rules apply to the subscriber.

The SAE returns a Diameter AA-Answer message with the Result-Code. The AA-Answer message can include the Juniper-Policy-Install AVP (AVP code 2020), which is used to specify a service to attach to the subscriber's IP address.

PTSP can send an AA-Request message to the SAE to confirm activation. The SAE returns a AA-Answer message in acknowledgment. If the AA-Request message fails or the SAE does not respond with an AA-Answer message, the subscriber session is managed by the SAE.

- Service activation and deactivation

The SAE policies provision subscriber services. After a packet-triggered subscriber is logged in, the SAE can send a PPR message to PTSP to activate or deactivate services. A given PPR can include the Juniper-Policy-Install AVP (AVP code 2020) to activate a service or the Juniper-Policy-Remove AVP (AVP code 2027) to deactivate a service.

PTSP sends a PPA message to the SAE when it has completed the tasks requested in the PPR. The PPA indicates the success or failure of the actions requested in the PPR.

- Resynchronization

Either PTSP or the SAE initiates the resynchronization.

The SAE initiates resynchronization at startup or when a backup SAE takes over session control due to resource limits or conditions on the primary SAE. The SAE clears its database of all entries in preparation for the synchronization.

PTSP initiates resynchronization at startup, such as when AAA starts or restarts. PTSP uses the Juniper-Last-Origin-Host AVP (AVP code 2055) to keep track of the active SAE host in a multi-SAE environment. When an SAE in a multi-SAE environment becomes active, it must send an SRQ to PTSP as its first message. PTSP initiates a synchronization when it receives any other message type from an SAE that is different from the SAE indicated in the Juniper-Last-Origin-Host AVP.

Both entities initiate a resynchronization by sending an SRQ message. The recipient responds with an SRR message.

- Statistics collection and reporting per service rule

Statistics information can be sent from the router to the SAE or from the SAE to the router. Both the Diameter Accounting-Request and Accounting-Answer messages include the Juniper-Acct-Record AVP (AVP code 2053) which identifies the policy for which accounting information is requested.

- Subscriber logout

PTSP can determine when there is a logout request for a packet-triggered subscriber in two ways:

- The SAE terminates a subscriber session by sending an ASR message to PTSP.
- PTSP monitors a subscriber session and starts the logout process after 30 minutes of inactivity.

The subscriber logout triggers the final statistics aggregation for all policies and the removal of any policies installed by the SAE. PTSP sends an STR message that indicates the logout event to the SAE.

#### Related Documentation

- Configuring the PTSP Application on page 311
- Configuring PTSP on page 317

## Packet-Triggered Subscribers Services Overview

The packet-triggered subscribers and policy control (PTSP) feature allows the application of policies to dynamic subscribers that are controlled by a subscriber termination device. You can associate specific subscriber contexts based on IPv4 addresses and provide dynamic service activation and deactivation for these subscribers. Once the subscribers are present in the subscriber database on the router, PTSP can report the subscribers to the SAE using the PTSP application so that the SRC software can manage the subscribers and services.

PTSP policies can be downloaded dynamically from the external policy manager (such as SRC) or configured statically on the router. The PTSP policies can be configured for each distinct IPv4 source address for a given interface on which the service is configured. Each distinct IPv4 address is considered a subscriber and all PTSP policies are applied on a per-subscriber basis. Dynamic policies, which are always specific to a subscriber, take precedence over static policies.

You can set up PTSP policies to:

- Manage traffic by configuring filtering, rate-limiting, and QoS enforcement in the rules.
- Steer traffic by specifying the forwarding instance in the forward rule.
- Collect accounting information by service rule or by application.

When you configure PTSP policies, you must specify the type of statistics collection (**count**) and the IP address used to identify the packet-triggered subscriber (**demux**) in

the service rule. All service rules attached to a given service set must have the same settings for these options.

For the statistics collection type, terms and rules also cannot mix and match the following styles:

- **rule**—Statistics are aggregated in one bucket for the service rule and Diameter is used to report the statistics.
- **application**—Statistics are aggregated by application for a specific application, for a specific application group, or in one bucket. The statistics are reported in a flat file.

Subscriber instantiation is triggered for ingress packets by the IP address. When source address is specified, the source IP address of the ingress packets is used to establish the subscriber context. When destination address is specified, the destination IP address of the ingress packets is used to establish the subscriber context. If the IP address does not correspond to a known subscriber, then a new subscriber context is created to log in the packet-triggered subscriber.

The match conditions include local address, local port, remote address, and remote port. The following table describes how the **demux** value changes the IP address or port used for these terms.

Match Conditions	demux source-address		demux destination-address	
	Ingress Flows	Egress Flows	Ingress Flows	Egress Flows
<b>local-address</b>	Source address	Destination address	Destination address	Source address
<b>remote-address</b>	Destination address	Source address	Source address	Destination address
<b>local-port</b>	Source port	Destination port	Destination port	Source port
<b>remote-port</b>	Destination port	Source port	Source port	Destination port

- Related Documentation**
- Configuring PTSP on page 317
  - Configuring Static PTSP Rules on page 319

## CHAPTER 26

# Configuring the PTSP Application

- Configuring the PTSP Application on page 311
- Configuring the PTSP Partition on page 312
- Assigning the PTSP Partition on page 312
- Tracing Packet-Triggered Subscriber Operations on page 313

### Configuring the PTSP Application

---

You can configure the PTSP client application to work with the Session and Resource Control (SRC) peer to centrally manage packet-triggered subscribers and services. PTSP requests address and service authorizations from the remote SRC peer (the SAE), activates and deactivates services as specified by the SAE, logs out subscribers as specified by the SAE, and synchronizes subscriber state and service information with the SAE. The PTSP application also performs statistics collection and reporting.

To configure the PTSP application:

1. Configure the PTSP partition.  
See “Configuring the PTSP Partition” on page 312.
2. Assign the PTSP partition.  
See “Assigning the PTSP Partition” on page 312.
3. Configure statistics collection and reporting.  
See “Tracing Packet-Triggered Subscriber Operations” on page 313.

#### Related Documentation

- Juniper Networks Session and Resource Control (SRC) and PTSP Overview on page 304

## Configuring the PTSP Partition

---

PTSP works within a specific logical system:routing instance context, called a partition. The partition is configured to connect to the external policy manager.



**NOTE:** Currently, only a single partition is supported; you must configure it within the default logical system:routing instance context.

Before you configure the PTSP partition to connect to the external policy manager, perform the following task:

- Configure the Diameter instance for the remote SRC peer at the **[edit diameter]** hierarchy level. See “Configuring Diameter” on page 259.

Configuration for the PTSP partition consists of naming the partition and then associating a Diameter instance, the SAE hostname, and the SAE realm with the partition.

To configure the PTSP partition:

1. Create the partition at the **[edit system services packet-triggered-subscribers]** hierarchy level.

```
[edit system services packet-triggered-subscribers]
user@host# edit partition ptsp-default
```

2. Specify the Diameter instance for the PTSP partition.

```
[edit system services packet-triggered-subscribers partition ptsp-default]
user@host# set diameter-instance master
```

3. Configure the destination host for the PTSP partition.

```
[edit system services packet-triggered-subscribers partition ptsp-default]
user@host# set destination-host sae1
```

4. Configure the destination realm for the PTSP partition.

```
[edit system services packet-triggered-subscribers partition ptsp-default]
user@host# set destination-realm generic.example.com
```

### Related Documentation

- Configuring the PTSP Application on page 311

## Assigning the PTSP Partition

---

You must associate the PTSP partition with the logical system:routing instance.



**NOTE:** Currently, only the global logical system:routing instance, *master* logical system and default routing instance, is supported.

Before you assign the PTSP partition, perform the following task:

- Configure the PTSP partition. See “Configuring the PTSP Partition” on page 312.

To assign the PTSP partition:

- Specify the partition name at the **[edit system]** hierarchy level.

```
[edit system]
user@host# set packet-triggered-subscribers-partition ptsp-default
```

#### Related Documentation

- Configuring the PTSP Application on page 311

## Tracing Packet-Triggered Subscriber Operations

Packet-triggered subscriber tracing operations track packet-triggered subscriber operations and record them in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

All log files are located in the **/var/log** directory. You cannot change the directory (**/var/log**) in which trace files are located. When the trace file reaches its maximum size, a **.0** is appended to the filename, then a new file is created with a **.1**, and finally a **.2**. When the maximum number of trace files is reached, the oldest trace file is overwritten.

To configure packet-triggered subscriber tracing operations:

1. Specify that you want to configure tracing options.

```
[edit system services packet-triggered-subscribers]
user@host# edit traceoptions
```

2. (Optional) Configure the name for the file used for the trace output.
3. (Optional) Configure the number and size of the log files.
4. (Optional) Configure flags to filter the operations to be logged.

The packet-triggered subscriber traceoptions operations are described in the following sections:

- Configuring the Packet-Triggered Subscribers Trace Log Filename on page 313
- Configuring the Size of Packet-Triggered Subscribers Log Files on page 314
- Configuring the Packet-Triggered Subscribers Tracing Flags on page 314

### Configuring the Packet-Triggered Subscribers Trace Log Filename

By default, the name of the file that records trace output for packet-triggered subscribers is **jptspd**. You can specify a different name with the **file** option.

To configure the filename for packet-triggered subscribers tracing operations:

- Specify the name of the file used for the trace output.

```
[edit system services packet-triggered-subscribers traceoptions]
```

```
user@host# set file ptsp-subs_1
```

## Configuring the Size of Packet-Triggered Subscribers Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed *filename.0*, then *filename.1*, and finally *filename.2*, 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).

For example, you can set the maximum file size to 2 MB. 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 three trace files. Then the oldest file (*filename.2*) is overwritten by the newest file (*filename.0*).

To configure the size of trace files:

- Specify the name and size of the file used for the trace output.  

```
[edit system services packet-triggered-subscribers traceoptions]
user@host# set file ptsp-subs_1 _logfile_1 size 2097152
```

## Configuring the Packet-Triggered Subscribers 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
<b>all</b>	Trace all operations
<b>configuration</b>	Trace configuration events
<b>general</b>	Trace general flow
<b>peer</b>	Trace SRC peer events
<b>pic</b>	Trace PIC events
<b>rtsock</b>	Trace routing socket events
<b>session</b>	Trace session events

To configure the flags for the events to be logged:

- Configure the flags.  

```
[edit system services packet-triggered-subscribers traceoptions]
```



```
user@host# set flag peer
user@host# set flag session
```

**Related Documentation**

- [Configuring the PTSP Application on page 311](#)



# Configuring Packet-Triggered Subscriber Services

- Configuring PTSP on page 317
- Configuring the Multiservices DPC for PTSP on page 318
- Configuring PTSP Service Rules on page 319
- Configuring Static PTSP Rules on page 319
- Configuring PTSP Rule Sets on page 321
- Configuring PTSP Service Sets on page 322
- Configuring the PTSP Forwarding Instance on page 322
- Configuring a Statistics Profile for PTSP on page 324
- Tracing PTSP Operations on page 326
- Verifying and Managing PTSP Configuration on page 327

## Configuring PTSP

---

You can configure the packet-triggered subscribers and policy control (PTSP) feature on MX Series routers to allow the application of policies to dynamic subscribers that are controlled by a subscriber termination device, such as a B-RAS or GGSN device, connected to an MX Series router. The subscribers are associated by their IPv4 address and dynamic or static policies can be applied. Dynamic policies take precedence over static policies. When you download a new dynamic policy, it takes effect only for new flows. All new flows and TCP connections use the new dynamic policy. Existing flows are not affected by the new policy unless they timeout, after which they are considered a new flow.

To configure PTSP services on the MX Series router:

1. Configure the Multiservices DPC.  
See “Configuring the Multiservices DPC for PTSP” on page 318.
2. Configure the Diameter application to support the download of dynamic PTSP policies from the external policy manager (such as SRC). The PTSP application also provides statistics collection and reporting.  
See “Configuring the PTSP Application” on page 311.

3. Configure the static PTSP service rules.  
See “Configuring Static PTSP Rules” on page 319.
4. Configure statistics collection and reporting in a flat file.  
See “Configuring a Statistics Profile for PTSP” on page 324 and “Tracing PTSP Operations” on page 326.

**Related Documentation**

- PTSP Overview on page 303

---

## Configuring the Multiservices DPC for PTSP

To configure the Multiservices Dense Port Concentrator (MS-DPC) to support PTSP services, perform the following tasks:

- Enabling the PTSP Service Package on the Multiservices DPC on page 318
- Configuring Services Interface for PTSP on page 318

### Enabling the PTSP Service Package on the Multiservices DPC

The PTSP feature runs on the Multiservices DPC, you must enable the PTSP service package on the Multiservices DPC before you can configure the PTSP software. The name of the PTSP service package is **jservices-ptsp**.

To enable the PTSP service package:

1. Determine the FPC slot number and the PIC number of the MS-DPC on which you want to enable the PTSP service package.

```
user@host> show chassis hardware
```

In this example, the FPC slot number is 3 and the PIC number is 0.

2. Enable the **jservices-ptsp** package on the Multiservices DPC.

```
[edit chassis]
user@host# set fpc 3 pic 0 adaptive-services service-package extension-provider
package jservices-ptsp
```

### Configuring Services Interface for PTSP

To configure the services interface for PTSP:

1. Enter edit mode for the interface.

```
[edit]
user@host# edit interfaces ms-3/0/0
```

2. Configure a logical unit and specify the protocol family.

```
[edit interfaces ms-3/0/0]
user@host# set unit 0 family inet
```

- Related Documentation**
- Configuring PTSP on page 317
  - PTSP Overview on page 303

## Configuring PTSP Service Rules

---

PTSP policies can be downloaded dynamically from the external policy manager (such as SRC) or configured statically on the router. The PTSP policies can be configured for each distinct IPv4 source address for a given interface on which the service is configured. Each distinct IPv4 address is considered a subscriber and all PTSP policies are applied on a per-subscriber basis.

Dynamic policies, which are always specific to a subscriber, take precedence over static policies. When you download a new dynamic policy, it takes effect only for new flows. All new flows and TCP connections use the new dynamic policy. Existing flows are not affected by the new policy unless they timeout, after which they are considered a new flow.

To configure the PTSP policies, perform these tasks:

- To download dynamic policies and to collect statistics with Diameter, configure the Diameter application for PTSP. See “Configuring the PTSP Application” on page 311.
- To configure static policies, see “Configuring Static PTSP Rules” on page 319. To collect statistics in a flat file, see “Configuring a Statistics Profile for PTSP” on page 324.

- Related Documentation**
- Configuring PTSP on page 317
  - PTSP Overview on page 303

## Configuring Static PTSP Rules

---

You can configure the static PTSP policies on the router. If the PTSP service is configured on the underlying interface, the PTSP service enforces the policies associated with the subscriber context.

To configure static PTSP rules:

1. Specify the rule that you want to configure.

```
[edit services ptsp]  
user@host# edit rule ptspRule1
```

2. Specify the direction in which the rule match is applied.

```
[edit services ptsp rule ptspRule1]  
user@host# set match-direction input
```

3. Specify the IP address used for the subscriber context. Subscriber instantiation is always triggered for ingress packets, so this value indicates which IP address in the ingress packets for the flow is used.

```
[edit services ptsp rule ptspRule1]
```

```
user@host# set demux source-address
```

- Specify the statistics aggregation, collection, and reporting style. Terms and rules cannot mix and match different styles.

```
[edit services ptsp rule ptspRule1]
user@host# set count-type rule
```

If you specify the rule style, statistics collection is performed by the Diameter application. If you specify the application style, statistics collection is in a flat file controlled by the local policy decision function (L-PDF).

- (Optional) Specify the forward rule used for forwarding packets. See “Configuring the PTSP Forwarding Instance” on page 322.

```
[edit services ptsp rule ptspRule1]
user@host# set forward-rule forward-rule-name
```

- Configure the term precedence for the rule.

```
[edit services ptsp rule ptspRule1]
user@host# edit term 1
```

- Configure the match conditions for the term. See Table 37 on page 320.

```
[edit services ptsp rule ptspRule1 term 1]
user@host# set from remote-address-range low 203.0.0.2 high 203.0.0.100
user@host# set from remote-address-range low 204.0.0.2 high 204.0.0.253
```

- (Optional) Specify the action taken when the match conditions are met. See Table 38 on page 321.

```
[edit services ptsp rule ptspRule1 term 1]
user@host# set then count rule
user@host# set then accept
```

Table 37 on page 320 describes the match conditions for PTSP rules.

**Table 37: PTSP Match Conditions**

Match Condition	Description
<b>application-group-any</b>	Application group name defined in the application identification configuration.
<b>application-groups</b> [ <i>application-group-name</i> ]	Application group name defined in the application identification configuration.
<b>applications</b>	Application name defined in the application identification configuration.
<b>local-port-range</b> low <i>low-value</i> high <i>high-value</i>	Local port range.
<b>local-ports</b> <i>value-list</i>	Local ports.
<b>protocol</b> <i>protocol-number</i>	IP protocol number.
<b>remote-address</b> ( <i>address</i>   any-unicast)	Remote IP address. IPv4 only.

Table 37: PTSP Match Conditions (*continued*)

Match Condition	Description
<code>remote-address-range low <i>low-value</i> high <i>high-value</i></code>	Remote address range. IPv4 only.
<code>remote-port-range low <i>low-value</i> high <i>high-value</i></code>	Remote port range.
<code>remote-ports <i>value-list</i></code>	Remote ports.
<code>remote-prefix-list <i>prefix-list-name</i></code>	Prefixes in the specified list.

Table 38 on page 321 describes the actions for PTSP rules.

Table 38: PTSP Actions

Action or Action Modifier	Description
<code>accept</code>	Accept the packet.
<code>count</code>	Increment the specified counter.
<code>discard</code>	Drop the packet.
<code>forwarding-class</code>	Classify the packet into the specified forwarding class.
<code>police</code>	Rate-limit packets based on the specified policer.

#### Related Documentation

- Configuring the PTSP Forwarding Instance on page 322
- Configuring a Statistics Profile for PTSP on page 324
- Configuring PTSP on page 317
- PTSP Overview on page 303
- Packet-Triggered Subscribers Services Overview on page 309

## Configuring PTSP Rule Sets

You can define a collection of PTSP rules to determine the actions performed on packets.

To configure static PTSP rule sets:

1. Specify the rule set that you want to configure.  

```
[edit services ptsp]
user@host# edit rule-set ptspRules
```
2. Specify the rules in the order that you want them processed.  

```
[edit services ptsp rule-set ptspRules]
```

```
user@host# set rule ptspRule1
user@host# set rule ptspRule2
```

- Related Documentation**
- [Configuring Static PTSP Rules on page 319](#)

## Configuring PTSP Service Sets

---

To configure the service set for the PTSP application:

1. Configure the service set that you want to contain the PTSP service.

```
[edit services service-set ptspServiceSet]
user@host# set service-set ptspServiceSet
```

2. Specify the PTSP rules that constitute the service set that is applied to the services interface.

```
[edit services service-set ptspServiceSet]
user@host# set ptsp-rules ptsp-rule1
user@host# set ptsp-rules ptsp-rule2
```

3. Configure the services interface.

```
[edit services service-set ptspServiceSet]
user@host# set interface-service service-interface ms-3/0/0.0
```

4. Associate the service set with the underlying interface from which the subscribers originate. The service set must be applied to the interface facing the subscriber, that is, the interface with the IP address of the subscriber.

```
[edit interfaces ge-4/0/0 unit 0 family inet service]
user@host# set input service-set ptspServiceSet
user@host# set output service-set ptspServiceSet
```

- Related Documentation**
- [Configuring Static PTSP Rules on page 319](#)
  - [Configuring PTSP Rule Sets on page 321](#)

## Configuring the PTSP Forwarding Instance

---

Before you can forward PTSP traffic, perform these tasks for each forwarding instance:

1. Configure each PTSP forwarding instance as a routing instance type of forwarding.
2. Configure a firewall filter with an action that specifies the routing instance configured in Step 1.
3. Configure the unit number for the Multiservices interface that specifies the filter configured in Step 2 as the input filter.





**NOTE:** To avoid service set dependency on specific unit numbers, use the same unit number across all Multiservices interfaces where PTSP services are applied.

4. Configure the PTSP forward rule to specify the forwarding instance.



**NOTE:** When the forwarding instance action is performed on the flow, any postservice filters are not applied to the underlying interface.

If you want to forward traffic for PTSP subscribers, you must specify the forwarding instance for specific subscribers based on IP address, network, or prefix list. The match direction for forward rules is always input.

To configure the PTSP forwarding instance:

1. Specify the PTSP forward rule that you want to use when configuring a PTSP forwarding instance.

```
[edit services ptsp]
user@host# edit forward-rule ptspForward
```

2. Set the term precedence for the forward rule. Term with lowest precedence is evaluated first.

```
[edit services ptsp forward-rule ptspForward]
user@host# edit term 5
```

3. Configure the match conditions for the IP address, address range, or prefix list. See Table 39 on page 323.

```
[edit services ptsp forward-rule ptspForward term 5]
user@host# set from local-address 200.0.0.1
```

**Table 39: PTSP Forward Rule Match Conditions**

Match Condition	Description
<b>application-groups</b> [ <i>application-group-name</i> ]	Application group name defined in the application identification configuration.
<b>applications</b>	Application name defined in the application identification configuration.
<b>local-address</b> ( <i>address</i>   <i>any-unicast</i> )	Local IP address. IPv4 only.
<b>local-address-range</b> <i>low low-value high high-value</i>	Local address range. IPv4 only.
<b>local-prefix-list</b> <i>prefix-list-name</i>	Prefixes in the specified list.



**NOTE:** You can specify match conditions for applications or application groups that support application identification (APPID) services, but we do not recommend specifying the forwarding instance action when you are using these match conditions in PTSP policies. In this situation, some network topologies may route packets in a manner that causes the flow to be dropped. For example, the APPID services might forward some packets on the default routing instance while the PTSP services forward other packets in the same flow to another routing instance.

4. Configure the forwarding instance action with the routing instance name and the unit number.

```
[edit services ptsp forward-rule ptspForward term 5]  
user@host# set then forwarding-instance less-effort-ri 144
```



**NOTE:** When the forwarding instance action is performed on the flow, any postservice filters are not applied to the underlying interface.

**Related  
Documentation**

- For information about APPID services, see the [Junos OS Services Interfaces Configuration Guide](#)
- For information about forwarding instances, see the [Junos OS Routing Protocols Configuration Guide](#)

---

## Configuring a Statistics Profile for PTSP

The local policy decision function (L-PDF) enables you to configure properties for statistics output by creating a statistics profile. The statistics profile configures the files to which statistics records are exported and the format that is exported. You configure the statistics profile so that the statistics records are exported to a flat file. Flat files contain statistics that are collected for each subscriber by application or application group. The statistics in a flat file are not transmitted to the external policy manager using Diameter.

To configure a statistics profile for PTSP:

1. Specify that you want to configure a statistics profile.

```
[edit system services local-policy-decision-function]  
user@host# edit statistics
```

2. Configure the file properties used for the trace output.
3. Configure the profile properties.
4. Specify the record type.

Tasks to configure a statistics profile for PTSP are:

- Configuring the File Properties for Statistics Data Output on page 325
- Configuring the Profile Properties for Statistics Data Output on page 325
- Configuring the Record Type for Statistics Data on page 326

## Configuring the File Properties for Statistics Data Output

You configure a file to which the statistics data output is exported in a specified format.

To configure the file properties:

1. Specify the unique filename for receiving statistics data output.

```
[edit system services local-policy-decision-function statistics]
user@host# edit file ptsp
```

2. (Optional) Specify the maximum number of files that are maintained at one time and the maximum size of each file. If you configure one of these options, you also must set the other option.

```
[edit system services local-policy-decision-function statistics file ptsp]
user@host# set files 10 size 1g
```

3. Specify the interval for transferring files to archive sites.

```
[edit system services local-policy-decision-function statistics file ptsp]
user@host# set transfer-interval 60
```

4. Specify one or more URLs for archiving the files. Archiving can be done by using FTP or SCP.

```
[edit system services local-policy-decision-function statistics file ptsp]
user@host# set archive-sites "ftp://anonymous@10.227.1.114"
```

## Configuring the Profile Properties for Statistics Data Output

You can create an AACL statistics profile, which configures the statistics to collect and write to a file in the `/var/stats/aacl` directory.

To configure the profile properties:

1. Specify the name of the profile.

```
[edit system services local-policy-decision-function statistics]
user@host# edit aacl-statistics-profile ptsp
```

2. (Optional) Specify the file in the `/var/stats/aacl` directory in which statistics are collected. Enclose the name within quotation marks.

```
[edit system services local-policy-decision-function statistics aacl-statistics-profile
ptsp]
user@host# set file "pstp"
```

3. Set the interval for reporting statistics.

```
[edit system services local-policy-decision-function statistics aacl-statistics-profile
ptsp]
user@host# set report-interval 5
```

4. Set the **interim-active-only** mode for reporting statistics. This mode reports only statistics that have changed in the past report interval.

```
[edit system services local-policy-decision-function statistics aacl-statistics-profile ptsp]
user@host# set record-mode interim-active-only
```

5. Specify the statistics to be collected in the log file.

```
[edit system services local-policy-decision-function statistics aacl-statistics-profile ptsp]
user@host# set aacl-fields all-fields
```

## Configuring the Record Type for Statistics Data

You must configure the interim record type for recording the AACL statistics.

To configure the record type:

- Specify interim as the record type.

```
[edit system services local-policy-decision-function statistics]
user@host# set record-type interim
```

### Related Documentation

- Tracing PTSP Operations on page 326
- Configuring PTSP on page 317

---

## Tracing PTSP Operations

Tracing operations track L-PDF 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, no events are traced. When you enable the tracing operation, the default tracing behavior is as follows:

1. Important events are logged in a file located in the **/var/log** directory. You cannot change the directory (**/var/log**) in which trace files are located.
2. When the trace file reaches its maximum size, a **.0** is appended to the filename, then a new file is created with a **.1** appended, and so on. When the maximum number of trace files is reached, the oldest trace file 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 OS System Log Messages Reference](#).)

To customize trace file settings:

1. Specify that you want to configure tracing options.

```
[edit system services local-policy-decision-function]
user@host# edit traceoptions
```

2. Configure the filename used for the trace output.

```
[edit system services local-policy-decision-function traceoptions]
user@host# set file lpdfd
```

3. (Optional) Configure the maximum number and size of the log files. If you configure one of these options, you also must set the other option.

```
[edit system services local-policy-decision-function traceoptions]
user@host# set files 10 size 1g
```

4. (Optional) Specify flags to filter the operations to be logged. To specify more than one flag, include multiple **flag** statements.

```
[edit system services local-policy-decision-function traceoptions]
user@host# set flag ptsp-statistics
```

The following table describes the flags that you can include.

Flag	Description
<b>configuration</b>	Trace configuration events
<b>database</b>	Trace database events
<b>general</b>	Trace general flow
<b>ptsp-statistics</b>	Trace PTSP events
<b>rtsock</b>	Trace routing socket events
<b>statistics</b>	Trace statistics events
<b>subscriber</b>	Trace subscriber events

#### Related Documentation

- Configuring a Statistics Profile for PTSP on page 324
- Configuring PTSP on page 317

## Verifying and Managing PTSP Configuration

**Purpose** Display and clear information about packet-triggered subscribers and PTSP services.

#### Action

- To display bandwidth information about subscribers:  

```
user@host> show services subscriber bandwidth
```
- To display information about the active dynamic policies applied to a subscriber:  

```
user@host> show services subscriber dynamic-policies client-id client-id
```
- To display information about the data flows associated with a subscriber:  

```
user@host> show services subscriber flows client-id client-id
```

- To display information about the active packet-triggered subscriber sessions on the router:

**user@host> show services subscriber sessions**

- To display information about the data traffic statistics for the packet-triggered subscriber:

**user@host> show services subscriber statistics client-id *client-id***

- To clear the active packet-triggered subscriber session on the router and log out the subscriber:

**user@host> clear services subscriber sessions client-id *client-id***

**Related  
Documentation**

- [\*Junos OS System Basics and Services Command Reference\*](#)

## CHAPTER 28

# Gx-Plus Overview

- Gx-Plus for Provisioning Subscribers Overview on page 329
- Diameter Messages Exchanged by Gx-Plus and the PCRF on page 330
- Understanding Diameter AVPs for Gx-Plus on page 332
- Understanding Gx-Plus–PCRF Interactions on page 335

### Gx-Plus for Provisioning Subscribers Overview

---

Gx-Plus is a Diameter-based application that extends the capability of the Gx interface. The 3rd Generation Partnership Project (3GPP) defined Gx as the online policy interface between the Policy Control and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF). to provide control over policy and flow-based charges for subscribers. The PCRF is a centralized policy decision point that deploys business policy rules to allocate broadband network resources and manages flow-based charges for subscribers and services.

Gx-Plus is a notification application; it is not used for subscriber admission control. Gx-Plus notifies the PCRF about subscriber login and termination. When Gx-Plus provisioning is configured, subscriber login is not contingent on whether the PCRF responds to the provisioning request or on the content of the received response. Login proceeds regardless.

Gx-Plus exchanges Diameter Credit-Control Application (DCCA) messages with a PCRF residing on a server to request credit authorization and service provisioning for authenticated subscribers. When an application requests AAA to activate a subscriber's session, the router sends a Credit-Control-Request (CCR) message to determine whether the subscriber has credit for the desired services and to request provisioning of those services from the PCRF policy manager. Subscriber access itself is granted immediately, often even before the CCR message is sent.

The PCRF responds with a Credit-Control-Answer (CCA) message that indicates success or failure for credit authorization. All other message content is ignored. If the subscriber has sufficient credit for the requested services, credit is authorized. If the subscriber has insufficient credit for the services, credit authorization fails. If the Result-Code is not included in the CCA, or if the response times out, then the router interprets this as a provisioning authorization failure and the services are not provided to the subscriber.

When a subscriber client application, such as DHCP, sends a subscriber logout notice to AAA, the router in turn sends a CCR message to the PCRF to request subscriber termination. The PCRF acknowledges the logout with a CCA message.

Different Diameter message types exchanged by Gx-Plus and the PCRF contain different sets of attribute-value pairs (AVPs). If data for an AVP is not available for a request to the PCRF, that AVP is omitted from the message. If the PCRF subsequently has insufficient information to decide on the request, it automatically denies the request.



**NOTE:** An exception to this flexibility exists in Junos OS Release 11.2, where subscribers must have a valid IPv4 address to be presented to the PCRF. This means that Gx-Plus does not generate a request for the PCRF when no IPv4 address or NAS-Port-Id is associated with the subscriber.

Gx-Plus sessions are established that correspond to IPv4 DHCP sessions on dual-stack IPv6/IPv4 or IPv4-only subscriber interfaces, depending on the access profile. However, IPv6 information is not communicated to the PCRF. Consequently, Gx-Plus sessions are not established that correspond to DHCPv6 sessions on IPv6-enabled subscriber interfaces and on dual-stack IPv6/IPv4-enabled interfaces.

---

Gx-Plus includes the following fault tolerance and recovery capabilities:

- Unlimited retries of unacknowledged provisioning requests
- Unlimited retries of logout requests
- Router event notification
- Router discovery



**NOTE:** More than one Diameter-based application (function) can run on a router simultaneously.

**Related Documentation**

- Diameter Messages Exchanged by Gx-Plus and the PCRF on page 330
- Understanding Diameter AVPs for Gx-Plus on page 332
- Understanding Gx-Plus–PCRF Interactions on page 335
- Configuring Gx-Plus on page 339

---

## Diameter Messages Exchanged by Gx-Plus and the PCRF

The Gx-Plus Diameter application extends the 3GPP Gx interface for wireline use cases. 3GPP Gx is registered with the IANA (<http://www.iana.org>). Gx-Plus communicates with a PCRF by exchanging the Diameter messages described in Table 40 on page 331. The messages include various sets of attribute-value pairs (AVPs). If data for a particular



AVP is not available to the router, it simply omits the AVP from the message it sends to the PCRF. If the PCRF determines it has insufficient information to make a decision, it denies the request. The Diameter answer messages include the Result-Code AVP (AVP 268); the values of this AVP convey success, failure, or errors to the requestor.

Juniper Networks has registered the Juniper-Session-Recovery application (16777296) and two new command codes (8388628 for Juniper-Session-Events and 8388629 for Juniper-Session-Discovery) with the IANA (<http://www.iana.org>).

**Table 40: Diameter Messages Used by Gx-Plus and the PCRF**

Diameter Message	Code	Description
Credit-Control-Request (CCR)	272	<p>Request from Gx-Plus to the PCRF at subscriber login or logout.</p> <p>An initial request (CCR-I) is sent when a subscriber logs in and AAA is requested to activate the subscriber's session. Gx-Plus retries the CCR-I message if a CCA-I message is not received from the PCRF within 10 seconds. The CCR-I message is retried up to 3 times.</p> <p>If no CCA-I is received after the 4 CCR-I messages have been sent—the first message plus 3 retries—then Gx-Plus starts sending CCR-N messages. CCR-N messages are retried forever until a success or failure response is received from the PCRF. CCR-N messages include the Juniper-Provisioning-Source AVP (AVP code 2101) set to local to notify the PCRF that the router has the authority to make a local decision regarding subscriber service activation.</p> <p>A termination request (CCR-T) is sent at subscriber logout to inform the PCRF that a provisioned subscriber session is being terminated. CCR-T messages are retried forever until a success response is received from the PCRF.</p>
Credit-Control-Answer (CCA)	272	<p>Reply from the PCRF to a CCR message.</p> <p>In response to a CCR-I, the PCRF returns a CCA-I message that indicates success (DIAMETER_SUCCESS) or failure (DIAMETER_AUTHORIZATION_REJECTED) depending on whether the subscriber has sufficient credit for the requested services. All other response are ignored and the logout is retried until successful.</p> <p>In response to a CCR-T, the PCRF returns a CCA-T message that indicates a successful termination with a value of 2002 (DIAMETER_SUCCESS) in the Result-Code AVP. All other responses are ignored and the logout is retried until successful.</p> <p>A CCA-N is a response to a CCR-N.</p>
Juniper-Session-Discovery-Request (JSDR)	8388629	Discovery request from the PCRF to Gx-Plus to discover subscriber sessions on the router.

Table 40: Diameter Messages Used by Gx-Plus and the PCRF (*continued*)

Diameter Message	Code	Description
Juniper-Session-Discovery-Answer (JSDA)	8388629	<p>Reply from Gx-Plus to a JSDR message; describes session information. The Result-Code AVP includes one of the following values, or an error value:</p> <ul style="list-style-type: none"> <li>2001—DIAMETER_SUCCESS; the end of the database was reached, meaning all information has been sent.</li> <li>2002—DIAMETER_LIMITED_SUCCESS; some of the session information was sent, but more remains to be sent.</li> </ul>
Juniper-Session-Event-Request (JSER)	8388628	<p>Request from Gx-Plus to PCRF regarding events that take place on the router. Notifies the PCRF of certain events on the router by including the Juniper-Event-Type AVP (AVP code 2103). Events reported include cold or warm boots, explicit discovery requests, substantial configuration changes, non-response or error response from PCRF, and exhaustion of fault-tolerant resources.</p>
Juniper-Session-Event-Answer (JSEA)	8388628	<p>Reply from PCRF to a JSER message.</p>
Re-Auth-Request (RAR)	258	<p>Audit request from the PCRF to Gx-Plus to determine whether a specific subscriber is still present.</p>
Re-Auth-Answer (RAA)	258	<p>Reply from Gx-Plus to a RAR message; indicates whether the subscriber is active. The Result-Code AVP includes one of the following values:</p> <ul style="list-style-type: none"> <li>2001—DIAMETER_SUCCESS; subscriber entry was found.</li> <li>5002—DIAMETER_UNKNOWN_SESSION_ID; subscriber entry was not found.</li> <li>3002—DIAMETER_UNABLE_TO_DELIVER; Gx-Plus is not configured.</li> </ul>

- Related Documentation**
- [Configuring Gx-Plus on page 339](#)
  - [Understanding Diameter AVPs for Gx-Plus on page 332](#)
  - [Diameter Base Protocol Overview on page 255](#)

## Understanding Diameter AVPs for Gx-Plus

Diameter conveys information by including various attribute-value pairs (AVPs) in Diameter messages. Table 41 on page 333 lists the standard Diameter AVPs used in Gx-Plus interactions. Diameter reserves AVP code numbers 0 through 255 for RADIUS functions that are implemented in Diameter.

Table 41: Standard Diameter AVPs for Gx-Plus

Diameter AVP	Code Number	Description	Type
Framed-IP-Address	8	Identifies the IPv4 address configured for the subscriber. This is the same value as for RADIUS Framed-IP-Address attribute [8].	OctetString
Event-Timestamp	55	Specifies the time of the event that triggered the message in which this AVP is included. Time is indicated in seconds since January 1, 1900, 00:00 UTC.	Time
NAS-Port-Id	87	Identifies the port of the NAS that authenticates the user. This is the same value as for RADIUS NAS-Port-Id attribute [87].	UTF8String
Session-Id	263	Specifies the subscriber session identifier. Gx-Plus assigns the value to uniquely identify the subscriber session.	UTF8String
Result-Code	268	<p>Indicates whether a request completed successfully. Provides an error code if the request failed.</p> <p>The following classes are recognized by Diameter:</p> <ul style="list-style-type: none"> <li>• 1xxx—Informational</li> <li>• 2xxx—Success</li> <li>• 3xxx—Protocol errors</li> <li>• 4xxx—Transient errors</li> <li>• 5xxx—Permanent failures</li> </ul> <p>Unrecognized classes, which begin with numerals 6–9 or 0, are handled as permanent failures.</p> <p>Gx-Plus supports the following values for errors in a PCRF response; when these values are received or the response is malformed or unrecognizable, the request is retried.</p> <ul style="list-style-type: none"> <li>• 3001—DIAMETER_COMMAND_NOT_SUPPORTED; the application is not running or the command is not recognized.</li> <li>• 3004—DIAMETER_TOO_BUSY; the received message is above either the quota of downstream transactions or the outstanding message memory limit for messages from the network.</li> <li>• 5012—DIAMETER_UNABLE_TO_COMPLY; the received message is greater than the local limit.</li> </ul>	Unsigned32
CC-Request-Number	415	Identifies a request within a session. The combination of Session-Id and CC-Request-Type is globally unique. The number is incremented for each request during the course of a session. The number is reset when a router high availability event takes place.	Unsigned32
CC-Request-Type	416	Specifies the type of credit control request: INITIAL_REQUEST (1) or TERMINATION_REQUEST (3) .	Enumerated

Juniper Networks AVPs are used in addition to the standard Diameter AVPs. These AVPs have an enterprise number of 2636. Table 42 on page 334 lists the Juniper Networks AVPs used in Gx-Plus interactions.

**Table 42: Juniper Networks Diameter AVPs for Gx-Plus**

Diameter AVP	Code Number	Description	Type
Juniper-Virtual-Router	2100	Specifies the name of the virtual router associated with the session.	UTF8String
Juniper-Provisioning-Source	2101	Specifies the provisioning source for the session in CCR-N and JSDA messages: <ul style="list-style-type: none"> <li>1—Local</li> <li>2—Remote</li> </ul>	Enumerated
Juniper-Provisioning-Descriptor	2102	Defines the group used in JSDA messages that includes the session ID, and optionally Juniper-Provisioning-Source and subscriber data.	Grouped
Juniper-Event-Type	2103	Communicates the event type in JSER messages: <ul style="list-style-type: none"> <li>1—Cold boot; all sessions are lost</li> <li>2—Warm boot; sessions are preserved</li> <li>3—Discovery requested by the operator</li> <li>4—<i>Are you there?</i> (AYT); application level ping sent when the notification is due to no response or an erroneous response from the PCRF, or due to a configuration change.</li> <li>5—AWD; application-level watchdog sent by the router when there has been no other activity for 15 seconds. The watchdog is sent every 5 seconds unless preempted by higher-priority synchronization event.</li> </ul>	Enumerated
Juniper-Discovery-Descriptor	2104	Defines the group used in JSER and JSDA messages that includes parameters of a discovery request: discovery type, request string, verbosity, max results.	Grouped
Juniper-Discovery-Type	2105	Specifies the discovery subcommand for JSER and JSDA messages: <ul style="list-style-type: none"> <li>1—Exact: look up the data for the specified session.</li> <li>2—Bulk: Provide get-bulk kinds of information after the specified string.</li> <li>3—Done: Stop retries for all sessions up to the specified session.</li> </ul>	Enumerated

Table 42: Juniper Networks Diameter AVPs for Gx-Plus (*continued*)

Diameter AVP	Code Number	Description	Type
Juniper-Verbosity-Level	2106	Specifies the verbosity level for JSDR and JSDA messages: <ul style="list-style-type: none"> <li>1—Summary; include only the Session-Id AVP.</li> <li>2—Brief; include the Session-Id, Juniper-Virtual-Router, and Framed-IP-Address AVPs.</li> <li>3—Detail; include the Session-Id, Juniper-Provisioning-Source, Juniper-Virtual-Router, Framed-IP-Address, and Event-Timestamp AVPs.</li> <li>4—Extensive; include all available session information.</li> </ul>	Enumerated
Juniper-String-A	2107	Specifies a generic string that is interpreted according to the context.	UTF8String
Juniper-String-B	2108	Specifies a generic string that is interpreted according to the context.	UTF8String
Juniper-String-C	2109	Specifies a generic string that is interpreted according to the context.	UTF8String
Juniper-Unsigned32-A	2110	Specifies a generic, unsigned 32-bit integer that is interpreted according to the context.	Unsigned32
Juniper-Unsigned32-B	2111	Specifies a generic, unsigned 32-bit integer that is interpreted according to the context.	Unsigned32
Juniper-Unsigned32-C	2112	Specifies a generic, unsigned 32-bit integer that is interpreted according to the context.	Unsigned32

- Related Documentation**
- Diameter Messages Exchanged by Gx-Plus and the PCRF on page 330
  - Understanding Gx-Plus–PCRF Interactions on page 335
  - Diameter Base Protocol Overview on page 255

## Understanding Gx-Plus–PCRF Interactions

This topic describes the sequences of Diameter messages exchanged between Gx-Plus and the Policy and Control Charging Function (PCRF) as they interact to perform the following tasks for subscriber access:

- Subscriber login
- Fault tolerance and event notification
- Subscriber audit
- Subscriber logout

## Subscriber Login

Gx-Plus provisioning is enabled for subscribers when you include the **provisioning-order gx-plus** statement at the **[edit access profile *profile-name*]** hierarchy level. When an application requests AAA to activate the subscriber's session, Gx-Plus sends a CCR-I message to the PCRF to request provisioning for the subscriber session. The CCR-I message must include the Juniper-Virtual-Router, Framed-IP-Address, and NAS-Port-ID AVPs. If no IPv4 address has been assigned to the subscriber, or if the NAS-Port-ID is unknown, then the request is not generated.

The PCRF returns a CCA-I message that includes the Result-Code AVP (AVP code 268). Gx-Plus ignores any other AVPs that are included in the response. Gx-Plus considers a CCA-I that does not include the Result-Code AVP as a failed response.

If the Result-Code value is DIAMETER\_SUCCESS (2001), Gx-Plus communicates to AAA that the requested service is activated. If the Result-Code value is DIAMETER\_AUTHORIZATION\_REJECTED, Gx-Plus communicates to AAA that the service activation is not permitted. If the Result-Code AVP has any other value, or is missing, the request is retried. A total of three CCR-I messages can be sent.

If the PCRF does not indicate success or failure, then by default Gx-Plus continues to send requests, but the retry requests are CCR-N messages (no-response notifications) that include the Juniper-Provisioning-Source AVP (AVP code 2101). This AVP indicates that the router has local decision-making authority to provision services in the absence of a PCRF response to the CCR-I. This AVP is not present in the CCR-I message.

## Fault Tolerance and Event Notification

Although the probability is low, it is possible for the PCRF and the router to have different values for the number of subscribers. This error can arise from the following scenarios:

- CCA-I loss: if no CCA-I is delivered to the router, then the PCRF considers a subscriber as provisioned whereas the router considers it not provisioned.
- CCR-T loss: if no CCR-T is delivered to the PCRF, then the PCRF considers a subscriber as provisioned whereas the router considers it not provisioned.

Loss of messages can be greater during cold boots and high availability events. Unacknowledged requests are retransmitted forever until a satisfactory response is received to reduce the incidence of failure, and significant events are reported to Gx-Plus. By default, the number of outstanding requests is limited to 40 to avoid overloading the PCRF. This limit reduces the possibility of losing requests. You can modify this number by including the **max-outstanding-requests** statement at the **[edit access-gx-plus global]** hierarchy level.

Gx-Plus does not rely on the connection state between devices to detect router or PCRF outages, because some events do not affect the connection state and others are not detected when there is a Diameter relay or proxy between the devices. Event notifications (JSER messages) are sent when certain events take place on the router. The Juniper-Event-Type AVP (AVP code 2103) in the message describes the event.

Event notifications are retried until Gx-Plus returns a JSEA message with a Result-Code value of DIAMETER\_SUCCESS (2001) to acknowledge receipt of the event notification. When retrying notifications, one notification is sent for each outstanding event. No other request are sent as long as there is any outstanding event other than an application watch dog (AWD).

Table 43 on page 337 lists router events and the subsequent router and PCRF actions.

**Table 43: Router Events, Router Actions, and PCRF Actions**

Router event	Router action	PCRF action
The router receives no response from the PCRF or an error response.	Send event notification.	Respond to event notification.
The configuration changes.  Significant changes such as the origin host or realm and the Gx-Plus partition destination host or realm also increment the value of the Origin-State-Id AVP.	Send event notification.	Respond to event notification and perform discovery.
The router receives an explicit discovery request from the PCRF.	Send event notification.	Respond to event notification.
The router undergoes a cold boot and all sessions are lost. This can result from a catastrophic failure or power cycle.	Send event notification.	Respond to event notification and clear the database.
The router undergoes a warm boot.	Send event notification.	Respond to event notification and clear the database.
Recovery resources that are needed to continuously retry unacknowledged requests (CCR-N and CCR-T messages) are exhausted. The value of the Origin-State-Id AVP is incremented.  This event is unlikely to occur.	Send event notification.	Respond to event notification and perform discovery.

An important aspect of Gx-Plus fault tolerance is that subscriber login and termination requests are retried (replayed) forever until a satisfactory response is received from the PCRF. In rare circumstances, this can result in a stack of pending requests being replayed over and over.

You can issue the **clear network-access gx-plus replay** command to clear all pending requests. This command causes Gx-Plus to send a JSER message to PCRF that includes the Juniper-Event-Type AVP (AVP code 2103) with a value of 3 indicating a discovery request. The PCRF then returns a JDER message to initiate discovery of all subscribers. When this discovery completes, all pending subscriber requests are cleared.

## PCRF-Generated Discovery

The PCRF runs a discovery process in response to data loss, exhaustion of router resources, operator request, or router request. The JSDR message specifies the level of verbosity desired in the reply from Gx-Plus. The message also specifies whether the request is for data about a particular session or information similar to an SNMP Get-Bulk for all sessions.

Gx-Plus returns a JSDA message that indicates complete success, limited success, or an error. In the event of success, the requested data is also returned.

## Subscriber Audit

The PCRF can send a reauthorization request (RAR message) to Gx-Plus at any time to determine whether a particular subscriber is still logged in. You can also manually trigger the PCRF to do so by issuing the **clear network-access aaa gx-plus replay** command.

The Session-Id AVP identifies the subscriber session. Gx-Plus returns an RAA message to provide status on the subscriber session. When the session is still up (found in the session database) the Result-Code AVP value in the RAA message is `DIAMETER_SUCCESS` (2001). When the session is not found, the Result-Code value is `DIAMETER_UNKNOWN_SESSION_ID` (5002). A Result-Code value of `DIAMETER_UNABLE_TO_DELIVER` (3002) indicates that Gx-Plus is not configured.

## Subscriber Logout

When the client application sends a subscriber logout notice to AAA, Gx-Plus sends a CCR-T message to notify the PCRF that the provisioned subscriber session is being terminated. The PCRF returns a CCA-T message that includes the Result-Code AVP. If the Result-Code value is `DIAMETER_SUCCESS`, Gx-Plus notifies AAA, and AAA notifies the application that the logout is complete. If Gx-Plus does not receive a CCA-T message, or if the Result-Code AVP has any other value or is missing, then the termination request is retried until the CCA-T message is returned with `DIAMETER_SUCCESS`.

### Related Documentation

- [Configuring Gx-Plus on page 339](#)
- [Gx-Plus for Provisioning Subscribers Overview on page 329](#)
- [Diameter Messages Exchanged by Gx-Plus and the PCRF on page 330](#)
- [Understanding Diameter AVPs for Gx-Plus on page 332](#)



## CHAPTER 29

# Configuring Gx-Plus

- Configuring Gx-Plus on page 339
- Configuring the Gx-Plus Partition on page 340
- Configuring the Gx-Plus Global Attribute on page 341
- Provisioning Subscribers with Gx-Plus on page 341

## Configuring Gx-Plus

---

You can configure the Gx-Plus client application to work with a PCRF policy manager residing on a server. The PCRF is a centralized policy decision point that deploys business rules to allocate broadband network resources and manage subscribers and services. Gx-Plus requests service provisioning from the PCRF.



**NOTE:** Contact the Juniper Networks Technical Assistance Center (JTAC) for information on supported PCRFs.

To configure Gx-Plus:

1. Configure the Gx-Plus partition.  
See “Configuring the Gx-Plus Partition” on page 340.
2. Configure the number of outstanding Gx-Plus requests permitted.  
See “Configuring the Gx-Plus Global Attribute” on page 341.
3. Configure Gx-Plus provisioning for subscribers.  
See “Provisioning Subscribers with Gx-Plus” on page 341.
4. Configure Gx-Plus event tracing as part of general authentication service tracing operations.  
See “Tracing General Authentication Service Processes” on page 74.

### Related Documentation

- Gx-Plus for Provisioning Subscribers Overview on page 329

## Configuring the Gx-Plus Partition

Gx-Plus works within a specific logical system: routing instance context, called a partition.



**NOTE:** Currently, only a single partition is supported; you must configure it within the default logical system: routing instance context.

Before you configure the Gx-Plus partition, perform the following task:

- Configure the Diameter instance at the **[edit diameter]** hierarchy level. See “Configuring Diameter” on page 259.

Configuration for the Gx-Plus partition consists of naming the partition and then associating a Diameter instance, the PCRF hostname, and the PCRF realm with the partition.

To configure the Gx-Plus partition:

1. Create the partition or specify the name of an existing partition.

```
[edit access gx-plus]
user@host# set partition partition-name
```

2. Specify the Diameter instance for the Gx-Plus partition.



**NOTE:** Currently, only the default Diameter instance, *master*, is supported.

```
[edit access gx-plus partition partition-name]
user@host# set diameter-instance instance-name
```

3. (Optional) Configure the destination host for the Gx-Plus partition.

```
[edit access gx-plus partition partition-name]
user@host# set destination-host hostname
```

4. Configure the destination realm for the Gx-Plus partition.

```
[edit access gx-plus partition partition-name]
user@host# set destination-realm realm
```

The following example shows a Gx-Plus partition configuration.

```
gx-plus {
  partition partition1 {
    diameter-instance master;
    destination-host pcrf1;
    destination-realm generic.example.com;
  }
}
```

### Related Documentation

- Configuring Gx-Plus on page 339
- Gx-Plus for Provisioning Subscribers Overview on page 329

## Configuring the Gx-Plus Global Attribute

You can configure one attribute that applies to all Gx-Plus partitions globally. When a request from Gx-Plus to the PCRF is not answered or is improperly answered, Gx-Plus keeps retrying the request until it receives an appropriate answer. If the number of requests grows too large, the PCRF can become overloaded and messages can be lost. To reduce this risk, you can set a limit on the number of outstanding requests to the PCRF that Gx-Plus can retry.

To configure the number of outstanding requests:

- Set the limit.

```
[edit access gx-plus]
user@host# set max-outstanding-requests number
```

The following example shows a Gx-Plus global configuration.

```
access {
  gx-plus {
    global {
      max-outstanding-requests 30;
    }
  }
}
```

### Related Documentation

- Configuring Gx-Plus on page 339
- Gx-Plus for Provisioning Subscribers Overview on page 329

## Provisioning Subscribers with Gx-Plus

You can configure AAA to use Gx-Plus to request provisioning from a PCRF to instantiate services for an authenticated subscriber.

Before you configure Gx-Plus provisioning for subscribers, perform the following task:

- Create the subscriber access profile at the **[edit access profile]** hierarchy level. See “Configuring an Access Profile for Subscriber Management” on page 53.

To configure Gx-Plus provisioning:

- Specify **gx-plus** as the provisioning method in the profile.

```
[edit access profile profile-name]
user@host# set provisioning-order gx-plus
```

### Related Documentation

- Configuring Gx-Plus on page 339
- Gx-Plus for Provisioning Subscribers Overview on page 329



## PART 8

# Mobile IP Access

- [Mobile IP Overview on page 345](#)
- [Configuring Mobile IP on page 357](#)



# Mobile IP Overview

- Mobile IP Home Agent Elements and Behavior on page 345
- Mobile IP Registration on page 348
- Mobile IP Routing and Forwarding on page 352
- Mobile IP in the WiMAX Environment on page 353

## Mobile IP Home Agent Elements and Behavior

---

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 level, the **[edit logical-systems logical-system-name]** hierarchy level, and the **[edit routing-instances routing-instances-name]** hierarchy level.



**NOTE:** Currently, Junos OS 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.

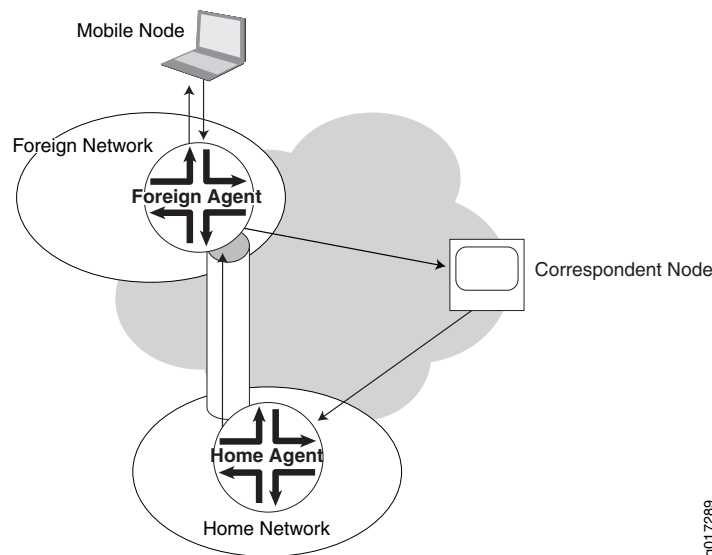
When a mobile node roams into a new, foreign network, it negotiates with the foreign agent to get a secondary IP address, which is referred to as the care-of address. The mobile node registers this care-of address with the home agent. The home agent then establishes a tunnel to the care-of address if 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. Figure 6 on page 346 illustrates this forwarding and routing process behavior. Although the traffic to the correspondent node comes from the foreign agent, to the correspondent node the traffic appears to come from the mobile node's home network.

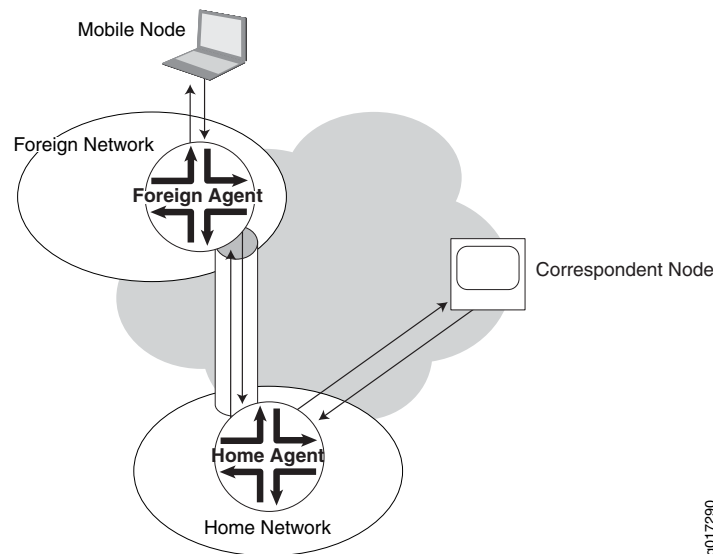
**Figure 6: Mobile IP Network Without Reverse Tunneling**



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. This reverse tunnel capability is negotiated between the foreign agent and the home agent when the mobile node requests registration. Traffic from a correspondent node to the mobile node is forwarded by the home agent through the foreign agent as in the other scenario. Figure 7 on page 347 shows how traffic from the mobile node to a correspondent node is tunneled from the foreign agent to the home agent and then routed to the correspondent node by the home agent.



Figure 7: Mobile IP Network with Reverse Tunneling



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 forwarded over any interface.

You can use the Mobile IP home agent feature to configure the home agent within the default router context with either local or AAA authentication. When you configure local authentication, you can also configure Mobile IP independently in any named routing instance in any configured logical router. When you configure AAA as the authentication method, you can configure Mobile IP only in the default router context.

The Mobile IP home agent can also receive, process, and send Worldwide Interoperability for Microwave Access (WiMAX) vendor-specific RADIUS attributes (VSAs). This feature enables Mobile IP home agent to work in a WiMAX home connectivity services network (H-CSN), to provide for mobility management at the IP layer.

The home agent handles the following tasks:

- Registration of mobile nodes
- Routing and forwarding of mobile node traffic

#### Related Documentation

- Mobile IP Registration on page 348
- Mobile IP Routing and Forwarding on page 352
- Mobile IP in the WiMAX Environment on page 353
- Configuring Mobile IP on page 357

## 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.

## Reauthentication

Reauthentication is not currently supported by the authentication process. Mobile IP caches a security association for each mobile node, which 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; vendor ID 4874) listed in Table 44 on page 349. 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 44: Juniper Networks 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

Table 44: Juniper Networks VSAs Used by Mobile IP (*continued*)

Attribute Number	Attribute Name	Description	Value
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. Include 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.

When local authentication is configured, you can configure Mobile IP independently in any named routing instance in any configured logical router. All Mobile IP statements are available in those contexts, except for the **order aaa** statement at the **[edit services mobile-ip authenticate]** hierarchy level.

## 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.

- Related Documentation**
- 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 45
  - Mobile IP Home Agent Elements and Behavior on page 345
  - Mobile IP Routing and Forwarding on page 352
  - Mobile IP in the WiMAX Environment on page 353
  - Configuring Mobile IP on page 357

---

## Mobile IP Routing and Forwarding

Mobile IP employs a care-of address to process traffic for the mobile node.

The mobile node acquires the 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 foreign agent 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.

Mobile IP does not support graceful Routing Engine switchover (GRES). It handles the rebooting of processes in the following ways:

- Mobile IP process—After Mobile IP completes a restart, it removes the Mobile IP subscriber entries from AAA and the session database. When that is complete, Mobile IP can process new mobile node registration requests.
- AAA process—After AAA completes a restart, Mobile IP removes all subscriber data held internally by AAA and all corresponding session database entries.
- Routing protocol process—When the connection between the routing protocol process and Mobile IP is lost, Mobile IP responds by clearing the mobile node bindings that are associated with the logical system in which the routing protocol process restarted. The

routing protocol process maintains routes to mobile nodes during the restart. The routing protocol process flushes these routes if they are not reinstalled after the restart completes and before the stale route timer expires.

**Related  
Documentation**

- Mobile IP Home Agent Elements and Behavior on page 345
- Mobile IP Registration on page 348
- Mobile IP in the WiMAX Environment on page 353
- Configuring Mobile IP on page 357

## Mobile IP in the WiMAX Environment

Worldwide Interoperability for Microwave Access (WiMAX) is the international standard for wide area radio access networks. It provides a framework for networks that are implemented in different ways to successfully interoperate with mobile subscribers that roam among the networks. This interoperability enables the subscribers to be authenticated by their home network wherever they roam, and to receive the services for which they are authorized.

The Mobile IP home agent can operate in either of two access modes, generic and WiMAX. The generic access type is appropriate when the home agent is deployed in a generic Mobile IP home network. When deployed as a home agent in a WiMAX home connectivity services network (H-CSN), you must configure the WiMAX access type. The WiMAX access type enables the Mobile IP home agent to receive, process, and send WiMAX vendor-specific attributes (VSAs) that are used by AAA and the RADIUS server to authenticate the mobile subscriber. When the access type is generic, the Mobile IP home agent cannot handle these VSAs.



**NOTE:** The Mobile IP configuration for WiMAX requires that AAA be used for the authentication method. For that reason, WiMAX is available only in the default router context.

A WiMAX H-CSN is analogous to the Mobile IP home network for non-WiMAX implementations. When WiMAX is enabled for the Mobile IP home agent in an H-CSN, the Mobile IP home agent triggers subscriber authentication when the agent receives the registration request. The home agent stores WiMAX Forum (vendor ID 24757) vendor-specific attributes (VSAs) listed in Table 45 on page 354 in the session database based on the registration request.

Table 45: WiMAX Forum VSAs used by Mobile IP

Attribute Number	Attribute Name	Description	Value
26-1	WiMAX-Capability	Identifies the WiMAX capabilities supported by the home agent (sent in the Access-Request message). In an Access-Accept message, identifies the capabilities selected by the RADIUS server (returned in the Access-Accept message).	string or integer
26-6	hHA-IP-MIP4	IP address of the home agent (hHA) making the request	octet string: IP address
26-10	MN-HA-MIP4-KEY	MN-hHA key sent by the RADIUS server for validation by the home agent	integer: 2-octet salt followed by 16-octet encrypted MN-hHA hash key
26-11	MN-HA-MIP4-SPI	Security parameter index (SPI) associated with the MN-HA-MIP4 key	integer: 4-octet
26-15	hHA-RK-KEY	Key used by the NAS to generate FA-HA keys	integer: 2-octet salt followed by 16-octet encrypted MN-hHA hash key
26-16	hHA-RK-SPI	SPI associated with the hHA-RK key	integer: 4-octet
26-17	HA-RK-Lifetime	Lifetime of the hHA-RK key and derived keys	integer: 4-octet
26-18	RRQ-HA-IP	IP address of the home agent contained in the Mobile IP registration request or the binding update	octet string: IP address



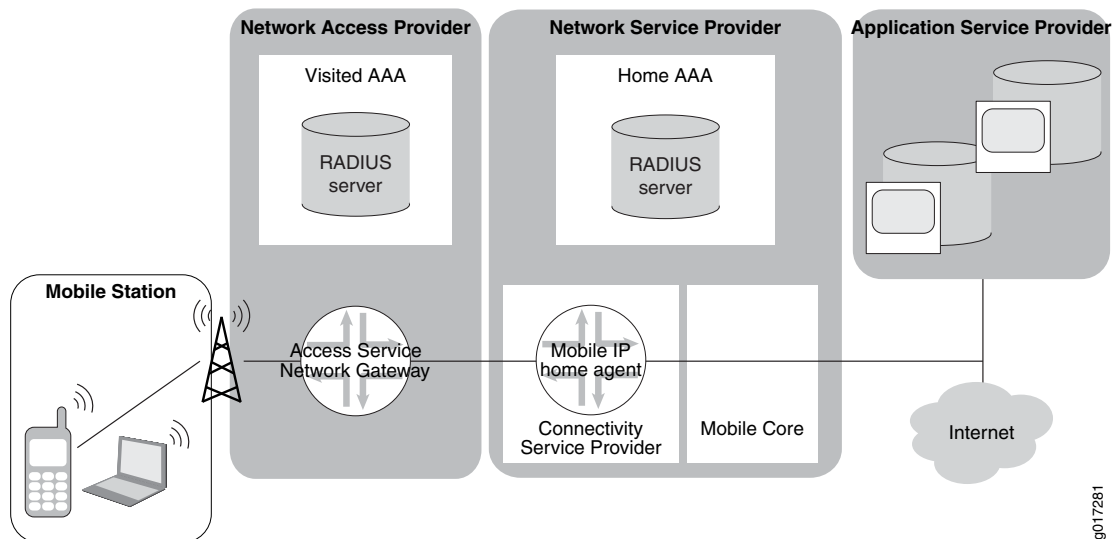
Table 45: WiMAX Forum VSAs used by Mobile IP (*continued*)

Attribute Number	Attribute Name	Description	Value
26–19	RRQ-MN-HA-KEY	The MN-HA key bound to the home agent IP address as reported by the RRQ-HA-IP attribute. Used to validate the MN-HA-AE of the Mobile IP registration request.	integer: 2-octet salt followed by 16-octet encrypted MN-hHA hash key

The home agent requests AAA to fetch the corresponding WiMAX-related information from the RADIUS server. The AAA client sends an Access-Request message to the server. The RADIUS server responds with the necessary WiMAX information, such as the MN-HA key and the HA-RK key, and then the AAA client passes the response to the home agent. The Mobile IP home agent verifies the response received from AAA, processes the registration request, and then grants, extends, or denies subscriber registration.

Figure 8 on page 355 shows the elements of a sample WiMAX topology.

Figure 8: Sample Mobile IP WiMAX Topology



The Mobile IP subscriber registration flow is a four-step process.

1. The access service network gateway (ASN-GW) sends the subscriber registration request from the mobile node to the Mobile IP home agent. The registration request is protected by the MN-HA authentication extension and the FA-HA authentication extension.
2. The home agent requests that the RADIUS server send the cryptographic keys for the Mobile IP session identified by user@realm. The home agent notifies the RADIUS server that it seeks to source IP session-based accounting messages.

3. The RADIUS server agrees to use IP session-based accounting, provides the requested cryptographic keys, and sends the AAA-Session-ID for this session.
4. The home agent replies to the Mobile IP registration request.

Reauthentication of WiMAX subscribers is not currently supported.

You can configure the Mobile IP home agent for WiMAX access by including the **wimax** statement at the **[edit services mobile-ip access-type]** hierarchy level. You can prevent the Mobile IP home agent from being able to process WiMAX VSAs by either removing the **wimax** statement at the **[edit services mobile-ip access-type]** hierarchy level or by including the **generic** statement at the **[edit services mobile-ip access-type]** hierarchy level. The default access type for Mobile IP home agent is generic.

**Related  
Documentation**

- 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 45
- *Mobile IP Home Agent Elements and Behavior* on page 345
- *Mobile IP Registration* on page 348
- *Mobile IP Routing and Forwarding* on page 352
- *Configuring Mobile IP* on page 357

## CHAPTER 31

# Configuring Mobile IP

- Configuring Mobile IP on page 357
- Configuring the Mobile IP Authentication Method on page 358
- Configuring the Mobile IP Home Agent on page 358
- Configuring the Local Authentication Attributes for the Mobile Node on page 359
- Configuring Accounting for Mobile IP Subscribers on page 360
- Configuring Dynamic Home Assignment for the Mobile Node on page 360
- Configuring the Access Type for Mobile IP on page 361
- Tracing Mobile IP Operations for Subscriber Access on page 361
- Configuring the Mobile IP Trace Log Filename on page 363
- Configuring the Number and Size of Mobile IP Log Files on page 363
- Configuring Access to the Mobile IP Log File on page 364
- Configuring a Regular Expression for Mobile IP Lines to Be Logged on page 364
- Configuring the Mobile IP Tracing Flags on page 365

## 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 the authentication method for registration requests, local or AAA.  
See “Configuring the Mobile IP Authentication Method” on page 358.
2. Configure the Mobile IP home agent.  
See “Configuring the Mobile IP Home Agent” on page 358.
3. Configure the authentication attributes for the mobile node.  
See “Configuring the Local Authentication Attributes for the Mobile Node” on page 359.
4. Configure accounting for Mobile IP subscribers.

- See “Configuring Accounting for Mobile IP Subscribers” on page 360
5. Configure the dynamic reassignment of the mobile node to another home agent.  
See “Configuring Dynamic Home Assignment for the Mobile Node” on page 360.
  6. Configure the access type for Mobile IP.  
See “Configuring the Access Type for Mobile IP” on page 361.
  7. Configure trace options for troubleshooting the configuration.  
See “Tracing Mobile IP Operations for Subscriber Access” on page 361.

---

## 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.



**NOTE:** AAA server authentication is available only in the default router context. Local authentication is available in both default and nondefault router contexts.

To configure the Mobile IP authentication method:

- Specify either local or AAA authentication.

```
[edit services mobile-ip]
user@host# set authenticate order local
```

### Related Documentation

- Configuring Mobile IP on page 357

---

## 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
```

**Related Documentation**

- Configuring Mobile IP on page 357

## 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
```

**Related Documentation**

- Configuring Mobile IP on page 357

## 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 Documentation

- Configuring Mobile IP on page 357
- Specifying the Authentication and Accounting Methods for Subscriber Access on page 21
- Configuring Per-Subscriber Session Accounting on page 24
- Configuring RADIUS Server Parameters for Subscriber Access on page 26

## 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
```

### Related Documentation

- Configuring Mobile IP on page 357

## Configuring the Access Type for Mobile IP

You can configure the Mobile IP home agent to operate in a Worldwide Interoperability for Microwave Access (WiMAX) home connectivity services network (H-CSN). This configuration enables the home agent to receive, process, and send WiMAX VSAs for subscriber authentication and registration. By default, Mobile IP cannot process the WiMAX VSAs. For operation in non-WiMAX environments, you can return it to this mode by configuring the **generic** access type.



**NOTE:** The Mobile IP configuration for WiMAX requires that AAA be used for the authentication method. For that reason, WiMAX is available only in the default router context.

To configure the access type, do one of the following:

- Configure generic operation.  

```
[edit services mobile-ip]
user@host# set access-type generic
```
- Configure WiMAX operation.  

```
[edit services mobile-ip]
user@host# set access-type wimax
```

### Related Documentation

- Configuring Mobile IP on page 357

## Tracing Mobile IP Operations for Subscriber Access

The Junos OS trace feature tracks Mobile IP operations and records events in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

Trace-related configurations are independent for each logical system and routing instance in which Mobile IP is configured. Mobile IP can generate two types of log messages:

- Trace messages common to all logical systems and routing instances in which Mobile IP is configured. Examples of this global message type are the messages generated by Mobile IP during initialization after it starts up. These trace messages are stored in the default trace file, **/var/log/mipd**. You cannot configure Mobile IP to save global messages in a different file. Mobile IP traces global messages by default.
- Trace messages specific to a logical system or routing instance in which Mobile IP is configured. An example of this message type is the message generated by Mobile IP when it receives a registration request. These trace messages are stored in the trace file configured for that logical system or routing instance. These messages cannot be saved in **/var/log/mipd**.

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

1. Global messages are logged in the `/var/log/mipd` file. Logical system or routing instance messages are logged in a file that you must configure, also located in the `/var/log` directory. You cannot change the directory (`/var/log`) in which trace files are located.
2. When the file reaches 128 kilobytes (KB), it is renamed until there are three trace files. For example, `mipd` becomes `mipd.0`, then `mipd.1`, and finally `mipd.2`. Then the oldest trace file (`mipd.2`) is overwritten.

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

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To configure Mobile IP tracing operations:

1. (Optional) Configure a trace log filename.  
See “Configuring the Mobile IP Trace Log Filename” on page 363.
2. (Optional) Configure the number and size of trace logs.  
See “Configuring the Number and Size of Mobile IP Log Files” on page 363.
3. (Optional) Configure user access to trace logs.  
See “Configuring Access to the Mobile IP Log File” on page 364.
4. (Optional) Configure a regular expression to filter the information to be included in the trace log.  
See “Configuring a Regular Expression for Mobile IP Lines to Be Logged” on page 364.
5. (Optional) Configure flags to specify which events are logged.  
See “Configuring the Mobile IP Tracing Flags” on page 365.

## Related Documentation



## Configuring the Mobile IP Trace Log Filename

Global messages common to all Mobile IP logical systems and routing instances are recorded only in `/var/log/mipd`. Mobile IP automatically creates this file if it is not present when Mobile IP starts. You cannot configure global messages to be recorded in any other file.

You must specify a different name with the **file** option for messages that are specific to a logical system or routing instance in which Mobile IP is configured. Ensure that filenames are unique for each logical system or routing instance in which Mobile IP is configured. If you do not configure a trace filename for a logical system or routing instance, then nothing is traced for that entity.

To configure the filename for Mobile IP tracing operations for a logical system or routing instance:

- Specify the name of the file used for the trace output.

```
[edit logical-systems lr1 services mobile-ip traceoptions]
user@host# set file mip-lr1_1
```

### Related Documentation

- Configuring Mobile IP on page 357
- Tracing Mobile IP Operations for Subscriber Access on page 361
- traceoptions (Mobile IP) on page 1229**

## 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 finally **filename.2**, until there are three trace files. Then the oldest trace file (**filename.2**) is overwritten.

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

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
```

- Related Documentation**
- [Configuring Mobile IP on page 357](#)
  - [Tracing Mobile IP Operations for Subscriber Access on page 361](#)
  - [traceoptions \(Mobile IP\) on page 1229](#)

---

## Configuring Access to the Mobile IP Log File

By default, only the user who configures the tracing operation can access the log files. 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, only the user who configured tracing can read the log file:

- 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
```

- Related Documentation**
- [Configuring Mobile IP on page 357](#)
  - [Tracing Mobile IP Operations for Subscriber Access on page 361](#)
  - [traceoptions \(Mobile IP\) on page 1229](#)

---

## 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
```

- Related Documentation**
- [Configuring Mobile IP on page 357](#)
  - [Tracing Mobile IP Operations for Subscriber Access on page 361](#)
  - [traceoptions \(Mobile IP\) on page 1229](#)

## 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
<b>all</b>	Trace all operations
<b>authentication</b>	Trace authentication operations
<b>binding</b>	Trace bindings
<b>event</b>	Trace events
<b>home-agent</b>	Trace home agent operations
<b>interface-database</b>	Trace interface database operations
<b>packet</b>	Trace packet decoding operations
<b>protocol</b>	Trace protocol operations
<b>rtsock</b>	Trace routing socket operations
<b>session-db</b>	Trace session database events
<b>signal</b>	Trace signal operations
<b>subscriber</b>	Trace subscriber events
<b>trace</b>	Trace changes in tracing
<b>tunnel</b>	Trace tunneling operations
<b>user-interface</b>	Trace user interface 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 Documentation

- [Configuring Mobile IP on page 357](#)
- [Tracing Mobile IP Operations for Subscriber Access on page 361](#)
- [traceoptions \(Mobile IP\) on page 1229](#)



## PART 9

# Dynamic Profiles for Access and Services

- [Dynamic Profiles Overview on page 369](#)
- [Configuring Dynamic Profiles on page 391](#)
- [Dynamic Profile Examples on page 401](#)



# Dynamic Profiles Overview

- Dynamic Profiles Overview on page 369
- Dynamic Variables Overview on page 371
- Junos OS Predefined Variables on page 372
- Junos OS Predefined Variables That Correspond to RADIUS Attributes and VSAs on page 385
- User-Defined Variables on page 389

## 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 subhierarchies within the **[edit dynamic-profiles]** hierarchy:

- **class-of-service**
- **firewall**
- **interfaces**
- **predefined-variable-defaults**
- **protocols**
- **routing-instances**
- **routing-options**
- **variables**

This topic covers:

- Dynamic Profile Interface Support on page 370
- What Dynamic Profiles Do on page 370

- [How Dynamic Profiles Work](#) on page 370
- [Dynamic Profile Semantic Checking](#) on page 370

## Dynamic Profile Interface Support

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 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.

## Dynamic Profile Semantic Checking

Variables are applied to dynamic profiles dynamically and cannot be checked with existing CLI checks. Semantic checking validates some variables in dynamic profiles to help identify potential configuration errors.

Semantic checks are performed during commit and during profile instantiation. Commit time checks ensure that variables appear in the correct location within the dynamic profile. Checks performed before profile instantiation ensure that the values that replace the variables are correct. The checks performed on the values include the following:

- Range validation
- Variable type validation
- Existence of variables where they are mandatory
- Variable matching to regular expressions

A commit time check failure results in an error message being displayed and logged in to **/var/log/messages** and the commit not taking place. An instantiation failure results in an error being logged in **/var/log/messages** and the profile instantiation failing.

### Related Documentation

- [Configuring a Basic Dynamic Profile](#) on page 391



- Configuring a Dynamic Profile for Client Access on page 395
- Configuring a Dynamic Profile for Various Levels of Services on page 397
- Dynamic Variables Overview on page 371
- Subscriber Interface Overview on page 433

## Dynamic Variables Overview

---

Variables constitute the dynamic component of a dynamic profile. You use variables in dynamic profiles as placeholders for dynamically obtained or dynamically generated information that the dynamic profiles use to configure subscriber interfaces.

- How Dynamic Variables Work on page 371
- Default Values for Predefined Variables on page 371

### 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), or a value associated with each user-configurable variable.

For your convenience, Junos OS 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 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 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 OS obtains values for each variable 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 and are used to configure the subscriber interface.

### Default Values for Predefined Variables

You can optionally configure default values for many of the predefined variables. If the external RADIUS server is not available or the VSA does not contain a value for the predefined variable, the Junos OS uses the default values.

When a default value is configured for a variable and RADIUS also returns a value, the system uses the value from RADIUS instead.

#### Related Documentation

- Configuring a Basic Dynamic Profile on page 391
- Configuring a Dynamic Profile for Client Access on page 395
- Configuring a Dynamic Profile for Various Levels of Services on page 397
- Junos OS Predefined Variables on page 372
- User-Defined Variables on page 389
- Junos OS Predefined Variables That Correspond to RADIUS Attributes and VSAs on page 385
- Configuring Predefined Dynamic Variables in Dynamic Profiles on page 392
- Configuring User-Defined Dynamic Variables in Dynamic Profiles on page 394
- Dynamic Profiles Overview on page 369
- Subscriber Interface Overview on page 433
- Example: Firewall Dynamic Profile on page 402
- Example: IGMP Dynamic Profile on page 401
- RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 39

## Junos OS Predefined Variables

Junos OS contains several predefined variables. The dynamic profile obtains and replaces data for these variables from an incoming client data packet and configuration (local and RADIUS). These variables are predefined—you use them in the body of a dynamic profile without first having to define the variables at the **[dynamic-profiles profile-name variables]** hierarchy level. Table 46 on page 372 provides a list of predefined variables, their descriptions, and where in the Junos OS hierarchy you can configure them.

**Table 46: Junos OS Predefined Variables and Definitions**

Variable	Definition
<b>Access and Access-Internal Routes</b>	
\$junos-framed-route-cost	Cost metric of an access route. You specify this variable at the <b>[edit dynamic-profiles profile-name routing-options access route address]</b> hierarchy level for the <b>metric</b> statement.
\$junos-framed-route-distance	Distance of an access route. You specify this variable at the <b>[edit dynamic-profiles profile-name routing-options access route address]</b> hierarchy level for the <b>preference</b> statement.

Table 46: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-framed-route-ip-address-prefix	Route prefix of an access route. You specify this variable at the <b>[edit dynamic-profiles profile-name routing-options access]</b> hierarchy level for the <b>route</b> statement.
\$junos-framed-route-ipv6-address-prefix	IPv6 route prefix of an access route. You specify this variable at the <b>[edit dynamic-profiles profile-name routing-options access]</b> hierarchy level for the <b>route</b> statement.
\$junos-framed-route-ipv6-nexthop	IPv6 next-hop address of an access route. You specify this variable at the <b>[edit dynamic-profiles profile-name routing-options access route address]</b> hierarchy level for the <b>next-hop</b> statement.
\$junos-framed-route-nexthop	Next-hop address of an access route. You specify this variable at the <b>[edit dynamic-profiles profile-name routing-options access route address]</b> hierarchy level for the <b>next-hop</b> statement.
\$junos-framed-route-tag	Tag value of an access route. You specify this variable at the <b>[edit dynamic-profiles profile-name routing-options access route address]</b> hierarchy level for the <b>tag</b> statement.
\$junos-interface-name	<p>Logical interface of an access-internal route. DHCP or PPP supplies this information when the subscriber logs in. You specify this variable at the <b>[edit dynamic-profiles profile-name routing-options access-internal route address]</b> hierarchy level for the <b>qualified-next-hop</b> statement.</p> <p>This variable is also used for creating dynamic IP demux interfaces.</p>
\$junos-subscriber-ip-address	<p>IP address of a subscriber identified in an access-internal route. You specify this variable at the <b>[edit dynamic-profiles profile-name routing-options access-internal]</b> hierarchy level for the <b>route</b> statement.</p> <p>This variable is also used for creating dynamic IP demux interfaces.</p>
\$junos-subscriber-mac-address	MAC address for a subscriber identified in an access-internal route. You specify this variable at the <b>[edit dynamic-profiles profile-name routing-options access-internal route address qualified-next hop underlying-interface]</b> hierarchy level for the <b>mac-address</b> statement.

Table 46: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
<b>Dynamic Protocols</b>	
\$junos-igmp-access-group-name	Specifies the access list to use for the source (S) filter.
\$junos-igmp-access-source-group-name	Specifies the access list to use for the source-group (S,G) filter.
\$junos-igmp-enable	Ensures that IGMP is not disabled on the interface by an AAA-based authentication and management method (for example, RADIUS). You specify this variable at the <b>[dynamic-profiles profile-name protocols igmp]</b> hierarchy level for the <b>interface</b> statement.
\$junos-igmp-immediate-leave	Enables IGMP immediate leave on the interface. You specify this variable at the <b>[dynamic-profiles profile-name protocols igmp]</b> hierarchy level for the <b>interface</b> statement.
\$junos-igmp-version	IGMP version configured in a client access profile. The Junos OS obtains this information from the RADIUS server when a subscriber accesses the router. The version is applied to the accessing subscriber when the profile is instantiated. You specify this variable at the <b>[dynamic-profiles profile-name protocols igmp]</b> hierarchy level for the <b>interface</b> statement.
\$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 <b>[dynamic-profiles profile-name protocols igmp]</b> hierarchy level for the <b>interface</b> statement.</p> <p>The interface name is derived from concatenating the <b>\$junos-interface-ifu-name</b> and the <b>\$junos-underlying-interface-unit</b> variables obtained when a subscriber is created dynamically at the <b>[dynamic-profiles profile-name interfaces]</b> hierarchy level.</p>
\$junos-ipv6-ndra-prefix	Prefix value for the router advertisement interface. The Junos OS obtains this information from the RADIUS server when a subscriber accesses the router. The prefix value is applied to the accessing subscriber when the profile is instantiated. You specify this variable at the <b>[dynamic-profiles profile-name protocols router-advertisement interface \$junos-interface-name]</b> hierarchy level.

Table 46: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-mld-access-group-name	Specifies the access list to use for the group (G) filter.
\$junos-mld-access-source-group-name	Specifies the access list to use for the source-group (S,G) filter.
\$junos-mld-enable	Ensures that MLD is not disabled on the interface by an AAA-based authentication and management method (for example, RADIUS). You specify this variable at the <b>[dynamic-profiles profile-name protocols mld]</b> hierarchy level for the <b>interface</b> statement.
\$junos-mld-immediate-leave	Enables MLD immediate leave on the interface. You specify this variable at the <b>[dynamic-profiles profile-name protocols mld]</b> hierarchy level for the <b>interface</b> statement.
\$junos-mld-version	MLD version configured in a client access profile. The Junos OS obtains this information from the RADIUS server when a subscriber accesses the router. The version is applied to the accessing subscriber when the profile is instantiated. You specify this variable at the <b>[dynamic-profiles profile-name protocols mld]</b> hierarchy level for the <b>interface</b> statement.
<b>Dynamic CoS — Traffic-Shaping Parameters</b>	
\$junos-cos-byte-adjust	<p>Byte adjustment value configured in a traffic-control profile in a dynamic profile for subscriber access. The Junos OS 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 <b>bytes</b> option with the <b>overhead-accounting</b> statement at the <b>[edit dynamic-profiles profile-name class-of-service traffic-control-profiles profile-name]</b> hierarchy level.</p>

Table 46: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-cos-delay-buffer-rate	<p>Delay-buffer rate configured in a traffic-control profile in a dynamic profile for subscriber access. The Junos OS 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 <b>delay-buffer-rate</b> statement at the <b>[edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>]</b> hierarchy level.</p>
\$junos-cos-excess-rate	<p>Excess rate configured in a traffic-control profile in a dynamic profile for subscriber access. The Junos OS 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 <b>excess-rate</b> statement at the <b>[edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>]</b> hierarchy level.</p>
\$junos-cos-guaranteed-rate	<p>Guaranteed rate configured in a traffic-control profile in a dynamic profile for subscriber access. The Junos OS 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 <b>guaranteed-rate</b> statement at the <b>[edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>]</b> hierarchy level.</p>

Table 46: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$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 OS 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 <b>scheduler-map</b> statement at the <b>[edit dynamic-profiles profile-name class-of-service traffic-control-profiles profile-name]</b> hierarchy level.</p> <p><b>NOTE:</b> The scheduler map can be defined dynamically (at the <b>[edit dynamic-profiles profile-name class-of-service scheduler-maps]</b> hierarchy level) or statically (at the <b>[edit class-of-service scheduler-maps]</b> hierarchy level).</p>
\$junos-cos-shaping-mode	<p>Shaping mode configured in a traffic-control profile in a dynamic profile for subscriber access. The Junos OS 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 <b>overhead-accounting</b> statement at the <b>[edit dynamic-profiles profile-name class-of-service traffic-control-profiles profile-name]</b> 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 OS 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 <b>shaping-rate</b> statement at the <b>[edit dynamic-profiles profile-name class-of-service traffic-control-profiles profile-name]</b> hierarchy level.</p>

---

Dynamic CoS — Scheduler Parameters

---

Table 46: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-cos-scheduler	<p>Name of a scheduler configured in a dynamic profile for subscriber access. The Junos OS 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 <b>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers]</b> 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 OS 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 <b>buffer-size</b> statement with the <b>percent</b> option at the <b>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>]</b> hierarchy level.</p>
\$junos-cos-scheduler-pri	<p>Packet-scheduling priority value specified for a scheduler configured in a dynamic profile for subscriber access. The Junos OS 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 <b>priority</b> statement at the <b>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>]</b> hierarchy level.</p>
\$junos-cos-scheduler-dropfile-any	<p>Name of the drop profile for random early detection (RED) for loss-priority level <b>any</b> specified for a scheduler configured in a dynamic profile for subscriber access. The Junos OS 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 <b>drop-profile</b> statement at the <b>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i> drop-profile-map loss-priority <i>any</i> protocol <i>any</i>]</b> hierarchy level.</p> <p><b>NOTE:</b> The drop profile must be configured statically (at the <b>[edit class-of-service drop-profiles]</b> hierarchy level).</p>



Table 46: Junos OS Predefined 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 <b>high</b> specified for a scheduler configured in a dynamic profile for subscriber access. The Junos OS 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 <b>drop-profile</b> statement at the <b>[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name drop-profile-map loss-priority high protocol any]</b> hierarchy level.</p> <p><b>NOTE:</b> The drop profile must be configured statically (at the <b>[edit class-of-service drop-profiles]</b> hierarchy level).</p>
\$junos-cos-scheduler-dropfile-low	<p>Name of the drop profile for random early detection (RED) for loss-priority level <b>low</b> specified for a scheduler configured in a dynamic profile for subscriber access. The Junos OS 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 <b>drop-profile</b> statement at the <b>[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name drop-profile-map loss-priority low protocol any]</b> hierarchy level.</p> <p><b>NOTE:</b> The drop profile must be configured statically (at the <b>[edit class-of-service drop-profiles]</b> hierarchy level) for loss-priority <b>low</b>.</p>

Table 46: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-cos-scheduler-dropfile-medium-high	<p>Name of the drop profile for random early detection (RED) for loss-priority level <b>medium-high</b> specified for a scheduler configured in a dynamic profile for subscriber access. The Junos OS 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 <b>drop-profile</b> statement at the <b>[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name drop-profile-map loss-priority medium-high protocol any]</b> hierarchy level.</p> <p><b>NOTE:</b> The drop profile must be configured statically (at the <b>[edit class-of-service drop-profiles]</b> hierarchy level).</p>
\$junos-cos-scheduler-dropfile-medium-low	<p>Name of the drop profile for random early detection (RED) for loss-priority level <b>medium-low</b> specified for a scheduler configured in a dynamic profile for subscriber access. The Junos OS 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 <b>drop-profile</b> statement at the <b>[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name drop-profile-map loss-priority medium-low protocol any]</b> hierarchy level.</p> <p><b>NOTE:</b> The drop profile must be configured statically (at the <b>[edit class-of-service drop-profiles]</b> hierarchy level).</p>
\$junos-cos-scheduler-excess-priority	<p>Priority value of the excess rate specified for a scheduler configured in a dynamic profile for subscriber access. The Junos OS 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 <b>excess-priority</b> statement at the <b>[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]</b> hierarchy level.</p>

Table 46: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-cos-scheduler-excess-rate	<p>Value of the excess rate specified for a scheduler configured in a dynamic profile for subscriber access. The Junos OS 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 <b>excess-rate</b> statement at the <b>[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]</b> hierarchy level.</p>
\$junos-cos-scheduler-shaping-rate	<p>Value of the shaping rate specified for a scheduler configured in a dynamic profile for subscriber access. The Junos OS 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 <b>shaping-rate</b> statement at the <b>[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]</b> hierarchy level.</p>
\$junos-cos-scheduler-tx	<p>Transmit rate specified for a scheduler configured in a dynamic profile for subscriber access. The Junos OS 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 <b>transmit-rate</b> statement at the <b>[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]</b> hierarchy level.</p>
<b>Filters — RADIUS-obtained Policies</b>	
\$junos-input-filter	Attaches a filter based on RADIUS VSA 26-10 (Ingress-Policy-Name) or RADIUS attribute 11 (Filter-ID) to the interface.
\$junos-input-ipv6-filter	Attaches a filter based on RADIUS VSA 26-106 (IPv6-Ingress-Policy-Name) to the interface.
\$junos-output-filter	Attaches a filter based on RADIUS VSA 26-11 (Egress-Policy-Name) to the interface.
\$junos-output-ipv6-filter	Attaches a filter based on RADIUS VSA 26-107 (IPv6-Egress-Policy-Name) to the interface.

Table 46: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
<b>Subscriber Interfaces — Dynamic Demux Interfaces</b>	
<code>\$junos-interface-ifd-name</code>	<p>Name of the device to which the subscriber access client connects. All interfaces are created on this device. Its primary use is in creating single or multiple subscribers on a statically created interface. You specify this variable at the <b>[dynamic-profiles <i>profile-name</i> interfaces]</b> hierarchy level.</p> <p>When creating a logical underlying interface for a dynamic VLAN demux interface, you must also specify this variable at the <b>[dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>\$junos-interface-unit</i> demux-options underlying-interface]</b> hierarchy level.</p>
<code>\$junos-interface-unit</code>	Creates a unit number assigned to the logical interface. The router supplies this information when the subscriber accesses the network. You specify this variable at the <b>[dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i>]</b> hierarchy level for the <b>unit</b> statement.
<code>\$junos-ipv6-address</code>	Selects the IPv6 address of the interface the subscriber uses. You specify this variable at the <b>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>]</b> , <b>[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family <i>family</i>]</b> , <b>[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "<i>\$junos-interface-unit</i>" family <i>family</i>]</b> , and <b>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>]</b> hierarchy level for the <b>address</b> statement.
<code>\$junos-loopback-interface</code>	Selects the loopback interface the subscriber uses. You specify this variable at the <b>[dynamic profiles <i>profile-name</i> interfaces demux0 unit "<i>\$junos-interface-unit</i>" family inet]</b> hierarchy level for the <b>unnumbered-address</b> statement.
<code>\$junos-preferred-source-address</code>	Selects the preferred source address associated with the loopback address used for the subscriber. You specify this variable at the <b>[dynamic profiles <i>profile-name</i> interfaces demux0 unit "<i>\$junos-interface-unit</i>" family inet unnumbered-address "<i>\$junos-loopback-interface</i>"]</b> hierarchy level for the <b>preferred-source-address</b> statement.

Table 46: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
<code>\$junos-subscriber-ip-address</code>	<p>IP address of the subscriber. You specify this variable at the <b>[dynamic-profiles <i>profile-name</i> interfaces <i>demux0</i> unit family <i>inet</i> demux-source]</b> hierarchy level.</p> <p>This variable is also used for creating access-internal routes.</p>
<code>\$junos-underlying-interface</code>	<p>Creates a logical underlying interface for a dynamic IP demux interface. The client logs in on this interface. You specify this variable at the <b>[dynamic-profiles <i>profile-name</i> interfaces <i>demux0</i> unit "<i>\$junos-interface-unit</i>" demux-options]</b> hierarchy level for the <b>underlying-interface</b> statement.</p> <p>When configured, the underlying interface is used to determine the <b><i>\$junos-underlying-interface</i></b>, <b><i>\$junos-underlying-interface-unit</i></b>, and <b><i>\$junos-ifd-name</i></b> variables. For example, if the receiving logical interface is <code>ge-0/0/0.1</code>, the <b><i>\$junos-underlying-interface</i></b> variable is set to <code>ge-0/0/0</code> and the <b><i>\$junos-underlying-interface-unit</i></b> variable is set to <code>1</code>.</p> <p>This variable is also used for creating access-internal routes.</p>
Subscriber Interfaces — Static VLAN Interfaces	
<code>\$junos-interface-ifd-name</code>	<p>Name of the device to which the subscriber access client connects. All interfaces are created on this device. Its primary use is in creating single or multiple subscribers on a statically created interface. You specify this variable at the <b>[dynamic-profiles <i>profile-name</i> interfaces]</b> hierarchy level.</p>
<code>\$junos-underlying-interface-unit</code>	<p>Obtains the unit number for the underlying interface. It specifies the use of the underlying interface for the subscriber. You specify this variable at the <b>[dynamic-profiles <i>profile-name</i> interfaces <i>\$junos-interface-ifd-name</i>]</b> hierarchy for the <b>unit</b> statement.</p>

Table 46: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
<b>Subscriber Interfaces — Dynamic PPPoE Interfaces</b>	
<code>\$junos-interface-unit</code>	Specifies the logical unit number when the router dynamically creates a PPPoE logical interface. The <code>\$junos-interface-unit</code> predefined variable is dynamically replaced with the unit number supplied by the network when the PPPoE subscriber logs in. You specify this variable at the <code>[edit dynamic-profiles profile-name interfaces pp0]</code> hierarchy level for the <code>unit</code> statement.
<code>\$junos-underlying-interface</code>	Specifies the name of the underlying Ethernet interface on which the router dynamically creates the PPPoE logical interface. The <code>\$junos-underlying-interface</code> predefined variable is dynamically replaced with the name of the underlying interface supplied by the network when the PPPoE subscriber logs in. You specify this variable at the <code>[edit dynamic-profiles profile-name interfaces pp0 unit "\$junos-interface-unit" pppoe-options]</code> hierarchy level for the <code>underlying-interface</code> statement.
<b>Wholesale Networking</b>	
<code>\$junos-interface-name</code>	<p>Name of the dynamic interface to which the subscriber access client connects. Its use is in identifying the subscriber interface. You specify this variable at the <code>[dynamic-profiles profile-name routing-instance \$junos-routing-instance]</code> hierarchy level for the <code>interface</code> statement.</p> <p>The interface name is derived from concatenating the <code>\$junos-interface-ld-name</code> and the <code>\$junos-underlying-interface-unit</code> variables obtained when a subscriber is created dynamically at the <code>[dynamic-profiles profile-name routing-instance \$junos-routing-instance interface]</code> hierarchy level.</p>
<code>\$junos-routing-instance</code>	<p>Name of the routing instance to which the subscriber is assigned. This variable triggers a return value from the RADIUS server for Virtual-Router (VSA 26–1).</p> <p>You reference this variable in the statement at the <code>[dynamic-profiles profile-name]</code> hierarchy level for the <code>routing-instance</code> statement.</p>

**Related Documentation**

- [Dynamic Variables Overview on page 371](#)
- [Configuring Predefined Dynamic Variables in Dynamic Profiles on page 392](#)

- Junos OS Predefined Variables That Correspond to RADIUS Attributes and VSAs on page 385
- User-Defined Variables on page 389

## Junos OS Predefined Variables That Correspond to RADIUS Attributes and VSAs

Table 47 on page 385 lists the RADIUS attributes and Juniper Networks VSAs and their corresponding Junos OS predefined variables that are used in dynamic profiles. When the router instantiates a dynamic profile following subscriber access, the Junos OS uses the predefined variable to specify the RADIUS attribute or VSA for the information obtained from the RADIUS server.

**Table 47: RADIUS Attributes and Corresponding Junos OS Predefined Variables**

RADIUS Attribute or VSA	Junos OS Predefined Variable	Description	Default Value Support for Junos OS Predefined Variable
<b>RADIUS Attribute</b>			
Framed-IP-Address (8)	\$junos-framed-route-ip-address	Address for the client	No
Filter-ID (11)	\$junos-input-filter <i>NOTE:</i> Variable is also used for VSA 26–10.	Input filter to apply to client IPv4 interface	Yes
Framed-Route (22)	\$junos-framed-route-ip-address-prefix	(Subattribute 1): Route prefix for access route	No
	\$junos-framed-route-nexthop	(Subattribute 2): Next hop address for access route	No
	\$junos-framed-route-cost	(Subattribute 3): Metric for access route	No
	\$junos-framed-route-distance	(Subattribute 5): Preference for access route	No
	\$junos-framed-route-tag	(Subattribute 6): Tag for access route	No
Framed-IPv6-Route (99)	\$junos-framed-route-ipv6-address-prefix	(Subattribute 1): Framed IPv6 route prefix configured for the client	No
	\$junos-framed-route-ipv6-nexthop	(Subattribute 2): IPv6 routing information configured for the client	No
<b>Juniper Networks VSA</b>			

Table 47: RADIUS Attributes and Corresponding Junos OS Predefined Variables (*continued*)

RADIUS Attribute or VSA	Junos OS Predefined Variable	Description	Default Value Support for Junos OS Predefined Variable
Virtual-Router (26–1)	\$junos-routing-instance	Routing instance to which subscriber is assigned	No
Ingress-Policy-Name (26–10)	\$junos-input-filter  <b>NOTE:</b> Variable is also used for RADIUS attribute 11.	Input filter to apply to client IPv4 interface	Yes
Egress-Policy-Name (26–11)	\$junos-output-filter	Output filter to apply to client IPv4 interface	Yes
IGMP-Enable (26–23)	\$junos-igmp-enable	Enable or disable IGMP on client interface	Yes
IGMP-Access-Name (26–71)	\$junos-igmp-access-group-name	Access list to use for the group (G) filter	Yes
IGMP-Access-Src-Name (26–72)	\$junos-igmp-access-source-group-name	Access List to use for the source group (S,G) filter	Yes
MLD-Access-Name (26–74)	\$junos-mld-access-group-name	Access list to use for the group (G) filter	Yes
MLD-Access-Src-Name (26–75)	\$junos-mld-access-source-group-name	Access List to use for the source group (S,G) filter	Yes
MLD-Version (26–77)	\$junos-mld-version	MLD protocol version	Yes
IGMP-Version (26–78)	\$junos-igmp-version	IGMP protocol version	Yes
IGMP-Immediate-Leave (26–97)	\$junos-igmp-immediate-leave	IGMP immediate leave	Yes
MLD-Immediate-Leave (26–100)	\$junos-mld-immediate-leave	MLD immediate leave	Yes
IPv6-Ingress-Policy-Name (26–106)	\$junos-input-ipv6-filter	Input filter to apply to client IPv6 interface	Yes
IPv6-Egress-Policy-Name (26–107)	\$junos-output-ipv6-filter	Output filter to apply to client IPv6 interface	Yes



Table 47: RADIUS Attributes and Corresponding Junos OS Predefined Variables (*continued*)

RADIUS Attribute or VSA	Junos OS Predefined Variable	Description	Default Value Support for Junos OS Predefined Variable
CoS-Shaping-Parameter-Type (26–108)	\$junos-cos-scheduler-map	(T01: Scheduler-map name) Name of scheduler map configured in traffic-control profile	Yes
	\$junos-cos-shaping-rate	(T02: Shaping rate) Shaping rate configured in traffic-control profile	Yes
	\$junos-cos-guaranteed-rate	(T03: Guaranteed rate) Guaranteed rate configured in traffic-control profile	Yes
	\$junos-cos-delay-buffer-rate	(T04: Delay-buffer rate) Delay-buffer rate configured in traffic-control profile	Yes
	\$junos-cos-excess-rate	(T05; Excess rate) Excess rate configured in traffic-control profile	Yes
	\$junos-cos-shaping-mode	(T07; Shaping mode) CoS shaping mode configured in a dynamic profile	Yes
	\$junos-cos-byte-adjust	(T08; Byte adjust) Byte adjustments configured for the shaping mode in a dynamic profile	Yes
IPv6-NdRa-Prefix (26–129)	\$junos-ipv6-ndra-prefix	Prefix value in IPv6 Neighbor Discovery route advertisements	No
Qos-Set-Name (26–130)	\$junos-interface-set-name	Name of an interface set configured in a dynamic profile	Yes
CoS-Scheduler-Pmt-Type (26–146)	\$junos-cos-scheduler	(Null: Scheduler name) Name of scheduler configured in a dynamic profile	Yes

Table 47: RADIUS Attributes and Corresponding Junos OS Predefined Variables (*continued*)

RADIUS Attribute or VSA	Junos OS Predefined Variable	Description	Default Value Support for Junos OS Predefined Variable
	\$junos-cos-scheduler-tx	(T01: CoS scheduler transmit rate) Transmit rate for scheduler configured in a dynamic profile	Yes  Available for multiple parameters: <ul style="list-style-type: none"> <li>• Percent</li> <li>• Rate</li> </ul>
	\$junos-cos-scheduler-bs	(T02: CoS scheduler buffer size) Buffer size for scheduler configured in a dynamic profile	Yes  Available for multiple parameters: <ul style="list-style-type: none"> <li>• Percent</li> <li>• Temporal</li> </ul>
	\$junos-cos-scheduler-pri	(T03: CoS scheduler priority) Packet-scheduling priority for scheduler configured in a dynamic profile	Yes
	\$junos-cos-scheduler-dropfile-low	(T04: CoS scheduler drop-profile low) Name of drop profile for RED loss-priority level <b>low</b> for scheduler configured in a dynamic profile	Yes
	\$junos-cos-scheduler-dropfile-medium-low	(T05: CoS scheduler drop-profile medium-low) Name of drop profile for RED loss-priority level <b>medium-low</b> for scheduler configured in a dynamic profile	Yes
	\$junos-cos-scheduler-dropfile-medium-high	(T06: CoS scheduler drop-profile medium-high) Name of drop profile for RED loss-priority level <b>medium-high</b> for scheduler configured in a dynamic profile	Yes

Table 47: RADIUS Attributes and Corresponding Junos OS Predefined Variables (*continued*)

RADIUS Attribute or VSA	Junos OS Predefined Variable	Description	Default Value Support for Junos OS Predefined Variable
	\$junos-cos-scheduler-dropfile-high	(T07: CoS scheduler drop-profile high) Name of drop profile for RED loss-priority level <b>high</b> for scheduler configured in a dynamic profile	Yes
	\$junos-cos-scheduler-dropfile-any	(T08: CoS scheduler drop-profile any) Name of drop profile for RED loss-priority level <b>any</b> for scheduler configured in a dynamic profile	Yes
	\$junos-cos-scheduler-excess-rate	(T09: CoS scheduler excess rate) Excess rate configured for a scheduler in a dynamic profile	Yes  Available for multiple parameters: <ul style="list-style-type: none"> <li>• Percent</li> <li>• Proportion</li> </ul>
	\$junos-cos-scheduler-shaping-rate	(T10: CoS scheduler shaping rate) Shaping rate configured for a scheduler in a dynamic profile	Yes  Available for multiple parameters: <ul style="list-style-type: none"> <li>• Percent</li> <li>• Rate</li> </ul>
	\$junos-cos-scheduler-excess-priority	(T11: CoS scheduler excess priority) Excess priority configured for a scheduler in a dynamic profile	Yes

- Related Documentation**
- Dynamic Variables Overview on page 371
  - Configuring Predefined Dynamic Variables in Dynamic Profiles on page 392
  - Junos OS Predefined Variables on page 372

## User-Defined Variables

Junos OS 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 39.

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  
Documentation**

- [Dynamic Profiles Overview on page 369](#)
- [Configuring User-Defined Dynamic Variables in Dynamic Profiles on page 394](#)
- [RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 39](#)
- [Junos OS Predefined Variables on page 372](#)

# Configuring Dynamic Profiles

- Configuring a Basic Dynamic Profile on page 391
- Configuring Predefined Dynamic Variables in Dynamic Profiles on page 392
- Configuring Default Values for Predefined Variables in a Dynamic Profile on page 393
- Configuring User-Defined Dynamic Variables in Dynamic Profiles on page 394
- Configuring a Dynamic Profile for Client Access on page 395
- Configuring a Dynamic Profile for Various Levels of Services on page 397
- Modifying Dynamic Profiles on page 398

## 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 an interface variable name (such as **\$junos-interface-ifd-name**) included at the **[edit dynamic-profiles *profile-name* interfaces** hierarchy level and logical interface variable name (such as **\$junos-underlying-interface-unit** or **\$junos-interface-unit**) at the **[edit dynamic-profiles *profile-name* interfaces *variable-interface-name* unit]** hierarchy level.

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 433 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 26

To configure a basic dynamic profile:

1. Name the profile.  
  
[edit]  
user@host# edit 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# edit interfaces $junos-interface-ifd-name
```

3. Define the **unit** statement with the internal variable:

- When referencing an existing interface, specify the **\$junos-underlying-interface-unit** variable used by the router to match the unit value of the receiving interface.
- When creating dynamic interfaces, specify the **\$junos-interface-unit** variable used by the router to generate a unit value for the interface.

```
[edit dynamic-profiles basic-profile interfaces "$junos-interface-ifd-name"]
user@host# set unit $junos-underlying-interface-unit
```

or

```
[edit dynamic-profiles basic-profile interfaces "$junos-interface-ifd-name"]
user@host# set unit $junos-interface-unit
```

#### Related Documentation

- [Configuring a Dynamic Profile for Client Access on page 395](#)
- [Configuring a Dynamic Profile for Various Levels of Services on page 397](#)
- [Configuring Predefined Dynamic Variables in Dynamic Profiles on page 392](#)
- [Configuring Static Subscriber Interfaces in Dynamic Profiles on page 439](#)
- [Configuring VLAN Dynamic Profiles on page 409](#)
- [Dynamic Profiles Overview on page 369](#)
- [Dynamic Variables Overview on page 371](#)
- [Junos OS Predefined Variables on page 372](#)
- [Example: Firewall Dynamic Profile on page 402](#)
- [Example: IGMP Dynamic Profile on page 401](#)

---

## Configuring Predefined Dynamic Variables in Dynamic Profiles

This topic discusses how to configure predefined 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 **[edit 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 391.
2. Ensure that the router hardware is configured in the network to accept subscriber access.

To configure predefined variables in a dynamic profile:

1. Access the desired dynamic profile.

```
[edit]
user@host# edit dynamic-profiles igmpProfile1
[edit dynamic-profiles igmpProfile1]
```

2. Configure the necessary variables.

```
[edit dynamic-profiles igmpProfile1]
user@host# set protocols igmp interface $junos-interface-name
```

For a complete list of supported predefined variables, see “Junos OS Predefined Variables” on page 372.

#### Related Documentation

- Configuring a Basic Dynamic Profile on page 391
- Configuring User-Defined Dynamic Variables in Dynamic Profiles on page 394
- Dynamic Profiles Overview on page 369
- Dynamic Variables Overview on page 371
- Junos OS Predefined Variables on page 372
- Example: Firewall Dynamic Profile on page 402
- Example: IGMP Dynamic Profile on page 401

## Configuring Default Values for Predefined Variables in a Dynamic Profile

You can configure default values for the predefined variables that are configured in a dynamic profile. These default values are used when RADIUS does not supply a value.

To configure default values for Junos predefined variables:

1. Specify that you want to configure the dynamic profile.

```
[edit]
user@host# edit dynamic-profile profile-name
```

2. Configure the default value for the predefined variable.

```
[edit dynamic-profiles profile-name]
user@host# set predefined-variable-defaults predefined-variable variable-option
default-value
```



**NOTE:** Do not use the “junos-” prefix when specifying the *predefined-variable*.

#### Related Documentation

- For a list of variables for which you can configure default values, see Junos OS Predefined Variables That Correspond to RADIUS Attributes and VSAs on page 385
- Junos OS Predefined Variables on page 372

- Dynamic Variables Overview on page 371

## 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 **[edit 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 391.
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 21.
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 26

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 igmpProfile1 variables]
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 igmpProfile1 variables]
```



```
user@host# set igmp-version default-value 3
```



**NOTE:** You can configure variables by 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 Documentation

- Dynamic Profiles Overview on page 369
- Dynamic Variables Overview on page 371
- Configuring a Basic Dynamic Profile on page 391
- User-Defined Variables on page 389
- Configuring Predefined Dynamic Variables in Dynamic Profiles on page 392
- Example: Configuring Dynamic Hierarchical Scheduling and Queuing for Subscriber Access on page 715
- Example: Firewall Dynamic Profile on page 402
- Example: IGMP Dynamic Profile on page 401

## 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 391.
2. Configure the necessary router interfaces that you want accessing DHCP clients to use.  
See “Subscriber Interface Overview” on page 433 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 21.

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 26

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-interface-name
```

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) 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 Documentation**
- Configuring a Basic Dynamic Profile on page 391
  - Dynamic Profiles Overview on page 369

## 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 391.
2. Configure a dynamic profile that enables DHCP clients access to the network.  
See “Configuring a Dynamic Profile for Client Access” on page 395



**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 21.
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 26

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 395.
3. (Optional) Specify any filters for the interface.  
See “Dynamically Attaching Statically Created Filters for Any Interface Type” on page 572, “Dynamically Attaching Statically Created Filters for a Specific Interface

Family Type” on page 571, or “Dynamically Attaching Filters Using RADIUS Variables” on page 573.

4. Define any CoS values for the service level you want this profile to configure on the interface.

- Related Documentation**
- Configuring a Basic Dynamic Profile on page 391
  - Dynamic Profiles Overview on page 369

---

## Modifying Dynamic Profiles

You use dynamic profiles to configure large groups of subscribers. However, after you have configured and applied dynamic profiles, be cautious 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 Documentation**
- [Configuring a Basic Dynamic Profile on page 391](#)
  - [Dynamic Profiles Overview on page 369](#)



# Dynamic Profile Examples

- Example: IGMP Dynamic Profile on page 401
- Example: Firewall Dynamic Profile on page 402
- Example: Minimum MLPPP Dynamic Profile on page 402
- Example: Minimum PPPoE Dynamic Profile on page 403
- Example: Subscriber Secure Policy Dynamic Profile on page 403

## Example: IGMP Dynamic Profile

In this example, IGMP is configured for subscriber access using Junos OS predefined variables.

The predefined variables equate to RADIUS settings as follows:

Junos OS Predefined Variable	RADIUS VSA Name	RADIUS Attribute Number
\$var-igmp-version	IGMP-Version	26–78
\$var-igmp-access-grp	IGMP-Access-Name	26–71
\$var-igmp-access-src-grp	IGMP-Access-Src-Name	26–72

```
[edit dynamic-profiles profile-name]  
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 Junos IPv4 predefined variables.

The predefined variables equate to RADIUS settings as follows:

Junos OS Predefined Variable	RADIUS VSA Name	RADIUS Attribute Number
\$junos-input-filter	Ingress-Policy-Name	26–10
\$junos-output-filter	Egress-Policy-Name	26–11

```

dynamic-profiles {
  DynamicFilterProfile {
    interfaces {
      "$junos-interface-ifd-name" {
        unit "$junos-underlying-interface-unit" {
          family inet {
            filter {
              input "$junos-input-filter";
              output "$junos-output-filter";
            }
          }
        }
      }
    }
  }
}

```



**NOTE:** You must also configure any global firewall parameters.

## Example: Minimum MLPPP Dynamic Profile

This example shows the minimum configuration for a dynamic profile that is used for static LSQ MLPPP bundle interfaces.

```

dynamic-profiles {
  mlppp-profile-1 {

```



```

    interfaces {
        "$junos-interface-ifd-name" {
            unit "$junos-underlying-interface-unit";
        }
    }
}

```

**Related  
Documentation**

- [Dynamic Profiles for PPP Subscriber Interfaces Overview on page 217](#)
- [Attaching Dynamic Profiles to MLPPP Bundles on page 227](#)

## Example: Minimum PPPoE Dynamic Profile

This example shows the minimum configuration for a dynamic profile that is used for static PPPoE interfaces. The configuration must include the **interfaces pp0** stanza.

```

dynamic-profiles {
  ppp-profile-1 {
    interfaces {
      pp0 {
        unit "$junos-interface-unit";
      }
    }
  }
}

```

**Related  
Documentation**

- [Dynamic Profiles for PPP Subscriber Interfaces Overview on page 217](#)
- [Configuring Dynamic Authentication for PPP Subscribers on page 219](#)
- [Attaching Dynamic Profiles to Static PPP Subscriber Interfaces on page 223](#)

## Example: Subscriber Secure Policy Dynamic Profile

In this example, subscriber secure policy mirroring is configured for subscriber access using user-defined variables and Junos OS predefined variables. This example is for the flow-tap service configured on a router without a Tunnel Services PIC.

The user-defined variables equate to RADIUS settings as follows:

User-Defined Variable Name	Junos OS Variable	RADIUS VSA Name	RADIUS Attribute Number	Example RADIUS Setting
ssp-intercept-id	\$ssp-intercept-id	Med-Dev-Handle	26-59	subscriber-bg-2350
ssp-destination-addr	\$ssp-destination-addr	Med-IP-Address	26-60	192.163.100.22
ssp-destination-port	\$ssp-destination-port	Med-Port-Number	26-61	2222

```

variables {
  var ssp-intercept-id;
}

```

```
var ssp-destination-addr;
var ssp-destination-port;
}
interfaces {
  <*> {
    unit <*> {
      family inet {
        filter {
          input ssp;
          output ssp;
        }
      }
    }
  }
}
firewall {
  family inet {
    filter ssp {
      term $ssp-id {
        from {
          # optional classifiers.
        }
        then {
          flowtap-destination-address $ssp-destination-addr;
          flowtap-destination-port $ssp-destination-port;
          flowtap;
        }
      }
    }
  }
}
```

## PART 10

# Dynamic VLANs

- [Dynamic VLAN Overview on page 407](#)
- [Configuring Dynamic VLANs on page 409](#)
- [Dynamic VLAN Examples on page 427](#)



# Dynamic VLAN Overview

- Dynamic 802.1Q VLAN Overview on page 407

## Dynamic 802.1Q VLAN Overview

---

You can identify VLANs statically or dynamically. You can also configure a mix of static and dynamic VLANs on the same underlying interface.

For Ethernet, Fast Ethernet, Tri-Rate Ethernet copper, Gigabit Ethernet, 10-Gigabit Ethernet, and aggregated Ethernet interfaces supporting VPLS, the Junos OS supports a subset of the IEEE 802.1Q standard for channelizing an Ethernet interface into multiple logical interfaces. Many hosts can be connected to the same Gigabit Ethernet switch, but they cannot be in the same routing or bridging domain.

To identify VLANs statically, you can reference a static VLAN interface in a dynamic profile. To identify subscribers dynamically, you use a variable to specify an 802.1Q VLAN that is dynamically created when a subscriber accesses the network.

## Static VLAN Configuration

Static VLAN configuration is not described in this guide. For information about how to statically configure VLANs and stacked VLANs, see the [Junos OS Network Interfaces Configuration Guide](#). For an example of how to configure static VLANs in a subscriber access network, see the [Junos OS Broadband Subscriber Management Solutions Guide](#).

## Dynamic VLAN Configuration

You can configure the router to dynamically create VLANs when a client accesses an interface and requests a VLAN ID that does not yet exist. When a client accesses a particular interface, the router instantiates a VLAN dynamic profile that you have associated with the interface. Using the settings in the dynamic profile, the router extracts information about the client from the incoming packet (for example, the interface and unit values), saves this information in the routing table, and creates a VLAN or stacked VLAN ID for the client from a range of VLAN IDs that you configure for the interface.



**NOTE:** Dynamic VLAN configuration supports the creation of IPv4 (inet), DHCPv4, IPv6 (inet6), and DHCPv6 VLANs.

Dynamically configuring VLANs or stacked VLANs requires the following general steps:

1. Configure a dynamic profile for dynamic VLAN or dynamic stacked VLAN creation.  
See “Configuring VLAN Dynamic Profiles” on page 409.
2. Associate the VLAN or stacked VLAN dynamic profile with the interface.  
See “Configuring VLAN Interfaces to Use Dynamic Profiles” on page 416.
3. Specify the Ethernet packet type that the VLAN dynamic profile accepts.  
See “Configuring Which VLAN Ethernet Packet Types Dynamic Profiles Can Accept” on page 417.
4. Define VLAN ranges for use by the dynamic profile when creating VLAN IDs.  
See “Configuring VLAN Ranges for Use with Dynamic Profiles” on page 419.

# Configuring Dynamic VLANs

- Configuring VLAN Dynamic Profiles on page 409
- Configuring VLAN Interfaces to Use Dynamic Profiles on page 416
- Configuring Which VLAN Ethernet Packet Types Dynamic Profiles Can Accept on page 417
- Configuring an Authentication Password for VLAN or Stacked VLAN Ranges on page 418
- Configuring VLAN Ranges for Use with Dynamic Profiles on page 419
- Configuring Dynamic Authentication for VLAN Interfaces on page 424
- Configuring VLAN Interface Username Information for AAA Authentication on page 425
- Verifying and Managing Dynamic VLAN Configuration on page 426

## Configuring VLAN Dynamic Profiles

---

Creating dynamic single-tag VLANs or stacked (dual-tag) VLANs requires the use of dynamic profiles. The dynamic profile automatically references the VLAN interface and creates the interface unit and the necessary VLAN IDs for each new single-tag VLAN or stacked VLAN.



**NOTE:** VLAN dynamic profiles do not support user-defined variables. Use only Junos VLAN predefined variables when configuring VLAN dynamic profiles. See “Dynamic Variables Overview” on page 371 for information about dynamic variables.

- Configuring a VLAN Dynamic Profile for Creating Single-Tag VLANs Using Standard TPID Values on page 410
- Configuring a VLAN Dynamic Profile for Creating Single-Tag VLANs Using Any TPID Values on page 411
- Configuring a Stacked VLAN Dynamic Profile on page 413
- Configuring a VLAN Dynamic Profile That Associates VLAN Interfaces with Separate Routing Instances on page 414

## Configuring a VLAN Dynamic Profile for Creating Single-Tag VLANs Using Standard TPID Values

You can configure a VLAN dynamic profile to create single-tag VLANs that accept only standard TPID values (a TPID value of 0x8100) by using the **vlan-id** statement and the **\$junos-vlan-id** variable.



**NOTE:** This procedure configures a dynamic profile that accepts only TPID values of 0x8100. To configure a VLAN dynamic profile for creating VLANs using any TPID values, see “Configuring a VLAN Dynamic Profile for Creating Single-Tag VLANs Using Any TPID Values” on page 411.

Before you begin:

- Configure the dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 391.

To configure a dynamic VLAN profile:

1. Ensure that the VLAN dynamic profile uses the **\$junos-interface-ifd-name** variable for the dynamic interface and the **\$junos-interface-unit** variable for the interface unit.
2. (Optional) To support dynamic demux interfaces, enable them using the **demux-source** statement.

- a. For IPv4 demux interfaces, specify **inet** as the source type.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit  
"$junos-interface-unit"]  
user@host# set demux-source inet
```

- b. For IPv6 demux interfaces, specify **inet6** as the source type.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit  
"$junos-interface-unit"]  
user@host# set demux-source inet6
```

3. (Optional) To configure the router to respond to any ARP request, specify the **proxy-arp** statement.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit  
"$junos-interface-unit"]  
user@host# set proxy-arp
```

4. Specify that you want to use dynamic VLAN IDs in the dynamic profile.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit  
"$junos-interface-unit"]  
user@host# set vlan-id $junos-vlan-id
```

When the dynamic profile is instantiated, the variable is dynamically replaced with a VLAN ID within the VLAN range specified at the **[interfaces]** hierarchy level.

5. Define the unit family type.
  - a. For IPv4 interfaces, specify the **inet** family type.



```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set family inet
```

- b. For IPv6 interfaces, specify the **inet6** family type.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set family inet6
```

6. (Optional) Enable IP and MAC address validation for dynamic demux interfaces in a dynamic profile.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit" family inet]
user@host# set mac-validate strict
```

7. Specify the unnumbered address and preferred source address.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit" family inet]
user@host# set unnumbered-address lo.0 preferred-source-address 192.0.16.1
```

## Configuring a VLAN Dynamic Profile for Creating Single-Tag VLANs Using Any TPID Values

You can configure a VLAN dynamic profile to create single-tag VLANs that accept any TPID values by configuring the **vlan-tags** statement and the **\$junos-vlan-id** variable.



**NOTE:** For procedures to configure a VLAN dynamic profile for creating single-tag VLANs that use only standard TPID values (a TPID value of 0x8100), see “Configuring a VLAN Dynamic Profile for Creating Single-Tag VLANs Using Standard TPID Values” on page 410.

Before you begin:

- Configure the dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 391.

To configure a dynamic VLAN profile:

1. Ensure that the VLAN dynamic profile uses the **\$junos-interface-ifd-name** variable for the dynamic interface and the **\$junos-interface-unit** variable for the interface unit.
2. (Optional) To support dynamic demux interfaces, enable them using the **demux-source** statement.

- a. For IPv4 demux interfaces, specify **inet** as the source type.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set demux-source inet
```

- b. For IPv6 demux interfaces, specify **inet6** as the source type.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set demux-source inet6
```

3. (Optional) To configure the router to respond to any ARP request, specify the **proxy-arp** statement.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set proxy-arp
```

4. Specify that you want to use dynamic VLAN IDs in the dynamic profile.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set vlan-tags outer $junos-vlan-id
```

The variable is dynamically replaced with both the TPID value and a VLAN ID within the VLAN range specified at the **[interfaces]** hierarchy level.

5. Define the unit family type.

- a. For IPv4 interfaces, specify the **inet** family type.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set family inet
```

- b. For IPv6 interfaces, specify the **inet6** family type.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set family inet6
```

6. (Optional) Enable IP and MAC address validation for dynamic demux interfaces in a dynamic profile.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit" family inet]
user@host# set mac-validate strict
```

7. Specify the unnumbered address and preferred source address.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit" family inet]
user@host# set unnumbered-address lo.0 preferred-source-address 192.0.16.1
```

## Configuring a Stacked VLAN Dynamic Profile

You can configure a dynamic profile for creating stacked 802.1Q VLANs.

Before you begin:

- Configure the dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 391.

To configure a stacked VLAN dynamic profile:

1. Ensure that the VLAN dynamic profile uses the **\$junos-interface-ifd-name** variable for the dynamic interface and the **\$junos-interface-unit** variable for the interface unit.
2. (Optional) To support dynamic demux interfaces, enable them using the **demux-source** statement.

- a. For IPv4 demux interfaces, specify **inet** as the source type.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set demux-source inet
```

- b. For IPv6 demux interfaces, specify **inet6** as the source type.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set demux-source inet6
```

3. (Optional) To configure the router to respond to any ARP request, specify the **proxy-arp** statement.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set proxy-arp
```

4. Specify the outer VLAN ID variable.

```
[edit dynamic-profiles STACKED-VLAN-PROF1 interfaces "$junos-interface-ifd-name"
unit "$junos-interface-unit"]
user@host# set vlan-tags outer $junos-stacked-vlan-id
```

The variable is dynamically replaced with an outer VLAN ID within the VLAN range specified at the **[interfaces]** hierarchy level.

5. Specify the inner VLAN ID variable.

```
[edit dynamic-profiles STACKED-VLAN-PROF1 interfaces "$junos-interface-ifd-name"
unit "$junos-interface-unit"]
user@host# set vlan-tags inner $junos-vlan-id
```

The variable is dynamically replaced with an inner VLAN ID within the VLAN range specified at the **[interfaces]** hierarchy level.

6. Define the unit family type.

- a. For IPv4 interfaces, specify the **inet** family type.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set family inet
```

- b. For IPv6 interfaces, specify the **inet6** family type.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set family inet6
```

7. (Optional) Enable IP and MAC address validation for dynamic demux interfaces in a dynamic profile.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit" family inet]
user@host# set mac-validate strict
```

8. Specify the unnumbered address and preferred source address.

```
[edit dynamic-profiles VLAN-PROF1 interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit" family inet]
user@host# set unnumbered-address lo.0 preferred-source-address 192.0.16.1
```

## Configuring a VLAN Dynamic Profile That Associates VLAN Interfaces with Separate Routing Instances

You can configure a VLAN dynamic profile that dynamically creates underlying VLAN interfaces and associates these interfaces with dynamically created routing instances. The VLAN interface is created in the default logical system (LS) for a specific routing instance as defined by VSA 26–1 (Virtual-Router) on the AAA server (for example, RADIUS server).

To configure a dynamic VLAN profile using routing instances:

1. Name the profile.

```
[edit]
user@host# edit dynamic-profiles VLAN_PROFILE_RI
```

2. Specify that you want to dynamically create routing instances on the default logical system.

```
[edit dynamic-profiles VLAN_PROFILE_RI]
user@host# edit routing-instances $junos-routing-instance
```

3. Define the routing instance **interface** statement with the internal **\$junos-interface-name** variable used by the router to match the interface name of the receiving interface.

```
[edit dynamic-profiles VLAN_PROFILE_RI routing-instances "$junos-routing-instance"]
user@host# set interface $junos-interface-name
```

4. Define the dynamic profile **interfaces** statement with the internal **\$junos-interface-ifd-name** variable.

```
[edit dynamic-profiles VLAN_PROFILE_RI]
user@host# edit interfaces $junos-interface-ifd-name
```

5. Define the **unit** statement with the internal **\$junos-interface-unit** variable used by the router to generate a unit value for the interface.

```
[edit dynamic-profiles VLAN_PROFILE_RI interfaces "$junos-interface-ifd-name"]
user@host# edit unit $junos-interface-unit
```

6. To support dynamic demux interfaces, enable them using the **demux-source** statement.

- a. For IPv4 demux interfaces, specify **inet** as the source type.

```
[edit dynamic-profiles VLAN_PROFILE interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set demux-source inet
```

- b. For IPv6 demux interfaces, specify **inet6** as the source type.

```
[edit dynamic-profiles VLAN_PROFILE interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set demux-source inet6
```

7. (Optional) To configure the router to respond to any ARP request, specify the **proxy-arp** statement.

```
[edit dynamic-profiles VLAN_PROFILE_RI interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set proxy-arp
```

8. Specify that you want to use dynamic VLAN IDs in the dynamic profile.

```
[edit dynamic-profiles VLAN_PROFILE_RI interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set vlan-id $junos-vlan-id
```

The variable is dynamically replaced with both the TPID value and a VLAN ID within the VLAN range specified at the **[interfaces]** hierarchy level.

9. Define the unit family type.

- a. For IPv4 interfaces, specify the **inet** family type.

```
[edit dynamic-profiles VLAN_PROFILE interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set family inet
```

- b. For IPv6 interfaces, specify the **inet6** family type.

```
[edit dynamic-profiles VLAN_PROFILE interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set family inet6
```

10. (Optional) Enable IP and MAC address validation for dynamic demux interfaces in a dynamic profile.

```
[edit dynamic-profiles VLAN_PROFILE_RI interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit" family inet]
user@host# set mac-validate strict
```

11. Specify the unnumbered address to dynamically create loopback interfaces.



**NOTE:** You can optionally specify the preferred source address. This option is included in the step.

```
[edit dynamic-profiles VLAN_PROFILE_RI interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit" family inet]
user@host# set unnumbered-address $junos-loopback-interface
preferred-source-address 192.0.16.1
```

## Configuring VLAN Interfaces to Use Dynamic Profiles

---

You can configure an interface to use a single-tag VLAN or stacked (dual-tag) VLAN dynamic profile when creating dynamic VLANs. The dynamic profile assigns a VLAN ID to each VLAN dynamically created over the interface by using the single-tag VLAN and stacked VLAN ranges configured for the VLAN interface. You can configure VLAN interfaces to use dynamic profiles in the following ways:

- Associating a Single-Tag VLAN Dynamic Profile with an Interface on page 416
- Associating a Stacked VLAN Dynamic Profile with an Interface on page 416

### Associating a Single-Tag VLAN Dynamic Profile with an Interface

Before you begin:

- Configure the VLAN dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 391.

To associate a single-tag VLAN dynamic profile with an interface:

1. Access the interface that you want to use for creating VLANs.

```
[edit]
user@host# edit interfaces ge-1/0/0
```

2. Edit the **auto-configure** stanza to automatically configure VLANs.

```
[edit interfaces ge-1/0/0]
user@host# edit auto-configure
```

3. Edit the **vlan-ranges** stanza.

```
[edit interfaces ge-1/0/0 auto-configure]
user@host# edit vlan-ranges
```

4. Specify the dynamic VLAN profile that you want the interface to use.

```
[edit interfaces ge-1/0/0 auto-configure vlan-ranges]
user@host# set dynamic-profile VLAN-PROF1
```

### Associating a Stacked VLAN Dynamic Profile with an Interface

To associate a stacked (dual-tag) VLAN dynamic profile with an interface:

1. Access the interface that you want to use for creating VLANs.

```
[edit interfaces]
user@host# edit interfaces ge-1/0/0
```

2. Edit the **auto-configure** stanza to automatically configure the stacked VLANs.

```
[edit interfaces ge-1/0/0]
```

```
user@host# edit auto-configure
```

3. Edit the **stacked-vlan-ranges** stanza.

```
[edit interfaces ge-1/0/0 auto-configure]
```

```
user@host# edit stacked-vlan-ranges
```

4. Specify the dynamic VLAN profile that you want the interface to use.

```
[edit interfaces ge-1/0/0 auto-configure stacked-vlan-ranges]
```

```
user@host# set dynamic-profile STACKED-VLAN-PROF1
```

## Configuring Which VLAN Ethernet Packet Types Dynamic Profiles Can Accept

To create dynamic single-tag VLANs and dynamic stacked (dual-tag) VLANs, you must specify what Ethernet packet type you want the single-tag VLAN or stacked VLAN dynamic profile to accept. You can configure which VLAN Ethernet packet types a dynamic profile accepts in the following ways:

- Configuring the VLAN Ethernet Packet Type for Single-Tag VLAN Dynamic Profiles on page 417
- Configuring the VLAN Ethernet Packet Type for Stacked VLAN Dynamic Profiles on page 418

### Configuring the VLAN Ethernet Packet Type for Single-Tag VLAN Dynamic Profiles

To configure the VLAN Ethernet packet type the VLAN dynamic profile can accept:

1. Access the interface over which you want to create dynamic VLANs.

```
user@host# edit interfaces ge-0/0/0
```

2. Edit the VLAN **auto-configure** stanza.

```
[edit interfaces ge-0/0/0]
```

```
user@host# edit auto-configure
```

3. Edit the **vlan-ranges** stanza.

```
[edit interfaces ge-0/0/0 auto-configure]
```

```
user@host# edit vlan-ranges
```

4. Access the VLAN dynamic profile for which you want to configure VLAN ranges.

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]
```

```
user@host# edit dynamic-profile VLAN-PROF1
```

5. Specify what VLAN Ethernet packet type the VLAN or stacked VLAN dynamic profile accepts.



**NOTE:** This release supports **inet** and **dhcp-v4** Ethernet packet types for IPv4 packets and **inet6** and **dhcp-v6** Ethernet packet types for IPv6 packets.

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]
```

```
user@host# set accept inet
```

## Configuring the VLAN Ethernet Packet Type for Stacked VLAN Dynamic Profiles

To configure the VLAN Ethernet packet type the stacked VLAN dynamic profile can accept:

1. Access the interface over which you want to create dynamic VLANs.

```
user@host# edit interfaces ge-0/0/0
```

2. Edit the VLAN **auto-configure** stanza.

```
[edit interfaces ge-0/0/0]  
user@host# edit auto-configure
```

3. Edit the **stacked-vlan-ranges** stanza.

```
[edit interfaces ge-0/0/0 auto-configure]  
user@host# edit stacked-vlan-ranges
```

4. Access the VLAN dynamic profile for which you want to configure VLAN ranges.

```
[edit interfaces ge-0/0/0 auto-configure stacked-vlan-ranges]  
user@host# edit dynamic-profile STACKED-VLAN-PROFI
```

5. Specify what VLAN Ethernet packet type the stacked VLAN dynamic profile accepts.



**NOTE:** This release supports **inet** and **dhcp-v4** Ethernet packet types for IPv4 packets and **inet6** and **dhcp-v6** Ethernet packet types for IPv6 packets.

```
[edit interfaces ge-0/0/0 auto-configure stacked-vlan-ranges]  
user@host# set accept inet
```

---

## Configuring an Authentication Password for VLAN or Stacked VLAN Ranges

You can specify an authentication password for dynamically created VLAN or stacked VLAN interfaces at the **[edit interfaces *interface-name* auto-configure vlan-ranges authentication]** or **[edit interfaces *interface-name* auto-configure stacked-vlan-ranges authentication]** hierarchy level. This password is sent to the external AAA authentication server for subscriber authentication.



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

To configure an authentication password:

1. Access the interface over which you want to create dynamic VLANs.

```
user@host# edit interfaces ge-0/0/0
```

2. Edit the VLAN **auto-configure** stanza.



```
[edit interfaces ge-0/0/0]
user@host# edit auto-configure
```

3. Edit the **vlan-ranges** or **stacked-vlan-ranges** stanza.

```
[edit interfaces ge-0/0/0 auto-configure]
user@host# edit vlan-ranges
```

or

```
[edit interfaces ge-0/0/0 auto-configure]
user@host# edit stacked-vlan-ranges
```

4. Edit the VLAN **authentication** stanza.

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]
user@host# edit authentication
```

5. Specify a password that is sent to the external AAA authentication server for subscriber authentication.

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]
user@host# set password PSSWD1
```

#### Related Documentation

- Configuring Dynamic Authentication for VLAN Interfaces on page 424

## Configuring VLAN Ranges for Use with Dynamic Profiles

You define dynamic VLAN ranges under the **[edit interfaces]** hierarchy. You can configure VLAN ranges in the following ways for use with dynamic profiles:

- Configuring Single-Level VLAN Ranges for Use with VLAN Dynamic Profiles on page 419
- Configuring Stacked VLAN Ranges for Use with Stacked VLAN Dynamic Profiles on page 420
- Configuring Dynamic Mixed VLAN Ranges on page 422
- Configuring VLAN Dynamic Profile Override on page 423

### Configuring Single-Level VLAN Ranges for Use with VLAN Dynamic Profiles

You configure VLAN ranges at the **[edit interfaces]** hierarchy level by specifying the **vlan-tagging** statement for the interface and defining up to 32 VLAN ranges for use with a VLAN dynamic profile.

To configure a VLAN range:

1. Access the interface over which you want to create dynamic VLANs.

```
user@host# edit interfaces ge-0/0/0
```

2. Specify the **vlan-tagging** statement to indicate that this interface is for use with stacked VLAN ranges.

```
[edit interfaces ge-0/0/0]
user@host# set vlan-tagging
```

3. Access the VLAN **[auto-configure]** hierarchy level.

```
[edit interfaces ge-0/0/0]
user@host# edit auto-configure
```

4. Access the **[vlan-ranges]** hierarchy level.

```
[edit interfaces ge-0/0/0 auto-configure]
user@host# edit vlan-ranges
```

5. Access the VLAN dynamic profile for which you want to configure VLAN ranges.

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]
user@host# edit dynamic-profile VLAN-PROF1
```

6. Specify the VLAN ranges that you want the dynamic profile to use. The following example specifies a lower VLAN ID limit of 3000 and any upper VLAN ID limit (a range from 1 through 4094).

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]
user@host# set ranges 3000-any
```



**NOTE:** You can configure multiple VLAN range groups (up to 32 total) on the same physical interface that use different VLAN dynamic profiles.

7. (Optional) Access another VLAN dynamic profile for which you want to configure VLAN ranges.

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]
user@host# edit dynamic-profile VLAN-PROF2
```

8. (Optional) Specify the VLAN ranges that you want the dynamic profile to use. The following example specifies a lower VLAN ID limit of 5000 and any upper VLAN ID limit (a range from 1 through 4094).

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]
user@host# set ranges 5000-any
```

## Configuring Stacked VLAN Ranges for Use with Stacked VLAN Dynamic Profiles

You configure stacked VLAN ranges at the **[edit interfaces]** hierarchy level by specifying the **stacked-vlan-tagging** statement for the interface and defining up to 32 stacked VLAN ranges for use with a stacked VLAN dynamic profile.

To configure a VLAN range:

1. Access the interface over which you want to create dynamic VLANs.

```
user@host# edit interfaces ge-0/0/0
```

2. Specify the **stacked-vlan-tagging** statement to indicate that this interface is for use with stacked VLAN ranges.

```
[edit interfaces ge-0/0/0]
user@host# set stacked-vlan-tagging
```

3. Access the VLAN **[auto-configure]** hierarchy level.

```
[edit interfaces ge-0/0/0]
user@host# edit auto-configure
```

4. Access the **[stacked-vlan-ranges]** hierarchy level.

```
[edit interfaces ge-0/0/0 auto-configure]
user@host# edit stacked-vlan-ranges
```

5. Access the VLAN dynamic profile for which you want to configure VLAN ranges.

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]
user@host# edit dynamic-profile VLAN-PROF1
```

6. Specify the outer and inner stacked VLAN ranges that you want the dynamic profile to use. The following example specifies an outer stacked VLAN ID range from 2000 through 4000 and an inner stacked VLAN ID range of **any** (enabling a range from 1 through 4094 for the inner stacked VLAN ID).

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]
user@host# set ranges 2000-4000,any
```



**NOTE:** You can configure multiple dynamic profile associations (up to 32) with different VLAN range groups on each physical interface.

7. (Optional) Access another VLAN dynamic profile for which you want to configure VLAN ranges.

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]
user@host# edit dynamic-profile VLAN-PROF2
```

8. (Optional) Specify the outer and inner stacked VLAN ranges that you want the dynamic profile to use. The following example specifies an outer stacked VLAN ID range from 4001 through 6000 and an inner stacked VLAN ID range of **any** (enabling a range from 1 through 4094 for the inner stacked VLAN ID).

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]
user@host# set ranges 4001-6000,any
```

## Configuring Dynamic Mixed VLAN Ranges

Dynamic VLAN and dynamic stacked VLAN configuration supports mixed (or flexible) VLAN ranges. You configure mixed VLAN ranges at the **[edit interfaces]** hierarchy level by specifying the **flexible-vlan-tagging** statement for the interface and defining up to 32 VLAN and stacked VLAN range groups for use with different VLAN or stacked VLAN dynamic profiles.



**NOTE:** Junos VLAN IDs for single-tag VLANs are equivalent to the outer tags used for stacked (dual-tag) VLANs. When configuring mixed (flexible) VLANs, any overlap on single-tag VLAN IDs and stacked VLAN outer tag values is supported only for dynamic VLANs on MPC line cards. When configuring mixed (flexible) VLANs on DPCE line cards, overlapping single-tag VLAN IDs and stacked VLAN outer tag values is not supported. This means that a dynamically created single-tagged VLAN interface prevents any overlapping stacked VLAN interfaces from being created or a dynamically created stacked VLAN interface prevents any overlapping single-tagged VLAN interfaces from being created.

To configure both VLAN and stacked VLAN ranges:

1. Access the interface over which you want to create dynamic VLANs.

```
user@host# edit interfaces ge-0/0/0
```

2. Specify the **flexible-vlan-tagging** statement to indicate that this interface is for use with both VLAN and stacked VLAN ranges.

```
[edit interfaces ge-0/0/0]  
user@host# set flexible-vlan-tagging
```

3. Define interface automatic configuration values.

```
[edit interfaces ge-0/0/0]  
user@host# edit auto-configure
```

4. Specify that you want to modify VLAN ranges.

```
[edit interfaces ge-0/0/0 auto-configure]  
user@host# edit vlan-ranges
```

5. Access the VLAN dynamic profile for which you want to configure VLAN ranges.

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]  
user@host# edit dynamic-profile VLAN-PROF1
```

6. Specify the VLAN ranges that you want the dynamic profile to use. The following example specifies a lower VLAN ID limit of 2000 and an upper VLAN ID limit of 3000.

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]  
user@host# set ranges 2000-3000
```



**NOTE:** You can configure multiple dynamic profile associations (up to 32) with different VLAN range groups on each physical interface.

7. Specify that you want to modify stacked VLAN ranges.

```
[edit interfaces ge-0/0/0 auto-configure]
user@host# edit stacked-vlan-ranges
```

8. Access the VLAN dynamic profile for which you want to configure VLAN ranges.

```
[edit interfaces ge-0/0/0 auto-configure stacked-vlan-ranges]
user@host# edit dynamic-profile VLAN-PROF2
```

9. Specify the outer and inner stacked VLAN ranges that you want the dynamic profile to use. The following example specifies an outer stacked VLAN ID range from 3001 through 4000 (to avoid overlapping VLAN IDs with single-tag VLANs) and an inner stacked VLAN ID range of **any** (enabling a range from 1 through 4094 for the inner stacked VLAN ID).

```
[edit interfaces ge-0/0/0 auto-configure stacked-vlan-ranges]
user@host# set ranges 3001-4000,any
```



**NOTE:** You can configure multiple dynamic profile associations (up to 32) with different VLAN range groups on each physical interface.

## Configuring VLAN Dynamic Profile Override

You can override dynamic profile assignment to individual VLANs that are already part of a previously defined VLAN range. This functionality provides a type of exception to an assigned VLAN range. It enables you to configure individual VLAN IDs to use a different dynamic profile from the one assigned to the VLAN range that includes the individual VLAN ID.

To configure dynamic profile override for a specific VLAN:

1. Access the interface on which you want to create a dynamic profile override.

```
user@host# edit interfaces ge-0/0/0
```

2. Access the interface automatic configuration hierarchy.

```
[edit interfaces ge-0/0/0]
user@host# edit auto-configure
```

3. Access either the single-tagged or dual-tagged (stacked) VLAN ranges that you want to modify.

```
[edit interfaces ge-0/0/0 auto-configure]
user@host# edit vlan-ranges
```

or

```
[edit interfaces ge-0/0/0 auto-configure]
user@host# edit stacked-vlan-ranges
```

4. Define the **override** statement along with the VLAN tag that you want to override and the dynamic profile that you want to use when overriding the specified VLAN tag.

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]
user@host# set override tag 20 dynamic-profile NewProfile
```

or

```
[edit interfaces ge-0/0/0 auto-configure stacked-vlan-ranges]  
user@host# set override tag 20 dynamic-profile NewProfile
```

## Configuring Dynamic Authentication for VLAN Interfaces

---

You can use dynamic profiles, in conjunction with RADIUS, to dynamically create logical VLAN interfaces in the default logical system and in a specified routing instance. As DHCP clients in the same VLAN become active, corresponding interfaces are assigned to any specified routing instances. You can also dynamically create an underlying VLAN interface for incoming subscribers, associate interfaces created on this VLAN with the default logical system and a specified routing instance, and define RADIUS authentication values for the dynamically created interfaces.

Before you configure dynamic VLAN authentication, configure DHCP Local Server or DHCP Relay over which you want the dynamic VLAN interfaces to function.

For information about DHCP Local Server or DHCP Relay, see:

- Extended DHCP Local Server Overview on page 98
- Extended DHCP Relay Agent Overview on page 154



**NOTE:** You can also configure dynamically created VLAN interfaces over PPP or PPPoE interfaces. For information about how to configure PPP or PPPoE, see the [Junos OS Network Interfaces Configuration Guide](#).

---

To configure dynamic authentication for dynamically created VLAN interfaces:

1. Configure an access profile that contains the appropriate accounting order, authentication order, and server access values.

For information about how to configure an access profile, RADIUS accounting, RADIUS statistics, and how to define RADIUS server access, see:

- Configuring an Access Profile for Subscriber Management on page 53
  - Specifying the Authentication and Accounting Methods for Subscriber Access on page 21
  - Configuring Per-Subscriber Session Accounting on page 24
  - Configuring Router or Switch Interaction with RADIUS Servers on page 20
2. Configure a dynamic profile that uses the default logical system and creates specific routing instances to contain dynamically created VLAN interfaces.

See “Configuring a VLAN Dynamic Profile That Associates VLAN Interfaces with Separate Routing Instances” on page 414.

3. Define the VLAN physical interface for automatic configuration.

See the following topics:

- Enabling VLAN Tagging
  - Configuring Which VLAN Ethernet Packet Types Dynamic Profiles Can Accept on page 417
  - Configuring VLAN Ranges for Use with Dynamic Profiles on page 419
  - Configuring an Authentication Password for VLAN or Stacked VLAN Ranges on page 418
  - Configuring VLAN Interface Username Information for AAA Authentication on page 425
4. Associate an access profile to the VLAN interface.  
See “Attaching Access Profiles” on page 53.
  5. Associate a dynamic profile to the VLAN interface.  
See “Configuring VLAN Interfaces to Use Dynamic Profiles” on page 416.

**Related  
Documentation**

- Dynamic 802.1Q VLAN Overview on page 407

## Configuring VLAN Interface Username Information for AAA Authentication

You can define interface information that is included in the username that is subsequently passed to the external AAA authentication service (for example, RADIUS) when creating dynamic VLANs or stacked VLANs. The AAA authentication service uses this information to authenticate the VLAN or stacked VLAN physical interface. After the interface is authenticated, the AAA service can send the required routing instance values to the system for use in dynamically creating VLAN or stacked VLAN interfaces.



**NOTE:** The following example configures username information on VLANs. However, you can also configure dynamic authentication on stacked VLANs by configuring the same statements at the `[edit interfaces interface-name auto-configure stacked-vlan-ranges authentication]` hierarchy level.

To configure VLAN interface username information:

1. Access the interface over which you want to configure username information.

```
user@host# edit interfaces ge-0/0/0
```

2. Edit the **auto-configure** stanza.

```
[edit interfaces ge-0/0/0]
user@host# edit auto-configure
```

3. Edit the **vlan-ranges** stanza.

```
[edit interfaces ge-0/0/0 auto-configure]  
user@host# edit vlan-ranges
```

4. Edit the **authentication** stanza.

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]  
user@host# edit authentication
```

5. Edit the **username-include** stanza.

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges]  
user@host# edit username-include
```

6. Specify the username statements that you want the AAA authentication service to use to authenticate the username.

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges authentication username-include]  
user@host# set delimiter
```

**Related Documentation**

- [Configuring Dynamic Authentication for VLAN Interfaces on page 424](#)

---

## Verifying and Managing Dynamic VLAN Configuration

---

**Purpose** View or clear information about dynamic VLANs and stacked VLANs.

- Action**
- To display subscriber dynamic VLAN information:  

```
user@host>show subscribers detail
```
  - To display interface-specific output for dynamic VLANs:  

```
user@host>show interfaces interface-name
```
  - To clear the binding state of dynamic VLAN interfaces:  

```
user@host> clear auto-configuration interfaces
```

**Related Documentation**

- [Junos OS System Basics and Services Command Reference](#)
- [Junos OS Interfaces Command Reference](#)



## Dynamic VLAN Examples

- Example: Configuring a VLAN Dynamic Profile for VLANs with a TPID of 0x8100 on page 427
- Example: Configuring a VLAN Dynamic Profile for VLANs with Any TPID Value and Enabling Demux Interfaces over the VLAN Interface on page 427
- Example: Configuring a Stacked VLAN Dynamic Profile on page 428
- Example: Dynamic VLAN Interface Configuration on page 428
- Example: Dynamic Stacked VLAN Interface Configuration on page 428
- Example: Dynamic Flexible VLAN Interface Configuration on page 429
- Example: Configuring a Flexible VLAN Interface for Use with a Nonstandard Ethertype on page 429

### Example: Configuring a VLAN Dynamic Profile for VLANs with a TPID of 0x8100

---

```
vlan-prof1 {
  interfaces {
    "$junos-interface-ifd-name" {
      unit "$junos-interface-unit" {
        vlan-id "$junos-vlan-id"; #Note the statement and variable use.
        family inet {
          unnumbered-address lo0.0 preferred-source-address 10.20.0.2;
        }
      }
    }
  }
}
```

### Example: Configuring a VLAN Dynamic Profile for VLANs with Any TPID Value and Enabling Demux Interfaces over the VLAN Interface

---

```
vlan-prof-any-tpid {
  interfaces {
    $junos-interface-ifd-name {
      unit $junos-interface-unit {
        demux-source inet; #Enables demux interface use over the VLAN interface.
        vlan-tags outer $junos-vlan-id; #Statement/variable combination enables the
          recognition of any VLAN interface TPID value.
        family inet {
```

```
        unnumbered-address lo0.0 preferred-source-address 10.20.0.2;
    }
}
}
}
```

---

### Example: Configuring a Stacked VLAN Dynamic Profile

---

```
svlan-prof1 {
  interfaces {
    $junos-interface-ifd-name {
      unit $junos-interface-unit {
        vlan-tags outer $junos-stacked-vlan-id inner $junos-vlan-id;
        family inet {
          unnumbered-address lo0.0 preferred-source-address 100.20.0.2;
        }
      }
    }
  }
}
```

---

### Example: Dynamic VLAN Interface Configuration

---

```
interfaces {
  ge-0/0/0 {
    vlan-tagging;
    auto-configure {
      vlan-ranges {
        dynamic-profile vlan-prof1 {
          accept inet;
          ranges {
            any;
          }
        }
      }
    }
  }
}
```

---

### Example: Dynamic Stacked VLAN Interface Configuration

---

```
interfaces {
  ge-0/0/0 {
    stacked-vlan-tagging;
    auto-configure {
      stacked-vlan-ranges {
        dynamic-profile svlan-prof {
          accept inet;
          ranges {
            1-1, any;
          }
        }
      }
    }
  }
}
```

```

    }
  }

```

### Example: Dynamic Flexible VLAN Interface Configuration

```

interfaces {
  ge-0/0/0 {
    flexible-vlan-tagging;
    auto-configure {
      vlan-ranges {
        dynamic-profile vlan-prof1 {
          accept inet;
          ranges {
            any;
          }
        }
      }
    }
    stacked-vlan-ranges {
      dynamic-profile svlan-prof1 {
        accept inet;
        ranges {
          1-1, any;
        }
      }
    }
  }
}

```

### Example: Configuring a Flexible VLAN Interface for Use with a Nonstandard Ethertype

This example specifies an ethertype of 0x9100 instead of the standard 0x8100.

```

interfaces {
  ge-0/0/0 {
    flexible-vlan-tagging;
    gigether-options {
      ethernet-switch-profile {
        tag-protocol-id 0x9100;
      }
    }
    auto-configure {
      vlan-ranges {
        dynamic-profile vlan-prof {
          accept inet;
          ranges {
            any;
          }
        }
      }
    }
    stacked-vlan-ranges {
      dynamic-profile svlan-prof {
        accept inet;
        ranges {
          1-1, any;
        }
      }
    }
  }
}

```

```
}  
}  
}  
}  
}  
}
```

## PART 11

# Subscriber Interfaces

- [Subscriber Interface Overview on page 433](#)
- [Configuring Subscriber Interfaces for Dynamic Profiles on page 439](#)
- [Subscriber Interface Examples on page 451](#)
- [Subscriber Interfaces over Aggregated Ethernet Overview on page 471](#)
- [Configuring Subscriber Interfaces over Aggregated Ethernet on page 479](#)
- [Subscriber Interfaces over Aggregated Ethernet Examples on page 489](#)
- [Dynamic PPPoE Subscriber Interfaces Overview on page 527](#)
- [Configuring Dynamic PPPoE Subscriber Interfaces on page 535](#)
- [Dynamic PPPoE Subscriber Interfaces Examples on page 547](#)



# Subscriber Interface Overview

- Subscriber Interface Overview on page 433
- Static Subscriber Interfaces and VLAN Overview on page 434
- Subscriber Interfaces and Demultiplexing Overview on page 435
- MAC Address Validation for Subscriber Interfaces Overview on page 437

## 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 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]
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;
}

```

## Dynamically Identifying Subscribers

You can configure 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 Documentation**
- Static Subscriber Interfaces and VLAN Overview on page 434
  - Subscriber Interfaces and Demultiplexing Overview on page 435

## Static Subscriber Interfaces and VLAN Overview

This topic describes the topology for configuring subscriber interfaces over static VLAN interfaces in the current release.

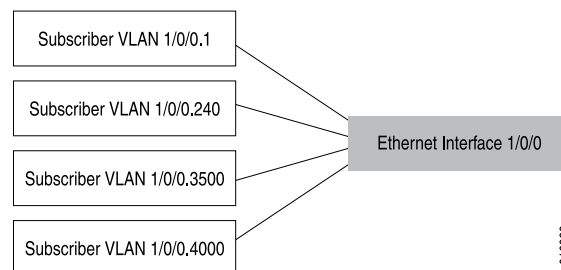
In a dynamic profile, you can configure VLAN subscriber interfaces over the following statically created logical interface types:

- GE—Gigabit Ethernet
- XE—10-Gigabit Ethernet
- AE—Aggregated Ethernet

We recommend that you configure each subscriber on a statically created VLAN.

Figure 9 on page 434 shows an example of subscriber interfaces on an individual VLAN.

**Figure 9: 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 Documentation**
- Configuring a Subscriber Interface with a Static VLAN Interface on page 440
  - For more information about demux interfaces, see Subscriber Interfaces and Demultiplexing Overview on page 435

## Subscriber Interfaces and Demultiplexing Overview

You can create logical subscriber interfaces using static or dynamic demultiplexing interfaces. In addition, you can use either IP demultiplexing interfaces or VLAN demultiplexing interfaces when creating logical subscriber interfaces.

Demultiplexing (demux) interfaces are logical interfaces that share a common, underlying logical interface (in the case of IP demux) or underlying physical interface (in the case of VLAN demux). You can use these interfaces to identify specific subscribers or to separate individual circuits by IP address (IP demux) or VLAN ID (VLAN demux).

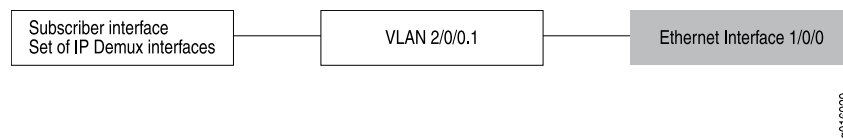
The subscriber interfaces can provide different levels of services for individual subscribers in an access network. For example, you can apply CoS parameters for each subscriber.

### Interface Sets of Static Demux Interfaces

You can group static demux interfaces 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 10 on page 435 shows a subscriber interface configured using a set of IP demux interfaces with an underlying VLAN interface.

**Figure 10: IP Demux Subscriber Interface**



### Dynamic Demultiplexing Interfaces

You can configure 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 (for IP demux interfaces) or VLAN ID (for VLAN demux interfaces).

To configure an IP demux interface in the dynamic profile, you specify variables for the unit number, the name of the underlying interface, and the IP address. To configure a VLAN demux interface in the dynamic profile, you specify variables for the unit number, the name of the underlying interface, and the VLAN ID. These variables are replaced with the values that are supplied by DHCP when the subscriber logs in.

## Guidelines for Configuring Demux Interfaces for Subscriber Access

When you configure static or dynamic demux interfaces for subscriber access, consider the following guidelines:

- You can only configure interface sets of static demux interfaces and dynamic demux interfaces on MX Series 3D Universal Edge Routers. Hierarchical and per-unit scheduling is supported for dynamically created demux interfaces on the EQ DPC.
- You can configure IPv4 and IPv6 addressing for static and dynamic demux interfaces.
- You can configure only one **demux0** interface per chassis.
- For IP demux interfaces, you can define logical demux interfaces on top of the **demux0** interface (for example, **demux0.1**, **demux0.2**, and so on).
- Demux interfaces currently support only Gigabit Ethernet, Fast Ethernet, 10-Gigabit Ethernet, and aggregated Ethernet underlying interfaces.
- You must associate IP demux interfaces with an underlying logical interface.
- You must associate VLAN demux interfaces with an underlying device (physical interface).
- 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 Documentation

- [Configuring Static Subscriber Interfaces Using IP Demux Interfaces on page 440](#)
- [Configuring Static Subscriber Interfaces Using VLAN Demux Interfaces on page 441](#)
- [Configuring a Subscriber Interface Using a Set of Static IP Demux Interfaces on page 443](#)
- [Configuring a Subscriber Interface Using a Set of Static VLAN Demux Interfaces on page 444](#)
- [Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 445](#)
- [Configuring Dynamic Subscriber Interfaces Using VLAN Demux Interfaces in Dynamic Profiles on page 446](#)
- [CoS and Static IP Demux Interface Set Overview on page 703](#)
- For more information about static demux interfaces and other configuration guidelines, see the [Junos OS 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 demux interfaces on MX Series 3D Universal Edge 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  
Documentation**

- [Configuring MAC Address Validation for Subscriber Interfaces on page 447](#)

# Configuring Subscriber Interfaces for Dynamic Profiles

- [Configuring Static Subscriber Interfaces in Dynamic Profiles on page 439](#)
- [Configuring a Subscriber Interface Using a Set of Static IP Demux Interfaces on page 443](#)
- [Configuring a Subscriber Interface Using a Set of Static VLAN Demux Interfaces on page 444](#)
- [Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 445](#)
- [Configuring Dynamic Subscriber Interfaces Using VLAN Demux Interfaces in Dynamic Profiles on page 446](#)
- [Configuring MAC Address Validation for Subscriber Interfaces on page 447](#)

## 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 440](#)
- [Configuring Static Subscriber Interfaces Using IP Demux Interfaces on page 440](#)
- [Configuring Static Subscriber Interfaces Using VLAN Demux Interfaces on page 441](#)
- [Associating Dynamic Profiles with Statically Created Interfaces on page 441](#)

## 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;
  }
}
```

3. Associate the static subscriber interface in a dynamic profile.

See “Associating Dynamic Profiles with Statically Created Interfaces” on page 441.

## Configuring Static Subscriber Interfaces Using IP Demux Interfaces

You can configure a subscriber interface using a statically created IP demux interface. This interface can be referenced in a dynamic profile.

To configure a static IP demux subscriber interface:

1. Configure the IP demux interface on a physical device represented by a logical unit number. The logical interface resides on a physical device.

See [Configuring an IP Demultiplexing Interface](#).

2. Configure the underlying interface on which the IP demux interface is running.

See [Configuring an IP Demux Underlying Interface](#).

3. Specify the underlying interface on which the IP demux interface is running.

See [Specifying the Demux Underlying Interface](#).

4. Specify how ingress IPv4 traffic is to be demultiplexed based on packet destination or source addresses.

See Configuring IP Demux Prefixes.

5. Associate the static subscriber interface in a dynamic profile.

See “Associating Dynamic Profiles with Statically Created Interfaces” on page 441.



**NOTE:** VLAN demux interfaces currently support the Internet Protocol version 4 (IPv4) suite (`family inet`) and the Internet Protocol version 6 (IPv6) suite (`family inet6`).

## Configuring Static Subscriber Interfaces Using VLAN Demux Interfaces

You can configure a subscriber interface using a statically created VLAN demux interface. This interface can be referenced in a dynamic profile.

To configure a static VLAN demux subscriber interface:

1. Configure the VLAN demux interface.  
See Configuring a VLAN Demultiplexing Interface.
2. Configure the underlying interface on which the VLAN demux interface is running.  
See Configuring a VLAN Demux Underlying Interface
3. Specify the underlying interface on which the VLAN demux interface is running.  
See Specifying the Demux Underlying Interface.
4. Specify how ingress IP traffic is to be demultiplexed based on the VLAN ID.  
See Associating VLAN IDs to VLAN Demux Interfaces.
5. Associate the static subscriber interface in a dynamic profile.  
See “Associating Dynamic Profiles with Statically Created Interfaces” on page 441.



**NOTE:** VLAN demux interfaces currently support the Internet Protocol version 4 (IPv4) suite (`family inet`) and the Internet Protocol version 6 (IPv6) suite (`family inet6`).

VLAN demux subscriber interfaces over aggregated Ethernet physical interfaces are supported only for MX Series routers that have only Trio MPCs installed. If the router has other cards in addition to Trio MPCs, the CLI accepts the configuration but errors are reported when the subscriber interfaces are brought up.

## 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 variable

and logical unit name variable with the actual interface name and logical unit number of the interface that received the DHCP request.



**NOTE:** Configuration of the interface name variable and logical interface name variable at the [edit dynamic-profiles *profile-name* interfaces] hierarchy level is required for a dynamic profile to function.

To configure the interface for a dynamic profile, specify the interface name variable and include the **unit** statement and associated logical interface name variable:

1. Access the profile.

```
[edit]
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 logical interface name variable with the **unit** statement.

When referencing an existing interface, specify the **\$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
```

When creating dynamic interfaces, specify the **\$junos-interface-unit** variable used by the router to generate a unit value for the interface:

```
[edit dynamic-profiles basic-profile]
user@host# set unit $junos-interface-unit
```

**Related  
Documentation**

- Static Subscriber Interfaces and VLAN Overview on page 434
- For information about configuring logical interfaces and static VLAN interfaces, see the [Junos OS 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 Documentation**
- [Configuring CoS on a Set of Static IP Demux Interfaces on page 709](#)
  - [Subscriber Interfaces and Demultiplexing Overview on page 435](#)

- For information about the **[edit interfaces]** hierarchy and the **interface-set** statement, see the *Junos OS Network Interfaces Configuration Guide*

## Configuring a Subscriber Interface Using a Set of Static VLAN Demux Interfaces

---

You can create logical subscriber interfaces from VLAN demux interfaces. VLAN demultiplexing (demux) interfaces are logical interfaces that share a common, underlying physical interface. VLAN 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 VLAN 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 {
    vlan-id 10;
    demux-options {
      underlying-interface ge-2/0/1;
    }
    family inet {
      address 1.1.1.1/24;
    }
  }
  unit 1 {
    vlan-id 20;
    demux-options {
      underlying-interface ge-2/0/1;
    }
    family inet {
      address 1.1.2.1/24;
    }
  }
}
```

### Related Documentation

- Configuring CoS on a Set of Static IP Demux Interfaces on page 709
- Subscriber Interfaces and Demultiplexing Overview on page 435

- For information about the **[edit interfaces]** hierarchy and the **interface-set** statement, see the *Junos OS 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 391.

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 interfaces demux0]
user@host# edit unit $junos-interface-unit
```

- b. Configure the variable for the underlying interface of the demux interfaces and specify the **\$junos-underlying-interface** variable.

The variable is dynamically replaced with the underlying interface that DHCP supplies when the subscriber logs in.

```
[edit dynamic-profiles business-profile interfaces demux0 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.

For IPv4:

```
[edit dynamic-profiles business-profile interfaces demux0 unit
 "$junos-interface-unit"]
user@host# edit family inet
```

For IPv6:

```
[edit dynamic-profiles business-profile interfaces demux0 unit  
"$junos-interface-unit"]  
user@host# edit family inet6
```

- 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 lo0.0
```

- 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. For IPv4, use **\$junos-subscriber-ip-address**; for IPv6, use **\$junos-subscriber-ipv6-address**

```
[edit dynamic-profiles business-profile interfaces demux0 unit "$junos-interface-unit"]  
user@host# set demux-source $junos-subscriber-ip-address
```

#### Related Documentation

- Subscriber Interfaces and Demultiplexing Overview on page 435
- Configuring MAC Address Validation for Dynamic Subscriber Interfaces on page 448
- Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125
- Example: Configuring Dynamic Subscriber Interfaces on IP Demux Interfaces on page 453
- Example: Configuring Subscribers on Dynamically Created VLAN Demux Interfaces

---

## Configuring Dynamic Subscriber Interfaces Using VLAN Demux Interfaces in Dynamic Profiles

---

You can configure dynamic subscriber interfaces using VLAN 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 391.

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 interfaces demux0]
user@host# edit unit $junos-interface-unit
```

- b. Configure the variable for the underlying interface of the demux interfaces by specifying the **\$junos-interface-ifd-name** variable.

The variable is dynamically replaced with the underlying device name that DHCP supplies when the subscriber logs in.

```
[edit dynamic-profiles business-profile interfaces demux0 unit
"$junos-interface-unit"]
user@host# set demux-options underlying-interface $junos-interface-ifd-name
```

- c. Configure the variable for the VLAN ID.

```
[edit dynamic-profiles business-profile interfaces demux0 unit
"$junos-interface-unit"]
user@host# set vlan-id $junos-vlan-id
```

3. Configure the family for the demux interfaces.

- a. Specify that you want to configure the family.

For IPv4:

```
[edit dynamic-profiles business-profile interfaces demux0 unit
"$junos-interface-unit"]
user@host# edit family inet
```

For IPv6:

```
[edit dynamic-profiles business-profile interfaces demux0 unit
"$junos-interface-unit"]
user@host# edit family inet6
```

- 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 lo0.0
```

#### Related Documentation

- Subscriber Interfaces and Demultiplexing Overview on page 435
- Configuring MAC Address Validation for Dynamic Subscriber Interfaces on page 448
- Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125
- Example: Configuring Subscribers on Dynamically Created VLAN Demux Interfaces

## 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 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 448
- Configuring MAC Address Validation for Dynamic Subscriber Interfaces on page 448

## 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 391.

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 441.

## 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 IP 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 391.

- Configure the dynamic IP demux interface.

See “Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles” on page 445.

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  
Documentation**

- MAC Address Validation for Subscriber Interfaces Overview on page 437
- Example: Configuring Dynamic Subscriber Interfaces on IP Demux Interfaces on page 453





## Subscriber Interface Examples

- Example: Configuring a Static Subscriber Interface on a Gigabit Ethernet VLAN Interface (Multiple Logical Units) on page 451
- Example: Configuring a Static Subscriber Interface on a Gigabit Ethernet VLAN Interface on page 452
- Example: Configuring a Static Subscriber Interface on a Gigabit Ethernet VLAN Interface (No Autonegotiation) on page 452
- Example: Configuring a Static Subscriber Interface with a Loopback on page 452
- Example: Configuring Dynamic Subscriber Interfaces on IP Demux Interfaces on page 453
- Example: Configuring IPv6 Addressing for a Dynamic IP Demux Interface over Static VLANs on page 455
- Example: Configuring IPv6 Addressing for a Dynamic IP Demux Interface over Dynamic VLANs on page 456
- Example: Configuring a Dynamic IP Demux Interface with Dual Stacking on page 459
- Example: Configuring IPv4 Static VLAN Demux Interfaces over a Gigabit Ethernet Underlying Interface with DHCP Local Server on page 462
- Example: Configuring IPv4 Dynamic VLAN Demux Interfaces over a Gigabit Ethernet Underlying Interface with DHCP Local Server on page 464
- Example: Configuring CoS on Static LSQ MLPPP Bundle Interfaces on page 467

### 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 Documentation** • [Configuring Static Subscriber Interfaces in Dynamic Profiles on page 439](#)

### 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 Documentation** • [Configuring Static Subscriber Interfaces in Dynamic Profiles on page 439](#)

### 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 Documentation** • [Configuring Static Subscriber Interfaces in Dynamic Profiles on page 439](#)

### Example: Configuring a Static Subscriber Interface with a Loopback

```
lo0 {
    unit 0 {
        family inet {
            address 192.1.1.1/32;
        }
    }
}
```

**Related Documentation** • [Configuring Static Subscriber Interfaces in Dynamic Profiles on page 439](#)

## 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 IP 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;  
      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  
Documentation**

- [Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 445](#)
- [Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125](#)

## Example: Configuring IPv6 Addressing for a Dynamic IP Demux Interface over Static VLANs

In this example, the network administrator configures IPv6 addressing for a dynamic IP demux interface over a group of static VLANs.

```
[edit]
dynamic-profiles {
  dhcp-demux-profile {
    interfaces {
      demux0 {
        unit "$junos-interface-unit" {
          demux-options {
            underlying-interface "$junos-underlying-interface";
          }
          family inet6 {
            address 2001::1/64;
            demux-source {
              $junos-subscriber-ipv6-address;
            }
          }
        }
      }
    }
  }
}
system {
  services {
    dhcp-local-server {
      dhcpv6 {
        dynamic-profile dhcp-demux-prof;
        group vlan {
          interface ge-1/0/0.100;
        }
      }
    }
  }
}
interfaces {
  ge-1/0/0 {
    vlan-tagging;
    unit 100 {
      demux-source inet6;
      vlan-id 100;
      family inet6 {
        address 2001::1/64;
      }
    }
  }
}
access {
  address-assignment {
    pool dhcp {
      family inet6 {
```

```
        prefix 2001:0000:0000:0000::/64;
        range limits prefix-length 74;
    }
}
}
```

**Related Documentation**

- [Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 445](#)

## Example: Configuring IPv6 Addressing for a Dynamic IP Demux Interface over Dynamic VLANs

---

In this example, the network administrator configures IPv6 addressing for a dynamic IP demux interface over a group of dynamic VLANs.

```
dynamic-profiles {
  vlan-profile {
    interfaces {
      "$junos-interface-ifd-name" {
        unit "$junos-interface-unit" {
          vlan-id "$junos-vlan-id";
          demux-source inet6;
          family inet6 {
            unnumbered-address lo0.0 preferred-source-address ::100.20.32.2;
          }
        }
      }
    }
  }
  svlan-profile {
    interfaces {
      $junos-interface-ifd-name {
        unit $junos-interface-unit {
          demux-source inet6;
          vlan-tags outer $junos-stacked-vlan-id inner $junos-vlan-id;
          family inet6 {
            unnumbered-address lo0.0 preferred-source-address ::100.20.32.2;
          }
        }
      }
    }
  }
  dhcp-demux-prof {
    interfaces {
      demux0 {
        unit "$junos-interface-unit" {
          demux-options {
            underlying-interface "$junos-underlying-interface";
          }
          family inet6 {
            demux-source {
              $junos-subscriber-ipv6-address;
            }
          }
        }
      }
    }
  }
}
```

```

        unnumbered-address lo0.0 preferred-source-address 2001:db8:ffff:1::1;
    }
}
}
}
all-profile {
    interfaces {
        $junos-interface-ifd-name {
            unit $junos-underlying-interface-unit {
            }
        }
    }
}
}
}
services {
    dhcp-local-server {
        traceoptions {
            file dhcp size 1g;
            flag all;
        }
        dhcpv6 {
            authentication {
                password delpref;
                username-include {
                    user-prefix localpool;
                }
            }
        }
        group one {
            authentication {
                password delpref;
                username-include {
                    user-prefix localpool;
                }
            }
        }
        dynamic-profile dhcp-demux-prof use-primary all-profile;
        interface ge-0/0/3.0;
    }
}
group v6 {
    authentication {
        password delpref;
        username-include {
            user-prefix localpool;
        }
    }
    dynamic-profile dynamic-profile dhcp-demux-prof use-primary all-profile;
    interface ge-1/0/0.0;
}
}
}
}
interfaces {
    ge-1/0/0 {
        vlan-tagging;
    }
}
}

```

```
auto-configure {
  vlan-ranges {
    dynamic-profile vlan-profile {
      accept inet6;
      ranges {
        any;
      }
    }
  }
}
ge-1/2/0 {
  flexible-vlan-tagging;
  auto-configure {
    vlan-ranges {
      dynamic-profile vlan-profile {
        accept inet6;
        ranges {
          any;
        }
      }
    }
    stacked-vlan-ranges {
      dynamic-profile svlan-profile {
        accept inet6;
        ranges {
          any,any;
        }
      }
    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 100.20.32.2/32;
    }
    family inet6 {
      address ::100.20.32.2/128;
    }
  }
}
access {
  address-assignment {
    pool v6 {
      family inet6 {
        network 100.20.0.0/16;
        range limited {
          low 100.20.0.10;
          high 100.20.128.250;
        }
      }
      dhcp-attributes {
        maximum-lease-time 84600;
      }
    }
  }
}
```



```

    }
  }
}

```

**Related  
Documentation**

- [Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 445](#)

## Example: Configuring a Dynamic IP Demux Interface with Dual Stacking

In this example, the network administrator configures IPv4 and IPv6 addressing for a dynamic IP demux interface with a group of underlying static VLANs.

```

[edit]
dynamic-profiles {
  dhcp-demux-prof {
    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 3.1.1.1;
          }
          family inet6 {
            demux-source {
              $junos-subscriber-ipv6-address;
            }
            unnumbered-address lo0.0 preferred-source-address 2001:db8:ffff:1::1;
          }
        }
      }
    }
  }
}
all-profile {
  interfaces {
    "$junos-interface-ifd-name" {
      unit "$junos-underlying-interface-unit";
    }
  }
}
services {
  dhcp-local-server {
    traceoptions {
      file dhcp size 1g;
      flag all;
    }
  }
  dhcpv6 {
    authentication {
      password delpref;
    }
  }
}

```

```
        username-include {
            user-prefix localpool;
        }
    }
    group groupv6 {
        authentication {
            password delpref;
            username-include {
                user-prefix localpool;
            }
        }
        dynamic-profile dhcp-demux-prof use-primary all-profile;
        interface ge-0/0/3.0;
    }
}
group groupv4 {
    authentication {
        password delprefv4;
        username-include {
            user-prefix localpoolv4;
        }
    }
    dynamic-profile dhcp-demux-prof;
    interface ge-0/0/2.0;
}
}
processes {
    general-authentication-service {
        traceoptions {
            file auth;
            flag all;
        }
    }
}
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            proxy-arp;
            family inet6 {
                address 4ffe::1:1/48;
            }
        }
    }
    ge-0/0/1 {
        vlan-tagging;
        gigether-options {
            no-auto-negotiation;
        }
        unit 10 {
            vlan-id 10;
            family inet {
                address 100.10.0.2/24;
            }
        }
    }
    ge-0/0/2 {
```

```

    unit 0 {
        demux-source inet;
        proxy-arp;
        family inet {
            unnumbered-address lo0.0 preferred-source-address 3.1.1.1;
        }
    }
}
ge-0/0/3 {
    unit 0 {
        demux-source inet6;
        proxy-arp;
        family inet6 {
            unnumbered-address lo0.0 preferred-source-address 2001:db8:ffff:1::1;
        }
    }
}
lo0 {
    unit 0 {
        family inet {
            address 3.1.1.1/32;
        }
        family inet6 {
            address 2001:db8:ffff:1::1/128;
        }
    }
}
}
access {
    radius-server {
        100.10.0.1 {
            port 1812;
            secret "$9$xs5-dsgoGDjqgo"; ## SECRET-DATA
        }
    }
}
profile wash-test {
    accounting-order radius;
    authentication-order radius;
    radius {
        authentication-server 100.10.0.1;
        accounting-server 100.10.0.1;
    }
    accounting {
        order radius;
        accounting-stop-on-failure;
        accounting-stop-on-access-deny;
        update-interval 10;
        statistics time;
    }
}
address-assignment {
    pool v4ville {
        family inet {
            network 3.1.1.0/24;
            range testv4 {
                low 3.1.1.3;
            }
        }
    }
}

```

```

        high 3.1.1.50;
    }
}
}
pool v6ville {
    family inet6 {
        prefix 2001:db8:ffff::/48;
        range test {
            low 2001:db8:ffff:1::2/128;
            high 2001:db8:ffff:1::ffff/128;
        }
    }
}
}
}
}
[edit]
dynamic-profiles {
    dhcp-demux-profile {
        interfaces {
            demux0 {
                unit "$junos-interface-unit" {
                    demux-options {
                        underlying-interface "$junos-underlying-interface";
                    }
                    family inet {
                        demux-source {
                            $junos-subscriber-ip-address;
                        }
                        unnumbered-address ge-0/0/0.0 preferred-source-address 1.1.1.2;
                    }
                    family inet6 {
                        demux-source {
                            $junos-subscriber-ipv6-address;
                        }
                        unnumbered-address ge-0/0/3.0 preferred-source-address ::22.22.22.2;
                    }
                }
            }
        }
    }
}
}

```

- Related Documentation**
- [Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 445](#)

## Example: Configuring IPv4 Static VLAN Demux Interfaces over a Gigabit Ethernet Underlying Interface with DHCP Local Server

This example shows how to configure a static IPv4 VLAN demux interface with gigabit Ethernet as the underlying interface. DHCP Local Server configuration enables the association of subscribers to the VLAN demux interface by listing the gigabit Ethernet interface in the DHCP local server configuration.

To configure dynamic subscribers on VLAN demux interfaces:

1. Enable VLAN tagging on the underlying interface that you plan to use for the VLAN demux interfaces.

```
interfaces {
  ge-5/0/0 {
    vlan-tagging;
  }
}
```

2. Define the loopback interface.

```
interfaces {
  lo0 {
    unit 0 {
      family inet {
        address 192.16.1.1/32;
      }
    }
  }
}
```

3. Define the demux interface.

```
interfaces {
  demux0 {
    unit 102 {
      proxy-arp;
      vlan-id 103;
      demux-options {
        underlying-interface ge-5/0/0;
      }
      family inet {
        unnumbered-address lo0.0 preferred-source-address 173.16.1.1;
      }
    }
  }
}
```

4. Configure a dynamic profile for subscriber access.

```
dynamic-profiles {
  user-profile {
    interfaces {
      "$junos-interface-ifd-name" {
        unit "$junos-underlying-interface-unit" {
          family inet;
        }
      }
    }
  }
}
```

5. Configure the access method used to dynamically create the subscriber interfaces.

The following stanza specifies the gigabit Ethernet interface (**ge-5/0/0.0**) for use with the dynamically created subscriber interfaces.

```
system {
  services {
    dhcp-local-server {
      group myDhcpGroup {
        authentication {
          password test;
          username-include {
            user-prefix igmp-user1;
          }
        }
        dynamic-profile user-profile;
        interface ge-5/0/0.0;
      }
    }
  }
}
```

Instead of using the gigabit Ethernet interface, you can alternatively specify the specific demux interface (**demux0.102**) as the device to use with the subscriber interfaces as follows:

```
system {
  services {
    dhcp-local-server {
      group myDhcpGroup {
        authentication {
          password test;
          username-include {
            user-prefix igmp-user1;
          }
        }
        dynamic-profile user-profile;
        interface demux0.102;
      }
    }
  }
}
```

- Related Documentation**
- [Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 445](#)
  - [Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125](#)

---

## Example: Configuring IPv4 Dynamic VLAN Demux Interfaces over a Gigabit Ethernet Underlying Interface with DHCP Local Server

---

This example shows how to configure the dynamic creation of IPv4 VLAN demux interfaces with gigabit Ethernet as the underlying interface. DHCP Local Server configuration enables the association of subscribers to the VLAN demux interface by listing the aggregated Ethernet interface in the DHCP local server configuration.

To configure dynamic subscribers on dynamic VLAN demux interfaces:

1. Enable VLAN tagging and VLAN auto-configuration on the underlying gigabit Ethernet interface that you plan to use for dynamically created VLAN demux interfaces.

```

interfaces {
  ge-5/0/0 {
    hierarchical-scheduler;
    vlan-tagging;
    auto-configure {
      vlan-ranges {
        dynamic-profile auto-vlanDemux-profile {
          accept inet;
          ranges {
            103-103;
          }
        }
      }
    }
  }
}

```

2. Define the loopback interface.

```

interfaces {
  lo0 {
    unit 0 {
      family inet {
        address 192.16.1.1/32;
      }
    }
  }
}

```

3. Configure a dynamic profile for subscriber access.

```

dynamic-profiles {
  user-profile {
    interfaces {
      "$junos-interface-ifd-name" {
        unit "$junos-underlying-interface-unit" {
          family inet;
        }
      }
    }
  }
}

```

4. Configure a dynamic profile for VLAN demux interface creation.

```

dynamic-profiles {
  auto-vlanDemux-profile {
    interfaces {
      demux0 {
        unit "$junos-interface-unit" {
          vlan-id "$junos-vlan-id";
          demux-options {
            underlying-interface "$junos-interface-ifd-name";
          }
        }
      }
    }
  }
}

```

```

    }
    family inet {
        filter {
            input rate_limit;
            output rate_limit;
        }
        unnumbered-address lo0.0 preferred-source-address 192.16.1.1;
    }
}
}
}
}
}
}
}

```

5. Configure the access method used to dynamically create the subscriber interfaces. The following stanza specifies the gigabit Ethernet interface (**ge-5/0/0.0**) for use with the dynamically created subscriber interfaces.

```

system {
  services {
    dhcp-local-server {
      group myDhcpGroup {
        authentication {
          password test;
          username-include {
            user-prefix igmp-user1;
          }
        }
        dynamic-profile user-profile;
        interface ge-5/0/0.0;
      }
    }
  }
}

```

Instead of using the gigabit Ethernet interface, you can alternatively specify **demux0** as the device to use with the subscriber interfaces as follows:



**NOTE:** Because the demux interfaces and unit numbers are created dynamically, the unit number is not specified for the demux0 interface.

```

system {
  services {
    dhcp-local-server {
      group myDhcpGroup {
        authentication {
          password test;
          username-include {
            user-prefix igmp-user1;
          }
        }
        dynamic-profile user-profile;
        interface demux0;
      }
    }
  }
}

```



```

    }
  }
}

```

**Related Documentation**

- [Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 445](#)
- [Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125](#)

## Example: Configuring CoS on Static LSQ MLPPP Bundle Interfaces

This example shows how to configure dynamic subscriber services on MLPPP bundle interfaces. The MLPPP bundles must be configured on link services intelligent queuing (LSQ) (LSQ) interfaces. The MLPPP interfaces must be statically configured.

To configure dynamic subscriber services on static LSQ MLPPP bundle interfaces:

1. Configure class of service features for the LSQ interfaces.

```

[edit]
class-of-service
  classifiers {
    inet-precedence inet_classifier {
      forwarding-class best-effort {
        loss-priority low code-points 000;
      }
      forwarding-class expedited-forwarding {
        loss-priority low code-points 011;
      }
      forwarding-class assured-forwarding {
        loss-priority low code-points 100;
      }
    }
  }
  fragmentation-maps {
    sample-fragmap {
      forwarding-class {
        best-effort {
          fragment-threshold 1000;
          multilink-class 1;
        }
        assured-forwarding {
          fragment-threshold 1000;
          multilink-class 2;
        }
        expedited-forwarding {
          multilink-class 3;
        }
      }
    }
  }
  forwarding-classes {
    queue 0 best-effort;
    queue 1 expedited-forwarding;
  }
}

```

```
    queue 2 assured-forwarding;
  }
# traffic classifiers are statically defined
network traffic interface{
  classifiers {
    inet-precedence inet_classifier;
  }
}
scheduler-maps {
  allthree {
    forwarding-class best-effort scheduler be-scheduler;
    forwarding-class expedited-forwarding scheduler hiprior-sched;
    forwarding-class assured-forwarding scheduler vpn-sched;
  }
}
schedulers {
  be-scheduler {
    transmit-rate percent 30;
    priority low;
  }
  hiprior-scheduler {
    transmit-rate percent 40;
    priority strict-high;
  }
  vpn-sched {
    transmit-rate percent 30;
    medium-high;
  }
}
}
```

2. Configure the MLPPP bundle interfaces and the LSQ interfaces.

```
[edit interfaces]
t1-3/1/0:1:1 {
  keepalives interval 600;
  encapsulation ppp;
  unit 0 {
    ppp-options {
      lcp-restart-timer 5000;
    }
    family mlppp {
      bundle lsq-3/3/0.0;
    }
  }
}
t1-3/1/0:1:2 {
  keepalives interval 600;
  encapsulation ppp;
  unit 0 {
    ppp-options {
      lcp-restart-timer 5000;
    }
    family mlppp {
      bundle lsq-3/3/0.0;
    }
  }
}
```

```

    }
  }
  lsq-3/3/0 {
    unit 0 {
      encapsulation multilink-ppp;
      multilink-max-classes 4;
      ppp-options {
        ncp-restart-timer 10000;
        dynamic-profile mlppp-profile;
      }
      family inet {
        address 192.168.1.1/32 {
          destination 192.168.25.45;
        }
      }
    }
  }
}

```

3. Configure the dynamic profile that is applied to the MLPPP bundle interfaces.

```

[edit]
dynamic-profiles {
  mlppp-profile {
    interfaces {
      "$junos-interface-ifd-name" {
        unit junos-underlying-interface-unit {
          family inet {
            filter {
              input "$junos-input-filter";
              output "$junos-output-filter";
            }
          }
        }
      }
    }
  }
  class-of-service {
    interfaces {
      "$junos-interface-ifd-name" {
        unit junos-underlying-interface-unit {
          output-traffic-control-profile tcp1;
          fragmentation-map sample-fragmap;
        }
      }
    }
  }
  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 {
    data_smap {
      forwarding-class be scheduler data_sch;
    }
  }
}

```

```
    }  
    schedulers {  
      be_sch {  
        ...  
      }  
    }  
  }  
}
```

**Related  
Documentation**

- For hardware requirements, see *Hardware Requirements for PPP Subscriber Services on Non-Ethernet Interfaces* on page 226
- For information about MLPPP and LSQ interfaces, see *Link Services IQ Interfaces Configuration* in the [Junos OS Services Interfaces Configuration Guide](#).

## CHAPTER 41

# Subscriber Interfaces over Aggregated Ethernet Overview

- Static and Dynamic VLAN Subscriber Interfaces over Aggregated Ethernet Overview on page 471
- Static or Dynamic Demux Subscriber Interfaces over Aggregated Ethernet Overview on page 472
- Distribution of Demux Subscribers in an Aggregated Ethernet Interface on page 474

### Static and Dynamic VLAN Subscriber Interfaces over Aggregated Ethernet Overview

You can configure 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) or Trio MPC/MIC interfaces in MX Series 3D Universal Edge Routers.

A static or dynamic 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 or dynamic VLAN subscriber interface over aggregated Ethernet, make sure you understand the following concepts.

- Guidelines for Configuring an Aggregated Ethernet Logical Interface to Support a Static or Dynamic VLAN Subscriber Interface on page 471

### **Guidelines for Configuring an Aggregated Ethernet Logical Interface to Support a Static or Dynamic VLAN Subscriber Interface**

The following guidelines for configuring an aggregated Ethernet logical interface also apply to configuring a static or dynamic 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 or MPC level, configure the aggregated Ethernet interface on physical interfaces that reside on different EQ DPC or Trio MPC modules.



**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 Documentation

- Static Subscriber Interfaces and VLAN Overview on page 434
- Configuring a Static or Dynamic VLAN Subscriber Interface over Aggregated Ethernet on page 479
- Example: Configuring a Static Subscriber Interface on a VLAN Interface over Aggregated Ethernet on page 489
- Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660
- CoS for Subscriber Access Overview on page 659

## Static or Dynamic Demux Subscriber Interfaces over Aggregated Ethernet Overview

---

You can configure a subscriber interface using a static or dynamic demux interface stacked on an aggregated Ethernet logical interface. Subscriber interfaces on static or dynamic 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 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 demux subscriber interface over aggregated Ethernet, make sure you understand the following concepts:

- Options for Aggregated Ethernet Logical Interfaces That Support Demux Subscriber Interfaces on page 472
- Hardware Requirements with Static or Dynamic Demux Subscriber Interfaces over Aggregated Ethernet on page 473
- Features Supported with Static or Dynamic Demux Subscriber Interfaces over Aggregated Ethernet on page 473

## Options for Aggregated Ethernet Logical Interfaces That Support Demux Subscriber Interfaces

Traffic forwarding through a demux logical interface is dependent on the configuration of the underlying interface. Using an aggregated Ethernet interface as the underlying interface for a static or dynamic 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 line card level, configure the aggregated Ethernet interface on physical interfaces that reside either on different EQ DPCs or on different Trio MPCs. When using LACP link protection, you can configure only two member links to an aggregated Ethernet interface: one active and one standby.

- **Load Balancing**—You can configure load balancing instead of 1:1 active/backup link redundancy. The Junos OS 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.

By default, the system supports hash-based distribution in load balancing scenarios. In this model, traffic for a logical interface can be distributed over multiple links in the aggregated Ethernet interface. If distribution flows are not even, egress CoS scheduling can be inaccurate. In addition, scheduler resources are required on every link of the aggregated Ethernet interface.

Targeted distribution enables you to target the egress traffic for IP and VLAN demux subscribers on a single member link, using a single scheduler resource. The system distributes the subscriber interfaces equally among the member links.

## Hardware Requirements with Static or Dynamic Demux Subscriber Interfaces over Aggregated Ethernet

IP demux subscriber interfaces over aggregated Ethernet interfaces are supported on EQ DPCs on MX Series routers.

VLAN demux subscriber interfaces over aggregated Ethernet interfaces are supported on MX Series routers that only have Trio MPCs installed. If the router has other line cards in addition to Trio MPCs, the CLI accepts the configuration but errors are reported when the subscriber interfaces are brought up.

## Features Supported with Static or Dynamic Demux Subscriber Interfaces over Aggregated Ethernet

Table 48 on page 474 lists key subscriber access features supported with static or dynamic demux subscriber interfaces, organized by type of underlying interface:

- Aggregated Ethernet
- Non-aggregated Ethernet (Gigabit Ethernet, Fast Ethernet, or 10-Gigabit Ethernet)

There are no feature limitations specific to demultiplexing. Instead, demux interfaces over aggregated Ethernet are subject to the same scaling and configuration limitations inherent to aggregated Ethernet logical interfaces.

Table 48: Features Supported with Static or Dynamic Demux Subscriber Interfaces

Feature	Static or Dynamic Demux Subscriber Interface	
	Aggregated Ethernet Underlying Interface	Non-aggregated Underlying Logical Interface
Protocol family support	IPv4, IPv6, and PPPoE	IPv4, IPv6, and PPPoE
Per-subscriber firewall filtering and statistics	Supported	Supported
Hierarchical CoS	Supported	Supported
Per-subscriber CoS parameters within the <b>[edit dynamic-profiles <i>profile-name</i> class-of-service]</b> hierarchy	Supported	Supported
Per-subscriber IGMP configuration within the <b>[edit dynamic-profiles <i>profile-name</i> protocols]</b> hierarchy	Yes	Yes

**NOTE:** IP demux interfaces must use OIF mapping. See Example: Configuring Multicast with Subscriber VLANs in the [Junos OS Multicast Protocols Configuration Guide](#) for additional information.

#### Related Documentation

- Subscriber Interfaces and Demultiplexing Overview on page 435
- Distribution of Demux Subscribers in an Aggregated Ethernet Interface on page 474
- Configuring a Static or Dynamic IP Demux Subscriber Interface over Aggregated Ethernet on page 481
- Configuring the PPPoE Family for an Underlying Interface on page 486
- Example: Configuring a Static Subscriber Interface on an IP Demux Interface over Aggregated Ethernet on page 492
- For more information about aggregated Ethernet interfaces, see the [Junos OS Network Interfaces Configuration Guide](#).

## Distribution of Demux Subscribers in an Aggregated Ethernet Interface

This topic describes the distribution options available for demux subscriber interfaces over aggregated Ethernet.

### Distribution Models

By default, the system supports hash-based distribution for all subscriber interface types in an aggregated Ethernet bundle configured without link protection. In this model, traffic for a logical interface can be distributed over multiple links in the bundle. This model is desirable when there are many flows through the logical interface and you need to load balance those flows.

Note that if the distribution flows are not even, egress CoS scheduling can be inaccurate. In addition, scheduler resources are required on every link of the aggregated Ethernet



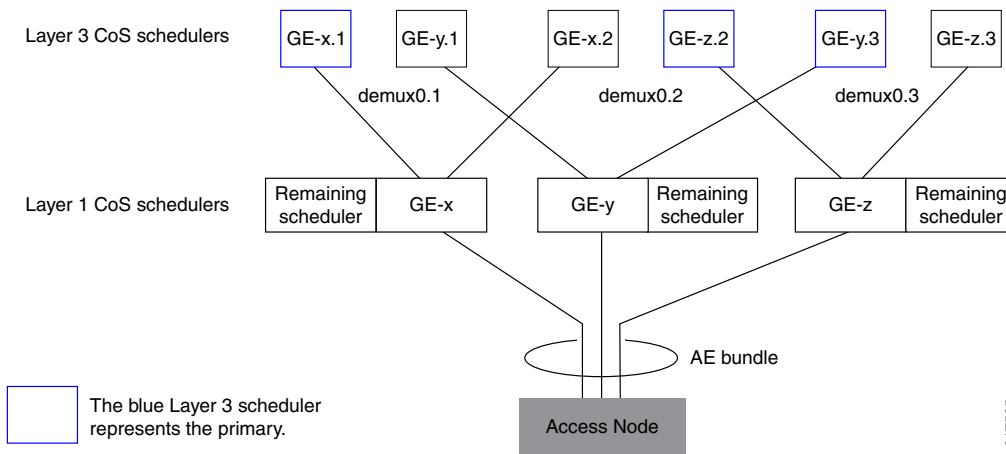
interface. For example, if subscriber traffic is allocated 10 MB for a triple-play service over four links in a bundle, each of the links could receive 2.5 MB of traffic. High-density services such as video could be limited by the bandwidth on one of the links.

Targeted distribution enables you to target the egress traffic for an IP or VLAN demux subscriber on a single member link, using a single scheduler resource. To achieve load balancing over the member links, the system distributes the subscriber interfaces equally among the links. This enables the subscriber that is allocated 10 MB to be accurately scheduled as the traffic flows through.

## Sample Targeted Distribution Topology

Figure 11 on page 475 displays a sample targeted distribution of subscriber traffic across links in an aggregated Ethernet interface. A primary and backup link is allocated for each subscriber.

Figure 11: Targeted Subscriber Links



For example, if link **GE-x** went down, subscriber 1 can begin forwarding over the backup, which is link **GE-y**. When link **GE-y** comes back up, subscriber 1 switches back to its primary link, **GE-x**.

In the event that both **GE-x** and **GE-y** go down, subscriber 3 starts forwarding through its backup, **GE-z**. Subscriber 1 will have lost its primary and backup links, and will also begin forwarding out the **GE-z** link. A new level 3 scheduler is assigned for this subscriber on link **GE-z**. If there is a momentary lapse between the time that a new scheduler is allocated and forwarding switches to **GE-z**, the traffic will be forwarding through to the remaining scheduler. Subscriber 2 continues to forward through its primary link, **GE-z**.

## Redundancy and Redistribution Mechanisms

Two types of redundancy are available in the targeted distribution model: link redundancy and module redundancy.

By default, an aggregated Ethernet interface is enabled with link redundancy. Backup links for a subscriber are chosen based on the link with the least number of subscribers, which provides redundancy if a link fails.

The module redundancy option enables you to provide redundancy if a module or a link fails. Backup links for a subscriber are chosen on a different DPC or MPC from the primary link, based on the link with the least number of subscribers among the links on different modules. You can enable this for the aggregated Ethernet interface.

When links are removed, affected subscribers are redistributed among the active remaining backup links. When links are added to the system, no automatic redistribution occurs. New subscribers are assigned to the links with the fewest subscribers (which are typically the new links).

## Considerations and Best Practices

Keep the following guidelines in mind when configuring targeted distribution for demux subscribers:

- You can manage subscribers with both hash-based and targeted distribution models in the same network. For example, you can allocate subscribers with interface types such as PPPoE with hash-based distribution, and enable demux subscribers with targeted distribution.
- We recommend that you configure module redundancy to protect against module failures. When module redundancy is enabled, you can ensure an even distribution of subscribers if you allocate no more than 50 percent of the links on a single DPC or MPC.
- During normal network operations, the system maintains an even balance of subscribers among the links in a bundle, even as subscribers log in and out. However, if the distribution of a bundle becomes uneven (for example, when a link goes down and new subscribers are logging in), you can perform a manual rebalance of the bundle. In addition, you can configure periodic rebalancing of the bundle with a specific time interval.
- When you anticipate that a link will be down for an extended time, and you want to ensure that backup links are provisioned for all subscribers, we recommend that you remove the failed link from the bundle. This forces the affected subscribers to redistribute to other links.
- We recommend that you apply a remaining traffic-control profile to the logical interface to ensure that minimal scheduling parameters are applied to the remaining subscriber traffic. This provides scheduling for subscribers that do not have schedulers allocated because they have not been configured or they have been over-provisioned, or because of scheduler transitions on multiple link failures.
- If you perform a cold restart on the router when it is forwarding active subscribers, the subscriber interfaces with targeted distribution are assigned to the first links that become available when the system is initializing so forwarding can begin. To rebalance the system following a cold restart, perform a manual rebalance of the bundle. In addition, we recommend that you configure Graceful Routing Engine switchover (GRES) on the router to enable nonstop forwarding during switchover, and avoid performing cold restarts.

### Related Documentation

- [Configuring the Distribution Type for Demux Subscribers on Aggregated Ethernet Interfaces on page 484](#)

- [Configuring Link and Module Redundancy for Demux Subscribers in an Aggregated Ethernet Interface on page 484](#)
- [Configuring Rebalancing of Demux Subscribers in an Aggregated Ethernet Interface on page 485](#)
- [For additional information about demux over aggregated Ethernet interfaces, see Static or Dynamic Demux Subscriber Interfaces over Aggregated Ethernet Overview on page 472](#)



# Configuring Subscriber Interfaces over Aggregated Ethernet

- Configuring a Static or Dynamic VLAN Subscriber Interface over Aggregated Ethernet on page 479
- Configuring a Static or Dynamic IP Demux Subscriber Interface over Aggregated Ethernet on page 481
- Configuring a Static or Dynamic VLAN Demux Subscriber Interface over Aggregated Ethernet on page 482
- Configuring the Distribution Type for Demux Subscribers on Aggregated Ethernet Interfaces on page 484
- Configuring Link and Module Redundancy for Demux Subscribers in an Aggregated Ethernet Interface on page 484
- Configuring Rebalancing of Demux Subscribers in an Aggregated Ethernet Interface on page 485
- Verifying the Distribution of Demux Subscribers in an Aggregated Ethernet Interface on page 486
- Configuring the PPPoE Family for an Underlying Interface on page 486

## Configuring a Static or Dynamic VLAN Subscriber Interface over Aggregated Ethernet

You can configure a subscriber link represented by a static virtual LAN (VLAN) stacked on an aggregated Ethernet logical interface.

You can configure subscriber management services such as firewall filters and CoS for this subscriber interface.

To configure a subscriber interface using a static VLAN interface over an aggregated Ethernet logical interface:

1. Configure the aggregated Ethernet interface.
  - a. Configure the number of aggregated Ethernet interfaces on the router.  
See *Configuring the Number of Aggregated Ethernet Interfaces on the Device*.
  - b. Configure the aggregated Ethernet interface.

See Configuring an Aggregated Ethernet Interface.

- c. (Optional) Configure LACP.

See Configuring Aggregated Ethernet LACP.

- d. (Optional) Configure the minimum number of links.

See Configuring Aggregated Ethernet Minimum Links.

- e. (Optional) Configure the link speed.

See Configuring Aggregated Ethernet Link Speed.

- f. (Optional) Configure the aggregated Ethernet logical interface to support one-to-one active/backup link redundancy or traffic load balancing.

See Configuring Aggregated Ethernet Link Protection.



**NOTE:** Link protection is required if you want to configure hierarchical CoS on the aggregated Ethernet interface. For more information, see “Configuring Hierarchical CoS for a Subscriber Interface of Aggregated Ethernet Links” on page 707.

---

2. Configure the static or dynamic VLAN interface.

- For static VLAN interfaces, see “Configuring a Subscriber Interface with a Static VLAN Interface” on page 440.
- For dynamic VLAN interfaces, see “Configuring VLAN Dynamic Profiles” on page 409 and “Configuring VLAN Interfaces to Use Dynamic Profiles” on page 416.

3. Configure subscriber management services on the subscriber interface.

- For firewall filters, see “Dynamically Attaching Statically Created Filters for Any Interface Type” on page 572 or “Dynamically Attaching Statically Created Filters for a Specific Interface Family Type” on page 571.
- For hierarchical CoS, see “Configuring Hierarchical CoS for a Subscriber Interface of Aggregated Ethernet Links” on page 707.

**Related  
Documentation**

- Static and Dynamic VLAN Subscriber Interfaces over Aggregated Ethernet Overview on page 471
- Example: Configuring a Static Subscriber Interface on a VLAN Interface over Aggregated Ethernet on page 489
- Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660
- CoS for Subscriber Access Overview on page 659

## 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.

1. Configure the aggregated Ethernet interface.
  - a. Configure the number of aggregated Ethernet interfaces on the router.  
See [Configuring the Number of Aggregated Ethernet Interfaces on the Device](#).
  - b. Configure the aggregated Ethernet interface.  
See [Configuring an Aggregated Ethernet Interface](#).
  - c. (Optional) Configure LACP.  
See [Configuring Aggregated Ethernet LACP](#).
  - d. (Optional) Configure the minimum number of links.  
See [Configuring Aggregated Ethernet Minimum Links](#).
  - e. (Optional) Configure the link speed.  
See [Configuring Aggregated Ethernet Link Speed](#).
  - f. (Optional) Configure the aggregated Ethernet logical interface to support one-to-one active/backup link redundancy or traffic load balancing.  
For general instructions, see [Configuring Aggregated Ethernet Link Protection](#).



**NOTE:** Link protection is required if you want to configure hierarchical CoS on the aggregated Ethernet interface. For more information, see “Configuring Hierarchical CoS for a Subscriber Interface of Aggregated Ethernet Links” on page 707.

2. Configure the aggregated Ethernet logical interface as the underlying interface to support the static or dynamic IP demux subscriber interface.  
  
The aggregated Ethernet interface needs to support demultiplexing of incoming traffic to the Ethernet links based on IPv4 destination or source addresses in the incoming packets. In addition, you must configure the IP address of each link.  
  
See [Configuring an IP Demux Underlying Interface](#).
3. Configure the static or dynamic IP demux interface.
  - For static subscriber interfaces, see “Configuring Static Subscriber Interfaces Using IP Demux Interfaces” on page 440.

- For dynamic subscriber interfaces, see “Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles” on page 445.



**NOTE:** IP demux interfaces currently support only the Internet Protocol version 4 (IPv4) suite (`family inet`).

4. (Optional) Configure subscriber management services on the subscriber interface.
  - For firewall filters, see “Dynamically Attaching Statically Created Filters for Any Interface Type” on page 572 or “Dynamically Attaching Statically Created Filters for a Specific Interface Family Type” on page 571.
  - For hierarchical CoS, see “Configuring Hierarchical CoS for a Subscriber Interface of Aggregated Ethernet Links” on page 707.

**Related Documentation**

- Subscriber Interfaces and Demultiplexing Overview on page 435
- Static or Dynamic Demux Subscriber Interfaces over Aggregated Ethernet Overview on page 472
- Example: Configuring a Static Subscriber Interface on an IP Demux Interface over Aggregated Ethernet on page 492
- Configuring the Distribution Type for Demux Subscribers on Aggregated Ethernet Interfaces on page 484

---

## Configuring a Static or Dynamic VLAN Demux Subscriber Interface over Aggregated Ethernet

---

You can configure a subscriber interface using a static or dynamic VLAN demultiplexing (demux) logical interface stacked on an aggregated Ethernet physical interface.

1. Configure the aggregated Ethernet interface.
  - a. Configure the number of aggregated Ethernet interfaces on the router.  
See [Configuring the Number of Aggregated Ethernet Interfaces on the Device](#).
  - b. Configure the aggregated Ethernet interface.  
See [Configuring an Aggregated Ethernet Interface](#).
  - c. (Optional) Configure LACP.  
See [Configuring Aggregated Ethernet LACP](#).
  - d. (Optional) Configure the minimum number of links.  
See [Configuring Aggregated Ethernet Minimum Links](#).
  - e. (Optional) Configure the link speed.



See Configuring Aggregated Ethernet Link Speed.

- f. (Optional) Configure the aggregated Ethernet logical interface to support one-to-one active/backup link redundancy or traffic load balancing.

For general instructions, see Configuring Aggregated Ethernet Link Protection.

2. Configure the aggregated Ethernet physical interface as the underlying interface to support the static or dynamic VLAN demux subscriber interface.

The aggregated Ethernet interface needs to support demultiplexing of incoming traffic to the Ethernet links based on the VLAN ID in the incoming packets.

See Configuring a VLAN Demux Underlying Interface.

3. Configure the static or dynamic VLAN demux interface.

- For static subscriber interfaces, see “Configuring Static Subscriber Interfaces Using VLAN Demux Interfaces” on page 441.
- For dynamic subscriber interfaces, see “Configuring Dynamic Subscriber Interfaces Using VLAN Demux Interfaces in Dynamic Profiles” on page 446.



**NOTE:** VLAN demux interfaces currently support the Internet Protocol version 4 (IPv4) suite (`family inet`) and the Internet Protocol version 6 (IPv6) suite (`family inet6`).

VLAN demux subscriber interfaces over aggregated Ethernet physical interfaces are supported only for MX Series routers that have only Trio MPCs installed. If the router has other cards in addition to Trio MPCs, the CLI accepts the configuration but errors are reported when the subscriber interfaces are brought up.

4. (Optional) Configure subscriber management services on the subscriber interface.
  - For firewall filters, see “Dynamically Attaching Statically Created Filters for Any Interface Type” on page 572 or “Dynamically Attaching Statically Created Filters for a Specific Interface Family Type” on page 571.
  - For hierarchical CoS, see “Configuring Hierarchical CoS for a Subscriber Interface of Aggregated Ethernet Links” on page 707.

#### Related Documentation

- Subscriber Interfaces and Demultiplexing Overview on page 435
- Static or Dynamic Demux Subscriber Interfaces over Aggregated Ethernet Overview on page 472
- Associating VLAN IDs to VLAN Demux Interfaces
- Example: Configuring IPv4 Static VLAN Demux Interfaces over a Gigabit Ethernet Underlying Interface with DHCP Local Server on page 462
- Example: Configuring IPv4 Static VLAN Demux Interfaces over an Aggregated Ethernet Underlying Interface with DHCP Local Server on page 497

- Example: Configuring IPv4 Dynamic VLAN Demux Interfaces over a Gigabit Ethernet Underlying Interface with DHCP Local Server on page 464
- Example: Configuring IPv4 Dynamic VLAN Demux Interfaces over an Aggregated Ethernet Underlying Interface with DHCP Local Server on page 500

## Configuring the Distribution Type for Demux Subscribers on Aggregated Ethernet Interfaces

---

By default, the system supports hash-based distribution of subscriber traffic in aggregated Ethernet bundles. You can configure the system to target the egress traffic for a subscriber on a single member link, using a single scheduler resource. The system distributes the subscriber interfaces equally among the member links.

To configure targeted distribution:

1. Access the logical interface.

```
[edit]
user@host#edit interfaces demux0 unit logical-unit-number
```

2. Enable targeted distribution for the interface.

```
[edit interfaces demux0 unit logical-unit-number]
user@host#set targeted-distribution
```

### Related Documentation

- Verifying the Distribution of Demux Subscribers in an Aggregated Ethernet Interface on page 486
- Distribution of Demux Subscribers in an Aggregated Ethernet Interface on page 474

## Configuring Link and Module Redundancy for Demux Subscribers in an Aggregated Ethernet Interface

---

By default, an aggregated Ethernet bundle with targeted distribution is enabled with link redundancy. Backup links for a subscriber are chosen based on the link with the fewest subscribers, which provides redundancy if a link fails.

We recommend that you configure the module redundancy option to provide redundancy if a module or a link fails. Backup links for a subscriber are chosen on a different DPC or MPC from the primary link, based on the link with the fewest subscribers among the links on different modules.

To configure module redundancy for an aggregated Ethernet bundle:

1. Access the aggregated Ethernet bundle for which you want to configure module redundancy.

```
edit
user@host# edit interfaces aex aggregated-ether-options
```

2. Enable module redundancy for the bundle.

```
[edit interfaces aex aggregated-ether-options]
user@host# logical-interface-fpc-redundancy
```

**Related  
Documentation**

- Configuring the Distribution Type for Demux Subscribers on Aggregated Ethernet Interfaces on page 484
- Distribution of Demux Subscribers in an Aggregated Ethernet Interface on page 474

## Configuring Rebalancing of Demux Subscribers in an Aggregated Ethernet Interface

In a targeted distribution model, the system allocates demux subscriber interfaces equally among the member links in the aggregated Ethernet interface. When links are removed, affected subscribers are redistributed among the active remaining backup links. When links are added to the system, no automatic redistribution occurs. New subscribers are assigned to the links with the fewest subscribers (which are typically the new links).

During normal network operations, the system maintains an even balance of traffic among the links in a bundle, even as subscribers log in and out. However, if the distribution of a bundle becomes uneven (for example, when a link goes down for a period of time and new subscribers are logging in), you can perform a manual rebalance of the bundle. In addition, you can configure periodic rebalancing of the bundle with a specific interval.

- Configuring Periodic Rebalancing of Subscribers in an Aggregated Ethernet Interface on page 485
- Configuring Manual Rebalancing of Subscribers on an Aggregated Ethernet Interface on page 485

## Configuring Periodic Rebalancing of Subscribers in an Aggregated Ethernet Interface

If subscribers are frequently logging in and logging out of your network, you can configure the system to periodically rebalance the links based on a specific time and interval.

To configure periodic rebalancing:

1. Access the aggregated Ethernet interface for which you want to configure periodic rebalancing.

```
edit
user@host# edit interfaces aenumber aggregated-ether-options
```

2. Configure the rebalancing parameters for the interface, including the time and the interval between rebalancing actions.

```
[edit interfaces aenumber aggregated-ether-options]
user@host# rebalance-periodic time hour:minute <interval hours>
```

## Configuring Manual Rebalancing of Subscribers on an Aggregated Ethernet Interface

To manually rebalance the subscribers among the links in an aggregated Ethernet bundle with targeted distribution:

- Issue the **request interface rebalance** command:

`user@host# request interface rebalance interface <interface-name>`

- Related Documentation**
- Verifying the Distribution of Demux Subscribers in an Aggregated Ethernet Interface on page 486
  - Configuring the Distribution Type for Demux Subscribers on Aggregated Ethernet Interfaces on page 484
  - Distribution of Demux Subscribers in an Aggregated Ethernet Interface on page 474

---

## Verifying the Distribution of Demux Subscribers in an Aggregated Ethernet Interface

**Purpose** View the distribution status of subscribers that are targeted to links in an aggregated Ethernet interface.

- Action**
- To display a summary of the distribution of links on the demux interface:  
`user@host> show interfaces demux0 extensive`
  - To display the targeted distribution on a specific aggregated Ethernet interface:  
`user@host> show interfaces targeting aex`

- Related Documentation**
- Configuring the Distribution Type for Demux Subscribers on Aggregated Ethernet Interfaces on page 484
  - Configuring Rebalancing of Demux Subscribers in an Aggregated Ethernet Interface on page 485

---

## Configuring the PPPoE Family for an Underlying Interface

You can configure the PPPoE family on an underlying interface as an alternative to configuring PPPoE encapsulation on that interface. You cannot configure both on the same interface. You can configure the same attributes for the PPPoE family as you can for an interface configured with **pppoe-underlying-options**.

Before you begin, configure the underlying interface. When you want to configure PPPoE on an aggregated Ethernet bundle, you must configure the PPPoE family over a VLAN demux interface as an intermediate underlying option. The VLAN demux interface can be static or dynamic.

The following topics describe how to configure basic static and dynamic interfaces.

- Configuring a Subscriber Interface with a Static VLAN Interface on page 440
- Configuring Static Subscriber Interfaces Using VLAN Demux Interfaces on page 441
- Configuring Dynamic Subscriber Interfaces Using VLAN Demux Interfaces in Dynamic Profiles on page 446

To configure the PPPoE family over an underlying interface:

1. Specify the PPPoE family.

```
[edit interfaces demux0 vlan-tagging unit logical-unit-number]
user@host# set family pppoe
```

2. (Optional) Configure an alternative access concentrator name to be used instead of the system name in PPPoE control packets for the dynamic PPPoE subscriber interface.

```
[edit interfaces demux0 vlan-tagging unit logical-unit-number family pppoe]
user@host# set access-concentrator name
```

3. (Optional) Configure duplicate protection to prevent the activation of another dynamic PPPoE logical interface on the same underlying interface when a dynamic PPPoE logical interface for a client with the same MAC address is already active on that interface.

```
[edit interfaces demux0 vlan-tagging unit logical-unit-number family pppoe]
user@host# set duplicate-protection
```

4. (Optional) Attach a dynamic profile to determine the properties of the dynamic PPPoE logical interface when it is created.

```
[edit interfaces demux0 vlan-tagging unit logical-unit-number family pppoe]
user@host# set dynamic-profile profile-name
```

5. (Optional) Configure the maximum number of PPPoE sessions allowed on the underlying interface.

```
[edit interfaces demux0 vlan-tagging unit logical-unit-number family pppoe]
user@host# set max-sessions number
```

6. (Optional) Specify the service name table assigned to the underlying interface.

```
[edit interfaces demux0 vlan-tagging unit logical-unit-number family pppoe]
user@host# set service-name-table table-name
```

#### Related Documentation

- Static or Dynamic Demux Subscriber Interfaces over Aggregated Ethernet Overview on page 472
- Example: Configuring a Static PPPoE Subscriber Interface on a Static Underlying VLAN Demux Interface over Aggregated Ethernet on page 509
- Example: Configuring a Dynamic PPPoE Subscriber Interface on a Static Underlying VLAN Demux Interface over Aggregated Ethernet on page 514
- Example: Configuring a Dynamic PPPoE Subscriber Interface on a Dynamic Underlying VLAN Demux Interface over Aggregated Ethernet on page 519



# Subscriber Interfaces over Aggregated Ethernet Examples

- Example: Configuring a Static Subscriber Interface on a VLAN Interface over Aggregated Ethernet on page 489
- Example: Configuring a Static Subscriber Interface on an IP Demux Interface over Aggregated Ethernet on page 492
- Example: Configuring a Static Subscriber Interface on a VLAN Interface over Aggregated Ethernet on page 494
- Example: Configuring IPv4 Static VLAN Demux Interfaces over an Aggregated Ethernet Underlying Interface with DHCP Local Server on page 497
- Example: Configuring IPv4 Dynamic VLAN Demux Interfaces over an Aggregated Ethernet Underlying Interface with DHCP Local Server on page 500
- Example: Configuring IPv6 Dynamic VLAN Demux Interfaces over an Aggregated Ethernet Underlying Interface with DHCP Local Server on page 503
- Example: Configuring IPv4 Dynamic Stacked VLAN Demux Interfaces over an Aggregated Ethernet Underlying Interface with DHCP Local Server on page 506
- Example: Configuring a Static PPPoE Subscriber Interface on a Static Underlying VLAN Demux Interface over Aggregated Ethernet on page 509
- Example: Configuring a Dynamic PPPoE Subscriber Interface on a Static Underlying VLAN Demux Interface over Aggregated Ethernet on page 514
- Example: Configuring a Dynamic PPPoE Subscriber Interface on a Dynamic Underlying VLAN Demux Interface over Aggregated Ethernet on page 519

## 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 MX Series routers.

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 **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 Documentation

- Static and Dynamic VLAN Subscriber Interfaces over Aggregated Ethernet Overview on page 471
- Configuring a Static or Dynamic VLAN Subscriber Interface over Aggregated Ethernet on page 479
- Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660
- CoS for Subscriber Access Overview on page 659

## 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 {
    gether-options {
      802.3ad {
        ae0;
        primary;
      }
    }
  }
  ge-5/1/2 {
    gether-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 Documentation**
- [Subscriber Interfaces and Demultiplexing Overview on page 435](#)
  - [Static or Dynamic Demux Subscriber Interfaces over Aggregated Ethernet Overview on page 472](#)
  - [Configuring a Static or Dynamic IP Demux Subscriber Interface over Aggregated Ethernet on page 481](#)

---

## 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 MX Series routers.

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 Documentation**

- Static and Dynamic VLAN Subscriber Interfaces over Aggregated Ethernet Overview on page 471
- Configuring a Static or Dynamic VLAN Subscriber Interface over Aggregated Ethernet on page 479
- Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660
- CoS for Subscriber Access Overview on page 659

## Example: Configuring IPv4 Static VLAN Demux Interfaces over an Aggregated Ethernet Underlying Interface with DHCP Local Server

This example shows how to configure a static IPv4 VLAN demux interface with aggregated Ethernet as the underlying interface. DHCP Local Server configuration enables the association of subscribers to the VLAN demux interface by listing the aggregated Ethernet interface in the DHCP local server configuration.

To configure dynamic subscribers on VLAN demux interfaces:

1. Enable hierarchical scheduling and VLAN tagging on the underlying interface that you plan to use for any VLAN demux interfaces.

```

interfaces {
  ae1 {
    hierarchical-scheduler;
    vlan-tagging;
    aggregated-ether-options {
      minimum-links 1;
      lacp {
        active;
        periodic slow;
        link-protection {
          non-revertive;
        }
      }
    }
  }
}

```

2. Define the gigabit Ethernet interfaces that are part of the aggregated Ethernet interface.

```

interfaces {
  ge-5/0/0 {
    gigether-options {

```

```
        802.3ad ae1;
    }
}
ge-5/2/0 {
    gige-ether-options {
        802.3ad ae1;
    }
}
}
```

3. Define the demux interface.

```
interfaces {
    demux0 {
        unit 102 {
            proxy-arp;
            vlan-id 103;
            demux-options {
                underlying-interface ae1;
            }
            family inet {
                unnumbered-address lo0.0 preferred-source-address 173.16.1.1;
            }
        }
    }
}
```

4. Define the loopback interface.

```
interfaces {
    lo0 {
        unit 0 {
            family inet {
                address 192.16.1.1/32;
            }
        }
    }
}
```

5. Configure a dynamic profile for initial subscriber access.

```
dynamic-profiles {
    user-profile {
        interfaces {
            "$junos-interface-ifd-name" {
                unit "$junos-underlying-interface-unit" {
                    family inet;
                }
            }
        }
    }
    protocols {
        igmp {
            interface "$junos-interface-name" {
                version 3;
                immediate-leave;
                promiscuous-mode;
            }
        }
    }
}
```



```

    }
  }
}

```

6. Configure the access method used to dynamically create the subscriber interfaces.

The following stanza specifies the aggregated Ethernet interface (**ae1.0**) for use with the dynamically created subscriber interfaces.

```

system {
  services {
    dhcp-local-server {
      group myDhcpGroup {
        authentication {
          password test;
          username-include {
            user-prefix igmp-user1;
          }
        }
        dynamic-profile user-profile;
        interface ae1.0;
      }
    }
  }
}

```

Instead of using the aggregated Ethernet interface, you can alternatively specify the specific demux interface (**demux0.102**) as the device to use with the subscriber interfaces as follows:

```

system {
  services {
    dhcp-local-server {
      group myDhcpGroup {
        authentication {
          password test;
          username-include {
            user-prefix igmp-user1;
          }
        }
        dynamic-profile user-profile;
        interface demux0.102;
      }
    }
  }
}

```

#### Related Documentation

- [Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 445](#)
- [Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125](#)

## Example: Configuring IPv4 Dynamic VLAN Demux Interfaces over an Aggregated Ethernet Underlying Interface with DHCP Local Server

This example shows how to configure the dynamic creation of IPv4 VLAN demux interfaces with aggregated Ethernet as the underlying interface. DHCP Local Server configuration enables the association of subscribers to the VLAN demux interface by listing the aggregated Ethernet interface in the DHCP local server configuration.



**NOTE:** VLAN demux subscriber interfaces over aggregated Ethernet physical interfaces are supported only for MX Series routers that have only Trio MPCs installed. If the router has other cards in addition to Trio MPCs, the CLI accepts the configuration but errors are reported when the subscriber interfaces are brought up.

To configure dynamic subscribers on dynamic VLAN demux interfaces:

1. Enable VLAN tagging and VLAN auto-configuration on the underlying aggregated Ethernet interface that you plan to use for dynamically created VLAN demux interfaces.

```
interfaces {
  ae1 {
    vlan-tagging;
    auto-configure {
      vlan-ranges {
        dynamic-profile auto-vlanDemux-profile {
          accept inet;
          ranges {
            any;
          }
        }
      }
    }
    aggregated-ether-options {
      minimum-links 1;
      lacp {
        active;
        periodic slow;
        link-protection {
          non-revertive;
        }
      }
    }
  }
}
```

2. Define the gigabit Ethernet interfaces that are part of the aggregated Ethernet interface.

```
interfaces {
  ge-5/0/0 {
    giger-options {
      802.3ad ae1;
    }
  }
}
```

```

    }
    ge-5/2/0 {
      gether-options {
        802.3ad ael;
      }
    }
  }
}

```

3. Define the loopback interface.

```

interfaces {
  lo0 {
    unit 0 {
      family inet {
        address 192.16.1.1/32;
      }
    }
  }
}

```

4. Configure a dynamic profile for subscriber access.

```

dynamic-profiles {
  user-profile {
    interfaces {
      "$junos-interface-ifd-name" {
        unit "$junos-underlying-interface-unit" {
          family inet;
        }
      }
    }
  }
}

```

5. Configure a dynamic profile for VLAN demux interface creation.

```

dynamic-profiles {
  auto-vlanDemux-profile {
    interfaces {
      demux0 {
        unit "$junos-interface-unit" {
          vlan-id "$junos-vlan-id";
          demux-options {
            underlying-interface "$junos-interface-ifd-name";
          }
          family inet {
            filter {
              input rate_limit;
              output rate_limit;
            }
            unnumbered-address lo0.0 preferred-source-address 192.16.1.1;
          }
        }
      }
    }
  }
}

```

6. Configure the access method used to dynamically create the subscriber interfaces. The following stanza specifies the aggregated Ethernet interface (**ae1.0**) for use with the dynamically created subscriber interfaces.

```
system {
  services {
    dhcp-local-server {
      group myDhcpGroup {
        authentication {
          password test;
          username-include {
            user-prefix igmp-user1;
          }
        }
        dynamic-profile user-profile;
        interface ae1.0;
      }
    }
  }
}
```

Instead of using the aggregated Ethernet interface, you can alternatively specify **demux0** as the device to use with the subscriber interfaces as follows:



**NOTE:** Because the demux interfaces and unit values are created dynamically, the unit number is not specified for the demux0 interface.

```
system {
  services {
    dhcp-local-server {
      group myDhcpGroup {
        authentication {
          password test;
          username-include {
            user-prefix igmp-user1;
          }
        }
        dynamic-profile user-profile;
        interface demux0;
      }
    }
  }
}
```

#### Related Documentation

- [Configuring Dynamic Subscriber Interfaces Using VLAN Demux Interfaces in Dynamic Profiles on page 446](#)
- [Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125](#)

## Example: Configuring IPv6 Dynamic VLAN Demux Interfaces over an Aggregated Ethernet Underlying Interface with DHCP Local Server

This example shows how to configure the dynamic creation of IPv6 VLAN demux interfaces with aggregated Ethernet as the underlying interface. DHCP Local Server configuration enables the association of subscribers to the VLAN demux interface by listing the aggregated Ethernet interface in the DHCP local server configuration.



**NOTE:** VLAN demux subscriber interfaces over aggregated Ethernet physical interfaces are supported only for MX Series routers that have only Trio MPCs installed. If the router has other cards in addition to Trio MPCs, the CLI accepts the configuration but errors are reported when the subscriber interfaces are brought up.

To configure dynamic subscribers on dynamic VLAN demux interfaces:

1. Enable VLAN tagging and VLAN auto-configuration on the underlying aggregated Ethernet interface that you plan to use for dynamically created VLAN demux interfaces.

```
interfaces {
  ae1 {
    vlan-tagging;
    auto-configure {
      vlan-ranges {
        dynamic-profile auto-vlanDemux-profile {
          accept inet6;
          ranges {
            any;
          }
        }
      }
    }
    aggregated-ether-options {
      minimum-links 1;
      lacp {
        active;
        periodic slow;
        link-protection {
          non-revertive;
        }
      }
    }
  }
}
```

2. Define the gigabit Ethernet interfaces that are part of the aggregated Ethernet interface.

```
interfaces {
  ge-5/0/0 {
    gigether-options {
      802.3ad ae1;
    }
  }
}
```

```
    }
    ge-5/2/0 {
      gigeether-options {
        802.3ad ael;
      }
    }
  }
}
```

3. Define the loopback interface.

```
interfaces {
  lo0 {
    unit 0 {
      family inet6 {
        address 2009:174:1:1::1/128;
      }
    }
  }
}
```

4. Configure a dynamic profile for subscriber access.

```
dynamic-profiles {
  user-profile {
    interfaces {
      "$junos-interface-ifd-name" {
        unit "$junos-underlying-interface-unit" {
          family inet6;
        }
      }
    }
  }
}
```

5. Configure a dynamic profile for VLAN demux interface creation.

```
dynamic-profiles {
  auto-vlanDemux-profile {
    interfaces {
      demux0 {
        unit "$junos-interface-unit" {
          vlan-id "$junos-vlan-id";
          demux-options {
            underlying-interface "$junos-interface-ifd-name";
          }
          family inet6 {
            filter {
              input v6_rate_limit;
              output v6_rate_limit;
            }
            unnumbered-address lo0.0 preferred-source-address 2009:174:1:1::1;
          }
        }
      }
    }
  }
}
```

6. Configure the access method used to dynamically create the subscriber interfaces. The following stanza specifies the aggregated Ethernet interface (**ae1.0**) for use with the dynamically created subscriber interfaces.

```
system {
  services {
    dhcp-local-server {
      dhcpv6 {
        group myV6DhcpGroup {
          authentication {
            password test;
            username-include {
              user-prefix igmp-user1;
            }
          }
          dynamic-profile user-profile;
          interface ae1.0;
        }
      }
    }
  }
}
```

Instead of using the aggregated Ethernet interface, you can alternatively specify **demux0** as the device to use with the subscriber interfaces as follows:



**NOTE:** Because the demux interfaces and unit values are created dynamically, the unit number is not specified for the demux0 interface.

```
system {
  services {
    dhcp-local-server {
      dhcpv6 {
        group myV6DhcpGroup {
          authentication {
            password test;
            username-include {
              user-prefix igmp-user1;
            }
          }
          dynamic-profile user-profile;
          interface demux0;
        }
      }
    }
  }
}
```

**Related Documentation**

- Configuring Dynamic Subscriber Interfaces Using VLAN Demux Interfaces in Dynamic Profiles on page 446
- Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125

## Example: Configuring IPv4 Dynamic Stacked VLAN Demux Interfaces over an Aggregated Ethernet Underlying Interface with DHCP Local Server

This example shows how to configure the dynamic creation of IPv4 stacked VLAN demux interfaces with aggregated Ethernet as the underlying interface. DHCP Local Server configuration enables the association of subscribers to the VLAN demux interface by listing the aggregated Ethernet interface in the DHCP local server configuration.



**NOTE:** VLAN demux subscriber interfaces over aggregated Ethernet physical interfaces are supported only for MX Series routers that have only Trio MPCs installed. If the router has other cards in addition to Trio MPCs, the CLI accepts the configuration but errors are reported when the subscriber interfaces are brought up.

To configure dynamic subscribers on dynamic VLAN demux interfaces:

1. Enable VLAN tagging and VLAN auto-configuration on the underlying aggregated Ethernet interface that you plan to use for dynamically created VLAN demux interfaces.

```

interfaces {
  ae1 {
    flexible-vlan-tagging;
    auto-configure {
      stacked-vlan-ranges {
        dynamic-profile auto-vlanDemux-profile {
          accept inet;
          ranges {
            any;
          }
        }
      }
    }
  }
  aggregated-ether-options {
    minimum-links 1;
    lacp {
      active;
      periodic slow;
      link-protection {
        non-revertive;
      }
    }
  }
}

```

2. Define the gigabit Ethernet interfaces that are part of the aggregated Ethernet interface.

```

interfaces {
  ge-5/0/0 {
    giger-options {
      802.3ad ae1;
    }
  }
}

```



```

    }
    ge-5/2/0 {
      gige-ether-options {
        802.3ad ael;
      }
    }
  }
}

```

3. Define the loopback interface.

```

interfaces {
  lo0 {
    unit 0 {
      family inet {
        address 192.16.1.1/32;
      }
    }
  }
}

```

4. Configure a dynamic profile for subscriber access.

```

dynamic-profiles {
  user-profile {
    interfaces {
      "$junos-interface-ifd-name" {
        unit "$junos-underlying-interface-unit" {
          family inet;
        }
      }
    }
  }
}

```

5. Configure a dynamic profile for VLAN demux interface creation.

```

dynamic-profiles {
  auto-vlanDemux-profile {
    interfaces {
      demux0 {
        unit "$junos-interface-unit" {
          vlan-tags outer "$junos-stacked-vlan-id" inner "$junos-vlan-id";
          demux-options {
            underlying-interface "$junos-interface-ifd-name";
          }
          family inet {
            filter {
              input rate_limit;
              output rate_limit;
            }
            unnumbered-address lo0.0 preferred-source-address 192.16.1.1;
          }
        }
      }
    }
  }
}

```

6. Configure the access method used to dynamically create the subscriber interfaces. The following stanza specifies the aggregated Ethernet interface (**ae1.0**) for use with the dynamically created subscriber interfaces.

```
system {
  services {
    dhcp-local-server {
      group myDhcpGroup {
        authentication {
          password test;
          username-include {
            user-prefix igmp-user1;
          }
        }
        dynamic-profile user-profile;
        interface ae1.0;
      }
    }
  }
}
```

Instead of using the aggregated Ethernet interface, you can alternatively specify **demux0** as the device to use with the subscriber interfaces as follows:



**NOTE:** Because the demux interfaces and unit values are created dynamically, the unit number is not specified for the demux0 interface.

```
system {
  services {
    dhcp-local-server {
      group myDhcpGroup {
        authentication {
          password test;
          username-include {
            user-prefix igmp-user1;
          }
        }
        dynamic-profile user-profile;
        interface demux0;
      }
    }
  }
}
```

#### Related Documentation

- Configuring Dynamic Subscriber Interfaces Using VLAN Demux Interfaces in Dynamic Profiles on page 446
- Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125

## Example: Configuring a Static PPPoE Subscriber Interface on a Static Underlying VLAN Demux Interface over Aggregated Ethernet

This example shows how you can configure static PPPoE subscriber interfaces over aggregated Ethernet bundles to provide subscriber link redundancy.

- Requirements on page 509
- Overview on page 509
- Configuration on page 509
- Verification on page 512

### Requirements

PPPoE over VLAN demux interfaces over aggregated Ethernet is supported only on Trio MPCs in MX Series routers.

No special configuration beyond device initialization is required before you can configure this feature.

### Overview

Aggregated Ethernet bundles enable link redundancy between the router and networking devices connected by Ethernet links. This example describes how to configure link redundancy for static PPPoE subscribers over aggregated Ethernet interface with an intermediate static VLAN demux interface. Sample tasks include configuring a two-member aggregated Ethernet bundle on **ae0**, configuring a static VLAN demux interface, **demux0.100**, that underlies the PPPoE subscriber interface, **pp0.100**, and configuring the PPPoE subscriber interface including characteristics of the PPPoE family.

This example does not show all possible configuration choices.

### Configuration

#### CLI Quick Configuration

To quickly configure link redundancy for static PPPoE subscribers over a static VLAN demux interface over aggregated Ethernet, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

```
[edit]
set chassis aggregated-devices ethernet device-count 1
set interfaces ge-5/0/3 gigether-options 802.3ad ae0
set interfaces ge-5/0/3 gigether-options 802.3ad primary
set interfaces ge-5/1/2 gigether-options 802.3ad ae0
set interfaces ge-5/1/2 gigether-options 802.3ad backup
set interfaces ae0 flexible-vlan-tagging
set interfaces ae0 aggregated-ether-options link-protection
edit interfaces demux0 unit 100
set vlan-id 100
set demux-options underlying-interface ae0
set family pppoe access-concentrator pppoe-server-1
set family pppoe duplicate-protection
set family pppoe max-sessions 16000
```

```
top
edit interfaces pp0 unit 100
set pppoe-options underlying-interface demux0.100
set pppoe-options server
set family inet unnumbered-address lo0.0
top
```

**Step-by-Step  
Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure link redundancy for static PPPoE subscribers over a static VLAN demux interface over aggregated Ethernet:

1. Define the number of aggregated Ethernet devices on the router.

```
[edit chassis]
user@host# set aggregated-devices ethernet device-count 1
```

2. Configure a two-link aggregated Ethernet logical interface to serve as the underlying interface for the static VLAN 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 MPC level, the LAG bundle attaches to ports from two different Trio MPCs.

```
[edit interfaces]
user@host# set ge-5/0/3 gigether-options 802.3ad ae0
user@host# set ge-5/0/3 gigether-options 802.3ad primary
user@host# set ge-5/1/2 gigether-options 802.3ad ae0
user@host# set ge-5/1/2 gigether-options 802.3ad backup
```

3. Enable link protection on the aggregated Ethernet logical interface and configure support for single and dual (stacked) VLAN tags.

```
[edit interfaces]
user@host# set ae0 aggregated-ether-options link-protection
user@host# set ae0 flexible-vlan-tagging
```

4. Configure the VLAN demux interface over the aggregated Ethernet logical interface.

```
[edit interfaces]
user@host# set demux0 unit 100 vlan-id 100
user@host# set demux0 unit 100 demux-options underlying-interface ae0
```

5. Configure the PPPoE family attributes on the VLAN demux interface.

```
[edit interfaces]
user@host# set demux0 unit 100 family pppoe access-concentrator pppoe-server-1
user@host# set demux0 unit 100 family pppoe duplicate-protection
user@host# set demux0 unit 100 family pppoe max-sessions 16000
```

6. Configure the VLAN demux interface as the underlying interface on which the PPPoE logical interface is created.

```
[edit interfaces]
user@host# set pp0 unit 100 pppoe-options underlying-interface demux0.100
user@host# set pp0 unit 100 pppoe-options server
user@host# set pp0 unit 100 family inet unnumbered-address lo0.0
```

**Results** From configuration mode, confirm the aggregated device configuration by entering the **show chassis** command. Confirm the interface configuration by entering the **show interfaces** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show chassis
aggregated-devices {
  ethernet {
    device-count 1;
  }
}

[edit]
user@host# show interfaces
ge-5/0/3 {
  gigether-options {
    802.3ad {
      ae0;
      primary;
    }
  }
}
ge-5/1/2 {
  gigether-options {
    802.3ad {
      ae0;
      backup;
    }
  }
}
ae0 {
  flexible-vlan-tagging;
  aggregated-ether-options {
    link-protection;
  }
}
demux0 {
  unit 100 {
    vlan-id 100;
    demux-options {
      underlying-interface ae0;
    }
    family pppoe {
      access-concentrator pppoe-server-1;
      duplicate-protection;
      max-sessions 16000;
    }
  }
}
pp0 {
  unit 100 {
    pppoe-options {
      underlying-interface demux0.100;
      server;
    }
  }
}
```

```

        family inet {
            unnumbered-address lo0.0;
        }
    }
}

```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying the Aggregated Ethernet Interface Configuration on page 512
- Verifying the demux0 Interface Configuration on page 513
- Verifying the pp0 Interface Configuration on page 513

### Verifying the Aggregated Ethernet Interface Configuration

**Purpose** Verify that the interface values match your configuration, the link is up, and traffic is flowing.

**Action** From operational mode, enter the **show interfaces redundancy** command.

```

user@host> show interfaces redundancy
Interface  State           Last change  Primary    Secondary  Current status
ae0        On primary                ge-5/0/3   ge-5/1/2   both up

```

From operational mode, enter the **show interfaces ae0** command.

```

user@host> show interfaces ae0
Physical interface: ae0, Enabled, Physical link is Up
Interface index: 128, SNMP ifIndex: 606
Link-level type: Ethernet, MTU: 1522, Speed: 1Gbps, BPDU Error: None,
MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled,
Flow control: Disabled, Minimum links needed: 1, Minimum bandwidth needed: 0
Device flags   : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Current address: 00:1f:12:b8:ef:c0, Hardware address: 00:1f:12:b8:ef:c0
Last flapped   : 2011-03-11 13:24:18 PST (2d 03:34 ago)
Input rate     : 1984 bps (2 pps)
Output rate    : 0 bps (0 pps)

Logical interface ae0.32767 (Index 69) (SNMP ifIndex 709)
Flags: SNMP-Traps 0x4004000 VLAN-Tag [ 0x0000.0 ] Encapsulation: ENET2
Statistics          Packets      pps          Bytes          bps
Bundle:
  Input :           371259          2       46036116       1984
  Output:              0          0           0           0
Protocol multiservice, MTU: Unlimited
Flags: Is-Primary

```

**Meaning** The **show interfaces redundancy** output shows the redundant link configuration and that both link interfaces are up. The **show interfaces ae0** output shows that the aggregated Ethernet interface is up and that traffic is being received on the logical interface.

### Verifying the demux0 Interface Configuration

**Purpose** Verify that the VLAN demux interface displays the configured PPPoE family attributes and the member links in the aggregated Ethernet bundle.

**Action** From operational mode, enter the **show interfaces demux0** command.

```
user@host> show interfaces demux0.100
Logical interface demux0.100 (Index 76) (SNMP ifIndex 61160)
  Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.100 ]
  Encapsulation: ENET2
  Demux:
    Underlying interface: ae0 (Index 199)
  Link:
    ge-5/0/3
    ge-5/1/2
  Input packets : 2
  Output packets: 18575
  Protocol pppoe
    Dynamic Profile: none,
    Service Name Table: None,
    Max Sessions: 16000, Duplicate Protection: On,
    AC Name: pppoe-server-1
```

Alternatively, you can enter **show pppoe underlying-interfaces detail** to display the state and PPPoE family configuration for all configured underlying interfaces.

**Meaning** The output shows the name of the underlying interface, the member links of the aggregated bundle, and the PPPoE family configuration. The output shows packet counts when traffic is present on the logical interface.

### Verifying the pp0 Interface Configuration

**Purpose** Verify that the interface values match your configuration.

**Action** From operational mode, enter the **show interfaces pp0** command.

```
user@host> show interfaces pp0.100
Logical interface pp0.100 (Index 71) (SNMP ifIndex 710)
  Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPPoE
  PPPoE:
    State: SessionUp, Session ID: 1,
    Session AC name: pppoe-server-1, Remote MAC address: 00:90:1a:00:18:34,
    Underlying interface: demux0.100 (Index 70)
  Link:
    ge-5/0/3.32767
    ge-5/1/2.32767
  Input packets : 18572
  Output packets: 18572
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 0 (never), Output: 18566 (00:00:02 ago)
  LCP state: Opened
  NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured, mpls:
  Not-configured
  CHAP state: Closed
  PAP state: Success
  Protocol inet, MTU: 1500
```

```
Flags: Sendbcst-pkt-to-re  
Addresses, Flags: Is-Primary  
Local: 45.63.24.1
```

**Meaning** This output shows information about the PPPoE logical interface created on the underlying VLAN demux interface. The output includes the PPPoE family and aggregated Ethernet redundant link information, and shows input and output traffic for the PPPoE interface.

**Related Documentation**

- [Subscriber Interfaces and Demultiplexing Overview on page 435](#)
- [Static or Dynamic Demux Subscriber Interfaces over Aggregated Ethernet Overview on page 472](#)
- [Configuring Static Subscriber Interfaces Using VLAN Demux Interfaces on page 441](#)
- [Configuring the PPPoE Family for an Underlying Interface on page 486](#)

---

## Example: Configuring a Dynamic PPPoE Subscriber Interface on a Static Underlying VLAN Demux Interface over Aggregated Ethernet

---

This example shows how you can configure dynamic PPPoE subscriber interfaces over aggregated Ethernet bundles to provide subscriber link redundancy.

- [Requirements on page 514](#)
- [Overview on page 514](#)
- [Configuration on page 515](#)
- [Verification on page 518](#)

### Requirements

PPPoE over VLAN demux interfaces over aggregated Ethernet is supported only on Trio MPCs in MX Series routers.

No special configuration beyond device initialization is required before you can configure this feature.

### Overview

Aggregated Ethernet bundles enable link redundancy between the router and networking devices connected by Ethernet links. This example describes how to configure link redundancy for dynamic PPPoE subscribers over aggregated Ethernet interface, **ae0**, with an intermediate static VLAN demux interface, **demux0.100**. Sample tasks include configuring a two-member aggregated Ethernet bundle, configuring a static VLAN demux interface that underlies the PPPoE subscriber interface, and configuring the dynamic profile that establishes the dynamic PPPoE subscriber interfaces.



The dynamic PPPoE profile (**pppoe-profile**) creates the PPPoE subscriber interface. It also configures the router to act as a PPPoE server and enables the local address to be derived from the specified address without assigning an explicit IP address to the interface. The **pppoe-profile** dynamic profile is assigned to the static, intermediate VLAN demux interface (**demux0.100**), which is configured with the PPPoE family (**family pppoe**) attributes. This dynamic profile includes the following predefined variables:

- **\$junos-interface-unit**—Represents the logical unit number of the dynamic PPPoE logical interface. This predefined variable is dynamically replaced with the unit number supplied by the router when the subscriber logs in.
- **\$junos-underlying-interface**—Represents the name of the underlying Ethernet interface. This predefined variable is dynamically replaced with the interface name supplied by the router when the subscriber logs in.

This example does not show all possible configuration choices.

## Configuration

### CLI Quick Configuration

To quickly configure link redundancy for dynamic PPPoE subscribers over a static VLAN demux interface over aggregated Ethernet, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

```
[edit]
set chassis aggregated-devices ethernet device-count 1
set interfaces ge-5/0/3 gigether-options 802.3ad ae0
set interfaces ge-5/0/3 gigether-options 802.3ad primary
set interfaces ge-5/1/2 gigether-options 802.3ad ae0
set interfaces ge-5/1/2 gigether-options 802.3ad backup
set interfaces ae0 flexible-vlan-tagging
set interfaces ae0 aggregated-ether-options link-protection
set interfaces demux0 unit 100 vlan-id 100
set interfaces demux0 unit 100 demux-options underlying-interface ae0
set interfaces demux0 unit 100 family pppoe access-concentrator pppoe-server-1
set interfaces demux0 unit 100 family pppoe duplicate-protection
set interfaces demux0 unit 100 family pppoe dynamic-profile pppoe-profile
edit dynamic-profiles pppoe-profile
edit interfaces pp0 unit $junos-interface-unit
set pppoe-options underlying-interface $junos-underlying-interface
set pppoe-options server
set family inet unnumbered-address lo0.0
top
```

### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure link redundancy for dynamic PPPoE subscribers over a static VLAN demux interface over aggregated Ethernet:

1. Define the number of aggregated Ethernet devices on the router.

```
[edit chassis]
user@host# set aggregated-devices ethernet device-count 1
```

2. Configure a two-link aggregated Ethernet logical interface to serve as the underlying interface for the static VLAN 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 MPC level, the LAG bundle attaches to ports from two different Trio MPCs.

```
[edit interfaces]
user@host# set ge-5/0/3 gigether-options 802.3ad ae0
user@host# set ge-5/0/3 gigether-options 802.3ad primary
user@host# set ge-5/1/2 gigether-options 802.3ad ae0
user@host# set ge-5/1/2 gigether-options 802.3ad backup
```

3. Enable link protection on the aggregated Ethernet logical interface and configure support for single and dual (stacked) VLAN tags.

```
[edit interfaces]
user@host# set ae0 aggregated-ether-options link-protection
user@host# set ae0 flexible-vlan-tagging
```

4. Configure the VLAN demux interface over the aggregated Ethernet logical interface.

```
[edit interfaces]
user@host# set demux0 unit 100 vlan-id 100
user@host# set demux0 unit 100 demux-options underlying-interface ae0
```

5. Configure the PPPoE family attributes on the VLAN demux interface, including the dynamic profile.

```
[edit interfaces]
user@host# set demux0 unit 100 family pppoe access-concentrator pppoe-server-1
user@host# set demux0 unit 100 family pppoe duplicate-protection
user@host# set demux0 unit 100 family pppoe dynamic-profile pppoe-profile
```

6. Configure the dynamic profile that creates the PPPoE subscriber interfaces.

```
[edit dynamic-profiles pppoe-profile]
user@host# edit interfaces pp0 unit $junos-interface-unit
[edit dynamic-profiles pppoe-profile interfaces pp0 unit "$junos-interface-unit"]
user@host# set pppoe-options underlying-interface $junos-underlying-interface
user@host# set pppoe-options server
user@host# set family inet unnumbered-address lo0.0
```

**Results** From configuration mode, confirm the aggregated device configuration by entering the **show chassis** command. Confirm the interface configuration by entering the **show interfaces** command. Confirm the dynamic profile configuration by entering the **show dynamic-profiles** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show chassis
aggregated-devices {
  ethernet {
    device-count 1;
  }
}

[edit]
user@host# show interfaces
```

```

ge-5/0/3 {
  gether-options {
    802.3ad {
      ae0;
      primary;
    }
  }
}
ge-5/1/2 {
  gether-options {
    802.3ad {
      ae0;
      backup;
    }
  }
}
ae0 {
  flexible-vlan-tagging;
  aggregated-ether-options {
    link-protection;
  }
}
demux0 {
  unit 100 {
    vlan-id 100;
    demux-options {
      underlying-interface ae0;
    }
    family pppoe {
      access-concentrator pppoe-server-1
      duplicate-protection;
      dynamic-profile pppoe-profile;
    }
  }
}
[edit]
user@host# show dynamic-profiles
pppoe-profile {
  interfaces {
    pp0 {
      unit $junos-interface-unit {
        pppoe-options {
          underlying-interface $junos-underlying-interface;
          server;
        }
        family inet {
          unnumbered-address lo0.0;
        }
      }
    }
  }
}

```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying the Aggregated Ethernet Interface Configuration on page 518
- Verifying the demux0 Interface Configuration on page 518

### Verifying the Aggregated Ethernet Interface Configuration

**Purpose** Verify that the interface values match your configuration, the link is up, and traffic is flowing.

**Action** From operational mode, enter the **show interfaces redundancy** command.

```
user@host> show interfaces redundancy
Interface State      Last change Primary      Secondary      Current status
ae0       On primary          ge-5/0/3      ge-5/1/2      both up
```

From operational mode, enter the **show interfaces ae0** command.

```
user@host> show interfaces ae0
Physical interface: ae0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 606
  Link-level type: Ethernet, MTU: 1522, Speed: 1Gbps, BPDU Error: None,
  MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled,
  Flow control: Disabled, Minimum links needed: 1, Minimum bandwidth needed: 0
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Current address: 00:1f:12:b8:ef:c0, Hardware address: 00:1f:12:b8:ef:c0
  Last flapped   : 2011-03-11 13:24:18 PST (2d 03:34 ago)
  Input rate      : 1984 bps (2 pps)
  Output rate     : 0 bps (0 pps)

Logical interface ae0.32767 (Index 69) (SNMP ifIndex 709)
  Flags: SNMP-Traps 0x4004000 VLAN-Tag [ 0x0000.0 ] Encapsulation: ENET2
  Statistics          Packets          pps          Bytes          bps
  Bundle:
    Input :           371259             2        46036116        1984
    Output:              0             0              0           0
  Protocol multiservice, MTU: Unlimited
  Flags: Is-Primary
```

**Meaning** The **show interfaces redundancy** output shows the redundant link configuration and that both link interfaces are up. The **show interfaces ae0** output shows that the aggregated Ethernet interface is up and that traffic is being received on the logical interface.

### Verifying the demux0 Interface Configuration

**Purpose** Verify that the VLAN demux interface displays the configured PPPoE family attributes and the member links in the aggregated Ethernet bundle.

**Action** From operational mode, enter the **show interfaces demux0** command.

```
user@host> show interfaces demux0.100
Logical interface demux0.100 (Index 76) (SNMP ifIndex 61160)
  Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.100 ]
  Encapsulation: ENET2
```

```

Demux:
  Underlying interface: ae0 (Index 199)
Link:
  ge-5/0/3
  ge-5/1/2
Input packets : 2
Output packets: 18575
Protocol pppoe
  Dynamic Profile: pppoe-profile,
  Service Name Table: None,
  Max Sessions: 16000, Duplicate Protection: On,
  AC Name: pppoe-server-1

```

Alternatively, you can enter **show pppoe underlying-interfaces detail** to display the state and PPPoE family configuration for all configured underlying interfaces. The output also provides information about PPPoE negotiation on a per-VLAN basis.

**Meaning** The output shows the name of the underlying interface, the member links of the aggregated bundle, and the PPPoE family configuration. The output shows packet counts when traffic is present on the logical interface.

- Related Documentation**
- Subscriber Interfaces and Demultiplexing Overview on page 435
  - Static or Dynamic Demux Subscriber Interfaces over Aggregated Ethernet Overview on page 472
  - Configuring Dynamic Subscriber Interfaces Using VLAN Demux Interfaces in Dynamic Profiles on page 446
  - Configuring the PPPoE Family for an Underlying Interface on page 486
  - Configuring a Basic PPPoE Dynamic Profile on page 536

## Example: Configuring a Dynamic PPPoE Subscriber Interface on a Dynamic Underlying VLAN Demux Interface over Aggregated Ethernet

This example shows how you can configure dynamic PPPoE subscriber interfaces over aggregated Ethernet bundles to provide subscriber link redundancy.

- Requirements on page 519
- Overview on page 520
- Configuration on page 521
- Verification on page 525

### Requirements

PPPoE over VLAN demux interfaces over aggregated Ethernet is supported only on Trio MPCs in MX Series routers.

No special configuration beyond device initialization is required before you can configure this feature.

## Overview

Aggregated Ethernet bundles enable link redundancy between the router and networking devices connected by Ethernet links. This example describes how to configure link redundancy for dynamic PPPoE subscribers over aggregated Ethernet with an intermediate dynamic VLAN demux interface. Sample tasks include configuring a two-member aggregated Ethernet bundle, configuring dynamic profiles that establish the dynamic VLAN demux interface that underlies the PPPoE subscriber interface, and configuring the dynamic profile that establishes the dynamic PPPoE subscriber interfaces.

In this example, two different dynamic profiles are configured to instantiate either VLAN (**vlan-profile**) or S-VLAN (**svlan-profile**) demux interfaces. These profiles define PPPoE family options and include the dynamic PPPoE profile (**pppoe-profile**) that creates the PPPoE subscriber interface. Junos OS predefined variables are used in each profile to represent the interfaces and VLAN identifiers that are dynamically created. These dynamic profiles include the following predefined variables:

- **\$junos-interface-unit**—Represents the logical unit number of the dynamic VLAN demux interface. This predefined variable is dynamically replaced with the unit number supplied by the router when the subscriber logs in.
- **\$junos-interface-ifd-name**—Represents the underlying logical interface on which the PPPoE subscriber interface is created. This predefined variable is dynamically replaced with the name of the underlying interface supplied by the router when the subscriber logs in.
- **\$junos-vlan-id**—Represents the VLAN identifier. This predefined variable is dynamically replaced with a VLAN ID when the subscriber logs in. The VLAN ID is allocated within the VLAN range specified in the aggregated Ethernet configuration. In the case of the S-VLAN demux, **\$junos-vlan-id** represents the inner VLAN identifier.
- **\$junos-stacked-vlan-id**—Represents the outer VLAN identifier for the stacked VLAN. This predefined variable is dynamically replaced with a VLAN ID when the subscriber logs in. The VLAN ID is allocated within the VLAN range specified in the aggregated Ethernet configuration. This variable is not used for the VLAN demux configuration.

The dynamic PPPoE profile (**pppoe-profile**) creates the PPPoE subscriber interface. It also configures the router to act as a PPPoE server and enables the local address to be derived from the specified address without assigning an explicit IP address to the interface. The **pppoe-profile** dynamic profile is assigned to the dynamic, intermediate VLAN and S-VLAN demux interfaces. This dynamic profile includes the following predefined variables:

- **\$junos-interface-unit**—Represents the logical unit number of the dynamic PPPoE logical interface. This predefined variable is dynamically replaced with the unit number supplied by the router when the subscriber logs in.
- **\$junos-underlying-interface**—Represents the name of the underlying Ethernet interface. This predefined variable is dynamically replaced with the interface name supplied by the router when the subscriber logs in.

This example does not show all possible configuration choices.

## Configuration

**CLI Quick Configuration** To quickly configure link redundancy for dynamic PPPoE subscribers over a dynamic VLAN demux interface over aggregated Ethernet, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

```
[edit]
set chassis aggregated-devices ethernet device-count 1
set interfaces ge-5/0/3 gigether-options 802.3ad ae0
set interfaces ge-5/0/3 gigether-options 802.3ad primary
set interfaces ge-5/1/2 gigether-options 802.3ad ae0
set interfaces ge-5/1/2 gigether-options 802.3ad backup
edit interfaces ae0
set flexible-vlan-tagging
set aggregated-ether-options link-protection
edit auto-configure
set vlan-ranges dynamic-profile vlan-profile accept pppoe
set vlan-ranges dynamic-profile vlan-profile ranges 1-4094
set stacked-vlan-ranges dynamic-profile svlan-profile accept pppoe
set stacked-vlan-ranges dynamic-profile svlan-profile ranges 1-4094,1-4094
top
edit dynamic-profiles pppoe-profile
edit interfaces pp0 unit $junos-interface-unit
set pppoe-options underlying-interface $junos-underlying-interface
set pppoe-options server
set family inet unnumbered-address lo0.0
top
edit dynamic-profiles vlan-profile interfaces demux0
edit unit $junos-interface-unit
set vlan-id $junos-vlan-id
set demux-options underlying-interface $junos-interface-ifd-name
set family pppoe access-concentrator pppoe-server-1
set family pppoe duplicate-protection
set family pppoe dynamic-profile pppoe-profile
top
edit dynamic-profiles svlan-profile interfaces demux0
edit unit $junos-interface-unit
set vlan-tags outer $junos-stacked-vlan-id
set vlan-tags inner $junos-vlan-id
set demux-options underlying-interface $junos-interface-ifd-name
set family pppoe access-concentrator pppoe-server-1
set family pppoe duplicate-protection
set family pppoe dynamic-profile pppoe-profile
top
```

**Step-by-Step Procedure** The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure link redundancy for dynamic PPPoE subscribers over a dynamic VLAN demux interface over aggregated Ethernet:

1. Define the number of aggregated Ethernet devices on the router.

```
[edit chassis]
user@host# set aggregated-devices ethernet device-count 1
```

2. Configure a two-link aggregated Ethernet logical interface to serve as the underlying interface for the dynamic VLAN 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 MPC level, the LAG bundle attaches to ports from two different Trio MPCs.

```
[edit interfaces]
user@host# set ge-5/0/3 gigether-options 802.3ad ae0
user@host# set ge-5/0/3 gigether-options 802.3ad primary
user@host# set ge-5/1/2 gigether-options 802.3ad ae0
user@host# set ge-5/1/2 gigether-options 802.3ad backup
```

3. Enable link protection on the aggregated Ethernet logical interface and configure support for single and dual (stacked) VLAN tags.

```
[edit interfaces]
user@host# set ae0 aggregated-ether-options link-protection
user@host# set ae0 flexible-vlan-tagging
```

4. Configure the parameters for automatically configuring VLANs and S-VLANs, including the VLAN ranges and dynamic profiles.

```
[edit interfaces]
user@host# set ae0 auto-configure vlan-ranges dynamic-profile vlan-profile accept
pppoe
user@host# set ae0 auto-configure vlan-ranges dynamic-profile vlan-profile ranges
1-4094
user@host# set ae0 auto-configure stacked-vlan-ranges dynamic-profile
svlan-profile accept pppoe
user@host# set ae0 auto-configure stacked-vlan-ranges dynamic-profile
svlan-profile ranges 1-4094,1-4094
```

5. Configure the dynamic profile that creates the PPPoE subscriber interface.

```
[edit dynamic-profiles pppoe-profile]
user@host# edit interfaces pp0 unit $junos-interface-unit
[edit dynamic-profiles pppoe-profile interfaces pp0 unit "$junos-interface-unit"]
user@host# set pppoe-options underlying-interface $junos-underlying-interface
user@host# set pppoe-options server
user@host# set family inet unnumbered-address lo0.0
```

6. Configure the dynamic profile that creates VLAN demux underlying interfaces, including the PPPoE family attributes.

```
[edit dynamic-profiles vlan-profile]
user@host# edit interfaces demux0 unit $junos-interface-unit
[edit dynamic-profiles vlan-profile interfaces demux0 unit "$junos-interface-unit"]
user@host# set vlan-id $junos-vlan-id
user@host# set demux-options underlying-interface $junos-interface-ifd-name
user@host# set family pppoe access-concentrator pppoe-server-1
user@host# set family pppoe duplicate-protection
user@host# set family pppoe dynamic-profile pppoe-profile
```

7. Configure the dynamic profile that creates S-VLAN demux underlying interfaces, including the PPPoE family attributes.



```
[edit dynamic-profiles svlan-profile]
user@host# edit interfaces demux0 unit $junos-interface-unit
[edit dynamic-profiles svlan-profile interfaces demux0 unit "$junos-interface-unit"]
user@host# set vlan-tags outer $junos-stacked-vlan-id
user@host# set vlan-tags inner $junos-vlan-id
user@host# set demux-options underlying-interface $junos-interface-ifd-name
user@host# set family pppoe access-concentrator pppoe-server-1
user@host# set family pppoe duplicate-protection
user@host# set family pppoe dynamic-profile pppoe-profile
```

**Results** From configuration mode, confirm the aggregated device configuration by entering the **show chassis** command. Confirm the interface configuration by entering the **show interfaces** command. Confirm the dynamic profile configuration by entering the **show dynamic-profiles** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show chassis
aggregated-devices {
  ethernet {
    device-count 1;
  }
}

[edit]
user@host# show interfaces
ge-5/0/3 {
  gigether-options {
    802.3ad {
      ae0;
      primary;
    }
  }
}
ge-5/1/2 {
  gigether-options {
    802.3ad {
      ae0;
      backup;
    }
  }
}
ae0 {
  flexible-vlan-tagging;
  aggregated-ether-options {
    link-protection;
  }
  auto-configure {
    vlan-ranges {
      dynamic-profile {
        vlan-profile {
          accept pppoe;
          vlan-ranges 1-4094;
        }
      }
    }
  }
}
```

```
}
stacked-vlan-ranges {
  dynamic-profile {
    svlan-profile {
      accept pppoe;
      vlan-ranges 1-4094,1-4094;
    }
  }
}
}
}
}
}
[edit]
user@host# show dynamic-profiles
pppoe-profile {
  interfaces {
    pp0 {
      unit $junos-interface-unit {
        pppoe-options {
          underlying-interface $junos-underlying-interface;
          server;
        }
        family inet {
          unnumbered-address lo0.0;
        }
      }
    }
  }
}
}
}
vlan-profile {
  interfaces {
    demux0 {
      unit "$junos-interface-unit" {
        vlan-id "$junos-vlan-id";
        demux-options {
          underlying-interface "$junos-interface-ifd-name";
        }
        family pppoe {
          access-concentrator pppoe-server-1;
          duplicate-protection;
          dynamic-profile pppoe-profile;
        }
      }
    }
  }
}
}
}
svlan-profile {
  interfaces {
    demux0 {
      unit "$junos-interface-unit" {
        vlan-tags outer "$junos-stacked-vlan-id" inner "$junos-vlan-id";
        demux-options {
          underlying-interface "$junos-interface-ifd-name";
        }
        family pppoe {
          access-concentrator pppoe-server-1;

```

```

        duplicate-protection;
        dynamic-profile pppoe-profile;
    }
}
}
}
}

```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

To confirm that the configuration is working properly, perform this task:

- Verifying the Aggregated Ethernet Interface Configuration on page 525

### Verifying the Aggregated Ethernet Interface Configuration

**Purpose** Verify that the interface values match your configuration, the link is up, and traffic is flowing.

**Action** From operational mode, enter the **show interfaces redundancy** command.

```

user@host> show interfaces redundancy
Interface  State           Last change  Primary    Secondary  Current status
ae0        On primary      ge-5/0/3    ge-5/1/2   both up

```

From operational mode, enter the **show interfaces ae0** command.

```

user@host> show interfaces ae0
Physical interface: ae0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 606
  Link-level type: Ethernet, MTU: 1522, Speed: 1Gbps, BPDU Error: None,
  MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled,
  Flow control: Disabled, Minimum links needed: 1, Minimum bandwidth needed: 0
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Current address: 00:1f:12:b8:ef:c0, Hardware address: 00:1f:12:b8:ef:c0
  Last flapped   : 2011-03-11 13:24:18 PST (2d 03:34 ago)
  Input rate      : 1984 bps (2 pps)
  Output rate     : 0 bps (0 pps)

```

```

Logical interface ae0.32767 (Index 69) (SNMP ifIndex 709)
  Flags: SNMP-Traps 0x4004000 VLAN-Tag [ 0x0000.0 ] Encapsulation: ENET2
  Statistics          Packets      pps      Bytes      bps
  Bundle:
    Input  :          371259          2    46036116    1984
    Output :              0              0           0           0
  Protocol multiservice, MTU: Unlimited
  Flags: Is-Primary

```

**Meaning** The **show interfaces redundancy** output shows the redundant link configuration and that both link interfaces are up. The **show interfaces ae0** output shows that the aggregated Ethernet interface is up and that traffic is being received on the logical interface.

**Related Documentation**

- Subscriber Interfaces and Demultiplexing Overview on page 435

- [Static or Dynamic Demux Subscriber Interfaces over Aggregated Ethernet Overview on page 472](#)
- [Configuring Dynamic Subscriber Interfaces Using VLAN Demux Interfaces in Dynamic Profiles on page 446](#)
- [Configuring the PPPoE Family for an Underlying Interface on page 486](#)
- [Configuring a Basic PPPoE Dynamic Profile on page 536](#)

# Dynamic PPPoE Subscriber Interfaces Overview

- Subscriber Interfaces and PPPoE Overview on page 527
- Dynamic PPPoE Subscriber Interfaces over Static Underlying Interfaces Overview on page 531

## Subscriber Interfaces and PPPoE Overview

---

You can configure the router to dynamically create Point-to-Point Protocol over Ethernet (PPPoE) logical interfaces on statically created underlying Ethernet interfaces. The router automatically and transparently creates the dynamic interface in response to the receipt of a PPPoE Active Discovery Request (PADR) control packet on the underlying interface. Because the router creates a dynamic PPPoE logical interface on demand when a subscriber logs in to the network, dynamic PPPoE logical interfaces are also referred to as *dynamic PPPoE subscriber interfaces*.

To enable the router to create a dynamic PPPoE logical interface on an underlying Ethernet interface, you define the attributes of the PPPoE logical interface in a dynamic profile, and then attach the dynamic profile to an Ethernet interface configured with PPPoE encapsulation. When the router receives a PADR control packet from a PPPoE client on an underlying interface with a PPPoE dynamic profile attached, the router uses the attributes defined in the profile to instantiate a dynamic PPPoE subscriber interface to handle the PPPoE session.

This overview covers the following topics:

- Benefits of Using Dynamic PPPoE Subscriber Interfaces on page 528
- Supported Platforms for Dynamic PPPoE Subscriber Interfaces on page 529
- Sequence of Operations for PPPoE Subscriber Access on page 529

## Benefits of Using Dynamic PPPoE Subscriber Interfaces

Configuring and using dynamic PPPoE subscriber interfaces offers the following benefits:

- On-demand dynamic interface creation

Configuring dynamic PPPoE subscriber interfaces provides the flexibility of dynamically creating the PPPoE subscriber interface only when needed; that is, when a subscriber logs in on the associated underlying Ethernet interface. By contrast, statically created interfaces allocate and consume system resources when the interface is created.

Configuring and using dynamically created interfaces helps you effectively and conveniently manage edge or access networks in which large numbers of subscribers are constantly logging in to and logging out from the network on a transient basis.

- Dynamic removal of PPPoE subscriber interfaces without manual intervention

When the PPPoE subscriber logs out or the PPPoE session is terminated, the router dynamically deletes the associated PPPoE subscriber interface without your intervention, thereby restoring any consumed resources to the router.

- Use of dynamic profiles to efficiently manage multiple subscriber interfaces

A *dynamic profile* is a set of characteristics that can be dynamically assigned to subscriber interfaces. By using a profile, you reduce the management of a large number of interfaces by applying a set of common characteristics to multiple interfaces. When you configure a dynamic profile for PPPoE, you use predefined dynamic variables in the profile to represent information that varies from subscriber to subscriber, such as the logical unit number and underlying interface name. These variables are dynamically replaced with the values supplied by the network when the subscriber logs in.

- Denial of service (DoS) protection

You can optionally configure the underlying Ethernet interface with certain PPPoE-specific attributes that can reduce the potential for DoS attacks. Duplicate protection, which is disabled by default, prevents activation of another dynamic PPPoE logical interface on the underlying interface when a PPPoE logical interface for the same client is already active on the underlying interface. You can also specify the maximum number of PPPoE sessions that the router can activate on the underlying interface. By enabling duplicate protection and restricting the maximum number of PPPoE sessions on the underlying interface, you can ensure that a single toxic PPPoE client cannot monopolize allocation of the PPPoE session.

- Support for dynamic PPPoE subscriber interface creation from PPPoE service name tables

You can assign a previously configured PPPoE dynamic profile to a named, **empty**, or **any** service entry in a PPPoE service name table, or to an agent circuit identifier/agent remote identifier (ACI/ARI) pair defined for these services. The router uses the attributes defined in the profile to instantiate a dynamic PPPoE subscriber interface based on the service name, ACI, and ARI information provided by the PPPoE client during PPPoE negotiation. To specify the routing instance in which to instantiate the dynamic PPPoE subscriber interface, you can assign a previously configured routing instance to a named, **empty**, or **any** service, or to an ACI/ARI pair defined for these services. The dynamic profile and routing instance configured for the PPPoE service name table overrides the

dynamic profile and routing instance assigned to the PPPoE underlying interface on which the dynamic subscriber interface is created.

## Supported Platforms for Dynamic PPPoE Subscriber Interfaces

Configuration of dynamic PPPoE subscriber interfaces over static underlying Ethernet interfaces is supported on the following routing platforms:

- Intelligent Queuing 2 (IQ2) PICs on M120 Multiservice Edge Router and M320 Multiservice Edge Router
- Trio MPC/MIC interfaces on MX Series 3D Universal Edge Routers

## Sequence of Operations for PPPoE Subscriber Access

When a PPPoE subscriber logs in to the network, the PPPoE protocol defines the sequence of operations by which a connection is established and traffic flow is enabled on the dynamic PPPoE subscriber interface. Similarly, when the PPPoE subscriber logs out from the network, PPPoE defines the sequence that occurs to terminate the connection and remove the dynamic PPPoE subscriber interface from the router.

The router creates a dynamic PPPoE subscriber interface for each new PPPoE session, and removes the dynamic PPPoE subscriber interface when the session is terminated due to subscriber logout, PPP negotiation failure, or down status of the underlying Ethernet interface. Dynamic PPPoE subscriber interfaces are never reused for multiple PPPoE sessions.

### Sequence When a PPPoE Subscriber Logs In

---

In a PPPoE subscriber network, the router acts as a *remote access concentrator*, also known as a *PPPoE server*. For a PPPoE client to initiate a PPPoE session with a PPPoE server, it must first perform PPPoE Discovery to identify the Ethernet MAC address of the remote access concentrator that can service its request. Based on the network topology, there may be more than one remote access concentrator with which the client can communicate. The Discovery process enables a PPPoE client to find all remote access concentrators and then select one to connect to.

The following sequence occurs when a PPPoE subscriber logs in to the network. Steps 1 through 5 in this sequence are part of the PPPoE Discovery process.

1. The PPPoE client broadcasts a PPPoE Active Discovery Initiation (PADI) packet to all remote access concentrators in the network.
2. One or more remote access concentrators respond to the PADI packet by sending a PPPoE Active Discovery Offer (PADO) packet, indicating that they can service the client request. The PADO packet includes the name of the access concentrator from which it was sent.
3. The client sends a unicast PPPoE Active Discovery Request (PADR) packet to the access concentrator it selects.

4. On receipt of the PADR packet on the underlying interface associated with a PPPoE dynamic profile, the router uses the attributes configured in the dynamic profile to create the dynamic PPPoE logical interface.
5. The router sends a PPPoE Active Discovery Session (PADS) packet to confirm establishment of the PPPoE connection.
6. The PPP Link Control Protocol (LCP) negotiates the PPP link between the client and the PPPoE server.
7. The subscriber is authenticated using the PPP authentication protocol (CHAP or PAP) configured in the PPPoE dynamic profile.
8. The PPP Network Control Protocol (NCP) negotiates the IP routing protocol and network family.
9. The PPP server issues an IP access address for the client, and the router adds the client access route to its routing table.
10. The router instantiates the dynamic profile and applies the attributes configured in the profile to the dynamic PPPoE subscriber interface.
11. PPP NCP negotiation completes, enabling traffic flow between the PPPoE client and the PPPoE server.

---

#### Sequence When a PPPoE Subscriber Logs Out

The following sequence occurs when a PPPoE subscriber logs out of the network:

1. The client terminates the PPP connection and the router receives an LCP termination request.
2. The router removes the client access router from its routing table.
3. The router sends or receives a PPPoE Active Discovery Termination (PADT) packet to end the PPPoE connection.
4. The router deactivates the subscriber, gathers final statistics for the PPPoE session, and sends the RADIUS server an Acct-Stop accounting message.
5. The router de-instantiates the PPPoE dynamic profile and removes the PPPoE logical interface. The router does not reuse the PPPoE logical interface for future dynamic PPPoE sessions.

#### Related Documentation

- [Dynamic PPPoE Subscriber Interfaces over Static Underlying Interfaces Overview](#) on page 531
- [Configuring Dynamic PPPoE Subscriber Interfaces Using Dynamic Profiles](#) on page 535
- For information about configuring static PPPoE interfaces and PPPoE service name tables, see the [Junos OS Network Interfaces Configuration Guide](#)



## Dynamic PPPoE Subscriber Interfaces over Static Underlying Interfaces Overview

Creating a dynamic PPPoE subscriber interface over a static underlying Ethernet interface consists of two basic steps:

1. Configure a dynamic profile to define the attributes of the PPPoE logical interface.
2. Attach the dynamic profile to a statically created underlying Ethernet interface configured with PPPoE encapsulation.

This overview describes the concepts you need to understand to configure a dynamic PPPoE subscriber interface, and covers the following topics:

- PPPoE Dynamic Profile Configuration on page 531
- PPPoE Underlying Interface Configuration on page 532
- Address Assignment for Dynamic PPPoE Subscriber Interfaces on page 532
- Guidelines for Configuring Dynamic PPPoE Subscriber Interfaces on page 533

### PPPoE Dynamic Profile Configuration

A *dynamic profile* is a template for configuring a dynamic interface. You use predefined dynamic variables in the PPPoE dynamic profile to represent information that varies from subscriber to subscriber, such as the logical unit number and underlying interface name. These variables are dynamically replaced with the values supplied by the network when the subscriber logs in. On receipt of traffic on an underlying Ethernet interface to which a dynamic profile is attached, the router creates the dynamic PPPoE logical interface, also referred to as a *dynamic PPPoE subscriber interface*, on the underlying interface and applies the properties configured in the dynamic profile.

To provide basic access for PPPoE subscribers, the dynamic profile must provide a minimal configuration for a **pp0** (PPPoE) logical interface that includes at least the following attributes:

- The logical unit number, represented by the **\$junos-interface-unit** predefined dynamic variable
- The name of the underlying Ethernet interface, represented by the **\$junos-underlying-interface** predefined dynamic variable
- Configuration of the router to act as a PPPoE server
- The PPP authentication protocol (PAP or CHAP)
- The unnumbered address for the **inet** (IPv4) family

You can also optionally configure additional options for PPPoE subscriber access in the dynamic profile, including:

- The keepalive interval, or the option to disable sending keepalive messages
- The IPv4 address of the dynamic PPPoE logical interface

- The service sets and filters, input filters, and output filters to be applied to the dynamic PPPoE logical interface

## PPPoE Underlying Interface Configuration

After you configure a dynamic profile to define the attributes of a dynamic PPPoE subscriber interface, you must attach the dynamic profile to the underlying Ethernet interface on which you want the router to dynamically create the PPPoE logical interface. The underlying interface for a dynamic PPPoE logical interface must be statically created and configured with PPPoE (**ppp-over-ether**) encapsulation. When a PPPoE subscriber logs in on the underlying interface, the router dynamically creates the PPPoE logical interface and applies the attributes defined in the profile to the interface.

In addition to attaching the dynamic profile to the interface, you can also configure the underlying interface with one or more of the following optional PPPoE-specific attributes:

- Prevention of another dynamic PPPoE logical interface from being activated on the underlying interface when a PPPoE logical interface for a client with the same MAC address is already active on that interface
- Maximum number of dynamic PPPoE logical interfaces (sessions) that the router can activate on the underlying interface
- An alternative access concentrator name in the AC-NAME tag in a PPPoE control packet

## Address Assignment for Dynamic PPPoE Subscriber Interfaces

If the subscriber address for a dynamic PPPoE interface is not specified by means of the Framed-IP-Address (8) or Framed-Pool (88) RADIUS IETF attributes during authentication, the router allocates an IP address from the first IPv4 local address-assignment pool defined in the routing instance. For this reason, make sure that the local address assigned for the **inet** (IPv4) address family is in the same subnet as the addresses obtained from the first IPv4 local address-assignment pool.

The router allocates the IP address from the first IPv4 local address-assignment pool under either of the following conditions:

- RADIUS returns no address attributes.
- RADIUS authentication does not take place because only address allocation is requested.

If the first IPv4 local address-assignment pool has no available addresses, or if no IPv4 local address-assignment pools are configured, the router does not allocate an IP address to the dynamic PPPoE subscriber interface, and denies access to the associated subscriber. To avoid depletion of IP addresses, you can configure linked address-assignment pools on the first IPv4 local address-assignment pool to create one or more backup pools.

For more information, see “Configuring Address-Assignment Pools” on page 68.

## Guidelines for Configuring Dynamic PPPoE Subscriber Interfaces

Observe the following guidelines when you configure dynamic PPPoE subscriber interfaces:

- You can configure dynamic PPPoE subscriber interfaces only for the **inet** (IPv4) protocol family in the current release.
- When you configure the **pp0** (PPPoE) logical interface in a PPPoE dynamic profile, you must include the **pppoe-options** subhierarchy at the **[edit dynamic-profiles profile-name interfaces pp0 unit "\$junos-interface-unit"]** hierarchy level. At a minimum, the **pppoe-options** subhierarchy must include the name of the underlying Ethernet interface, represented by the **\$junos-underlying-interface** predefined dynamic variable, and the **server** statement, which configures the router to act as a PPPoE server. If you omit the **pppoe-options** subhierarchy from the configuration, the **commit** operation fails.
- When you configure CHAP or PAP authentication in a PPPoE dynamic profile, you cannot configure additional options for the **chap** or **pap** statements. This is because the router supports only unidirectional authentication for dynamic interfaces; that is, the router always functions as the authenticator.
- When you attach the PPPoE dynamic profile to an underlying Ethernet interface, ensure that both of the following conditions are met:
  - The PPPoE dynamic profile has already been configured on the router.
  - The underlying Ethernet interface has already been statically configured on the router with PPPoE (**ppp-over-ether**) encapsulation.
- You cannot attach a PPPoE dynamic profile to an underlying Ethernet interface that is already associated with static PPPoE logical interfaces. Conversely, you cannot associate static PPPoE logical interfaces with an underlying Ethernet interface that already has a PPPoE dynamic profile attached.

### Related Documentation

- Subscriber Interfaces and PPPoE Overview on page 527
- Configuring Dynamic PPPoE Subscriber Interfaces Using Dynamic Profiles on page 535
- Example: Configuring a Dynamic PPPoE Subscriber Interface on a Static Gigabit Ethernet VLAN Interface on page 547
- For more information about static PPPoE interfaces, see the [Junos OS Network Interfaces Configuration Guide](#)



# Configuring Dynamic PPPoE Subscriber Interfaces

- Configuring Dynamic PPPoE Subscriber Interfaces Using Dynamic Profiles on page 535
- Configuring a Basic PPPoE Dynamic Profile on page 536
- Configuring a PPPoE Dynamic Profile with Additional Options on page 539
- Configuring an Underlying Interface for Dynamic PPPoE Subscriber Interfaces on page 541
- Assigning a Dynamic Profile and Routing Instance to a Service Name or ACI/ARI Pair for Dynamic PPPoE Interface Creation on page 543
- Verifying and Managing Dynamic PPPoE Configuration on page 544

## Configuring Dynamic PPPoE Subscriber Interfaces Using Dynamic Profiles

---

You can configure dynamic PPP-over-Ethernet (PPPoE) subscriber interfaces by using dynamic profiles. To enable the router to create a dynamic PPPoE subscriber interface on a PPPoE underlying interface, you define the attributes of the PPPoE logical interface in a dynamic profile, and then configure the underlying interface to use the dynamic profile.

To configure a dynamic PPPoE subscriber interface:

1. Configure a dynamic profile to define the attributes of the PPPoE logical interface.
  - To configure a basic dynamic profile for PPPoE subscriber access, see “Configuring a Basic PPPoE Dynamic Profile” on page 536.
  - To configure a dynamic profile for PPPoE with additional options for subscriber access, see “Configuring a PPPoE Dynamic Profile with Additional Options” on page 539.
2. Configure the underlying Ethernet interface to use the dynamic profile for PPPoE.

See “Configuring an Underlying Interface for Dynamic PPPoE Subscriber Interfaces” on page 541.
3. (Optional) Assign a dynamic profile and routing instance to a service name or ACI/ARI pair in a PPPoE service name table to instantiate a dynamic PPPoE subscriber interface based on the information provided by the PPPoE client.

See “Assigning a Dynamic Profile and Routing Instance to a Service Name or ACI/ARI Pair for Dynamic PPPoE Interface Creation” on page 543.

4. (Optional) Verify the dynamic PPPoE configuration by displaying or clearing PPPoE session statistics, and displaying information about the underlying Ethernet interface and PPPoE logical interface.

See “Verifying and Managing Dynamic PPPoE Configuration” on page 544.

**Related  
Documentation**

- Subscriber Interfaces and PPPoE Overview on page 527
- Dynamic PPPoE Subscriber Interfaces over Static Underlying Interfaces Overview on page 531
- Example: Configuring a Dynamic PPPoE Subscriber Interface on a Static Gigabit Ethernet VLAN Interface on page 547
- Example: Configuring a PPPoE Service Name Table for Dynamic Subscriber Interface Creation on page 549

---

## Configuring a Basic PPPoE Dynamic Profile

You can configure a basic dynamic profile for PPPoE subscribers that access the network. The dynamic profile defines the attributes of the dynamic PPPoE logical interface, also referred to as a *dynamic PPPoE subscriber interface*.

To provide basic access for PPPoE subscribers, the dynamic profile must provide a minimal configuration for a **pp0** (PPPoE) logical interface that includes the following:

- The logical unit number, represented by the **\$junos-interface-unit** predefined dynamic variable
- The name of the underlying Ethernet interface, represented by the **\$junos-underlying-interface** predefined dynamic variable
- The **server** statement, which configures the router to act as a PPPoE server
- The PPP authentication protocol (PAP or CHAP)
- The unnumbered address for the **inet** (IPv4) family

To configure a basic PPPoE dynamic profile:

1. Name the dynamic profile.

```
[edit]
user@host# edit dynamic-profiles basic-pppoe-profile
```

2. Specify that you want to configure the **pp0** logical interface in the dynamic profile.

```
[edit dynamic-profiles basic-pppoe-profile]
user@host# edit interfaces pp0
```

3. Configure the predefined variable to represent the logical unit number for the **pp0** interface.

You must use the **\$junos-interface-unit** variable instead of the logical unit number for the **unit** statement. The **\$junos-interface-unit** variable is dynamically replaced with the actual unit number supplied by the network when the subscriber logs in.

```
[edit dynamic-profiles basic-pppoe-profile interfaces pp0]
user@host# edit unit $junos-interface-unit
```

4. Configure PPPoE-specific options for the **pp0** interface.

- a. Configure the predefined variable to represent the name of the underlying Ethernet interface on which the router creates the dynamic PPPoE logical interface.

You must use the **\$junos-underlying-interface** variable instead of the underlying interface name for the **underlying-interface** statement. The **\$junos-underlying-interface** variable is dynamically replaced with the actual name of the underlying interface supplied by the network when the subscriber logs in.

```
[edit dynamic-profiles basic-pppoe-profile interfaces pp0 unit
"$junos-interface-unit"]
user@host# set pppoe-options underlying-interface $junos-underlying-interface
```

- b. Configure the router to act as a PPPoE server, also known as a remote access concentrator.

```
[edit dynamic-profiles basic-pppoe-profile interfaces pp0 unit
"$junos-interface-unit"]
user@host# set pppoe-options server
```

5. Configure the PPP authentication protocol for the **pp0** interface.

For dynamic interfaces, the router supports only unidirectional authentication; that is, the router always functions as the authenticator. When you configure PPP authentication in a dynamic profile, the **chap** and **pap** statements do not support any additional configuration options.

- To configure CHAP authentication:

```
[edit dynamic-profiles basic-pppoe-profile interfaces pp0 unit "$junos-interface-unit"]
user@host# set ppp-options chap
```

- To configure PAP authentication:

```
[edit dynamic-profiles basic-pppoe-profile interfaces pp0 unit "$junos-interface-unit"]
user@host# set ppp-options pap
```

6. Configure the family for the **pp0** interface.

- a. Specify that you want to configure the **inet** (IPv4) family.



**NOTE:** The creation of dynamic PPPoE subscriber interfaces is currently supported only for the **inet** family.

```
[edit dynamic-profiles basic-pppoe-profile interfaces pp0 unit
"$junos-interface-unit"]
user@host# edit family inet
```

- b. Configure the unnumbered address for the family.

```
[edit dynamic-profiles basic-pppoe-profile interfaces pp0 unit "$junos-interface-unit"  
family inet]  
user@host# set unnumbered-address lo0.0
```

**Related  
Documentation**

- [Subscriber Interfaces and PPPoE Overview on page 527](#)
- [Dynamic PPPoE Subscriber Interfaces over Static Underlying Interfaces Overview on page 531](#)
- [Configuring an Underlying Interface for Dynamic PPPoE Subscriber Interfaces on page 541](#)
- [Example: Configuring a Dynamic PPPoE Subscriber Interface on a Static Gigabit Ethernet VLAN Interface on page 547](#)
- [Verifying and Managing Dynamic PPPoE Configuration on page 544](#)



## Configuring a PPPoE Dynamic Profile with Additional Options

You can configure a dynamic profile for PPPoE that has additional options for subscriber access. All of these optional statements, with the exception of the **keepalives** and **no-keepalives** statements, are configured at the **[edit dynamic-profiles *profile-name* interfaces pp0 unit “\$junos-interface-unit” family inet]** hierarchy level. The **keepalives** and **no-keepalives** statements are configured at the **[edit dynamic-profiles *profile-name* interfaces pp0 unit “\$junos-interface-unit”]** hierarchy level.

The additional options for PPPoE subscriber access in a dynamic profile can include one or more of the following:

- The keepalive interval (**keepalives**), or the option to disable sending keepalive messages (**no-keepalives**)
- The IPv4 address of the dynamic PPPoE logical interface (**address**)
- Definition of the service sets and filters to be applied to the dynamic PPPoE logical interface, configured at the **[edit dynamic-profiles *profile-name* interfaces pp0 unit “\$junos-interface-unit” family inet service]** hierarchy level
- Association of an input and output filter to the dynamic PPPoE logical interface, configured at the **[edit dynamic-profiles *profile-name* interfaces pp0 unit “\$junos-interface-unit” family inet filter]** hierarchy level

Before you begin:

- Configure a basic PPPoE dynamic profile.

See “Configuring a Basic PPPoE Dynamic Profile” on page 536.

To configure a PPPoE dynamic profile with additional options for subscriber access:

1. Modify the keepalive interval, or configure the router to disable sending keepalive messages.
  - To modify the keepalive interval:
 

```
[edit dynamic-profiles business-pppoe-profile interfaces pp0 unit
"$junos-interface-unit"]
user@host# set keepalives interval 15
```
  - To disable sending keepalive messages:
 

```
[edit dynamic-profiles business-pppoe-profile interfaces pp0 unit
"$junos-interface-unit"]
user@host# set no-keepalives
```
2. Specify that you want to configure the **inet** (IPv4) family.



**NOTE:** The creation of dynamic PPPoE subscriber interfaces is currently supported only for the **inet** family.

```
[edit dynamic-profiles business-pppoe-profile interfaces pp0 unit
"$junos-interface-unit"]
user@host# edit family inet
```

3. Specify the IPv4 address of the dynamic PPPoE logical interface.

```
[edit dynamic-profiles business-pppoe-profile interfaces pp0 unit
"$junos-interface-unit" family inet]
user@host# set address 6.6.6.7/32
```

4. Specify the input and output service sets that you want to apply to the dynamic PPPoE logical interface.

```
[edit dynamic-profiles business-pppoe-profile interfaces pp0 unit
"$junos-interface-unit" family inet]
user@host# set service input service-set inputService_100
user@host# set service input post-service-filter postService_20
user@host# set service output service-set outputService_200
```

5. Specify the input and output filters that you want to apply to the dynamic PPPoE logical interface.

To control the order in which filters are processed, you can optionally specify a precedence value for the input filter, output filter, or both.

```
[edit dynamic-profiles business-pppoe-profile interfaces pp0 unit
"$junos-interface-unit" family inet]
user@host# set filter input pppoe-input-filter
user@host# set filter output pppoe-output-filter precedence 50
```

#### **Related Documentation**

- Subscriber Interfaces and PPPoE Overview on page 527
- Dynamic PPPoE Subscriber Interfaces over Static Underlying Interfaces Overview on page 531
- Configuring a Basic PPPoE Dynamic Profile on page 536
- Configuring an Underlying Interface for Dynamic PPPoE Subscriber Interfaces on page 541
- Example: Configuring a Dynamic PPPoE Subscriber Interface on a Static Gigabit Ethernet VLAN Interface on page 547
- Verifying and Managing Dynamic PPPoE Configuration on page 544
- Dynamic Service Sets Overview on page 569
- Associating Service Sets with Interfaces in a Dynamic Profile on page 595
- Dynamic Firewall Filters Overview on page 555
- Dynamically Attaching Statically Created Filters for a Specific Interface Family Type on page 571

## Configuring an Underlying Interface for Dynamic PPPoE Subscriber Interfaces

After you configure a dynamic profile to define the attributes of a dynamic PPPoE subscriber interface, you must attach the dynamic profile to a statically created underlying Ethernet interface configured with PPPoE (**ppp-over-ether**) encapsulation. You configure the underlying interface at the **[edit interfaces *interface-name* unit *logical-unit-number* pppoe-underlying-options]** hierarchy level.

In addition to attaching the dynamic profile to the interface by using the required **dynamic-profile** statement, you can also configure the underlying interface with one or more of the following optional PPPoE-specific attributes:

- Prevention of another dynamic PPPoE logical interface from being activated on the underlying interface when a PPPoE logical interface for a client with the same MAC address is already active on that interface (**duplicate-protection**)
- Maximum number of dynamic PPPoE logical interfaces (sessions) that the router can activate on the underlying interface (**max-sessions**)
- An alternative access concentrator name in the AC-NAME tag in a PPPoE control packet (**access-concentrator**)

Before you begin:

1. Configure the static underlying Ethernet interface on which you want the router to dynamically create the PPPoE logical interface.

For information about configuring static Ethernet interfaces, see the [Junos OS Network Interfaces Configuration Guide](#).

2. Configure a PPPoE dynamic profile in either of the following ways:
  - To configure a basic PPPoE dynamic profile, see “Configuring a Basic PPPoE Dynamic Profile” on page 536.
  - To configure a PPPoE dynamic profile with additional options for subscriber access, see “Configuring a PPPoE Dynamic Profile with Additional Options” on page 539.

To configure an underlying Ethernet interface for a dynamic PPPoE subscriber interface:

1. Specify the name and logical unit number of the static underlying Ethernet interface to which you want to attach the PPPoE dynamic profile.

```
[edit]
user@host# edit interfaces ge-1/0/1 unit 0
```

2. Configure PPPoE encapsulation on the underlying interface.

```
[edit interfaces ge-1/0/1 unit 0]
user@host# set encapsulation ppp-over-ether
```

3. Specify that you want to configure PPPoE-specific options on the underlying interface.

```
[edit interfaces ge-1/0/1 unit 0]
user@host# edit pppoe-underlying-options
```

4. Attach a previously configured PPPoE dynamic profile to the underlying interface.

The specified PPPoE dynamic profile must already be configured on the router. In addition, you cannot attach a PPPoE dynamic profile to an underlying Ethernet interface that is already associated with static PPPoE logical interfaces. Conversely, you cannot associate static PPPoE logical interfaces with an underlying Ethernet interface that already has a PPPoE dynamic profile attached.

```
[edit interfaces ge-1/0/1 unit 0 pppoe-underlying-options]  
user@host# set dynamic-profile basic-pppoe-profile
```

5. (Optional) Enable duplicate protection to prevent activation of another dynamic PPPoE logical interface for the same client on the underlying interface.

```
[edit interfaces ge-1/0/1 unit 0 pppoe-underlying-options]  
user@host# set duplicate-protection
```

6. (Optional) Specify the maximum number of dynamic PPPoE sessions that the router can activate on the underlying interface, from 1 to the maximum number of PPPoE sessions supported on your routing platform.

```
[edit interfaces ge-1/0/1 unit 0 pppoe-underlying-options]  
user@host# set max-sessions 20
```

7. (Optional) Specify the alternative name for the access concentrator, also known as the PPPoE server.

```
[edit interfaces ge-1/0/1 unit 0 pppoe-underlying-options]  
user@host# set access-concentrator server-east
```

#### **Related Documentation**

- [Subscriber Interfaces and PPPoE Overview on page 527](#)
- [Dynamic PPPoE Subscriber Interfaces over Static Underlying Interfaces Overview on page 531](#)
- [Configuring a Basic PPPoE Dynamic Profile on page 536](#)
- [Configuring a PPPoE Dynamic Profile with Additional Options on page 539](#)
- [Example: Configuring a Dynamic PPPoE Subscriber Interface on a Static Gigabit Ethernet VLAN Interface on page 547](#)
- [Verifying and Managing Dynamic PPPoE Configuration on page 544](#)
- For information about configuring static Ethernet underlying interfaces, see the [Junos OS Network Interfaces Configuration Guide](#)

## Assigning a Dynamic Profile and Routing Instance to a Service Name or ACI/ARI Pair for Dynamic PPPoE Interface Creation

You can create a dynamic PPPoE subscriber interface based on the service name, agent circuit identifier (ACI), and agent remote identifier (ARI) information provided by the PPPoE client during PPPoE negotiation. To do so, you assign a previously configured PPPoE dynamic profile to a named service, **empty** service, or **any** service entry in a PPPoE service name table, or to an ACI/ARI pair defined for these services.

Similarly, to specify the routing instance in which to instantiate the dynamic PPPoE subscriber interface, you can assign a previously configured routing instance to a named service, **empty** service, or **any** service in a PPPoE service name table, or to an ACI/ARI pair defined for these services.

Observe the following configuration guidelines when you assign a dynamic profile and routing instance to a PPPoE service name table to create a dynamic PPPoE subscriber interface:

- The dynamic profile and routing instance must already be configured on the router.
- The dynamic profile or routing instance assigned to the PPPoE service name table overrides the dynamic profile or routing instance assigned to the PPPoE underlying interface on which the dynamic subscriber interface is created.
- You cannot configure a dynamic profile or routing instance for an ACI/ARI pair already configured with a static interface (by using the **static-interface** statement). Conversely, you cannot configure a static interface for an ACI/ARI pair already configured with a dynamic profile or routing instance.

Before you begin:

1. Configure a PPPoE dynamic profile in either of the following ways:
  - To configure a basic PPPoE dynamic profile, see “Configuring a Basic PPPoE Dynamic Profile” on page 536.
  - To configure a PPPoE dynamic profile with additional options for subscriber access, see “Configuring a PPPoE Dynamic Profile with Additional Options” on page 539.
2. Configure the routing instance in which you want the router to instantiate the dynamic profile.

For information about configuring routing instances, see the [Junos OS Routing Protocols Configuration Guide](#).

3. Create the PPPoE service name table on the router.

See Creating a Service Name Table in the [Junos OS Network Interfaces Configuration Guide](#).

To create a dynamic PPPoE subscriber interface based on the service name and, optionally, associated ACI/ARI pair configured in a PPPoE service name table, do one of the following:

- Assign a previously configured dynamic profile and routing instance to a named, **empty**, or **any** service.

```
[edit protocols pppoe service-name-tables table1]
user@host# set service premium dynamic-profile premiumProfile routing-instance
premiumRI
```

- Assign a previously configured dynamic profile and routing instance to the ACI/ARI pair defined for a named, **empty**, or **any** service.

```
[edit protocols pppoe service-name-tables table1]
user@host# set service any agent-specifier aci west-ge-3/0/3 ari sunnyvale
dynamic-profile standardProfile routing-instance standardRI
```

**Related  
Documentation**

- Example: Configuring a PPPoE Service Name Table for Dynamic Subscriber Interface Creation on page 549
- Subscriber Interfaces and PPPoE Overview on page 527
- Configuring Dynamic PPPoE Subscriber Interfaces Using Dynamic Profiles on page 535
- Configuring PPPoE Service Name Tables

---

## Verifying and Managing Dynamic PPPoE Configuration

---

**Purpose** View or clear information about dynamic PPPoE logical interfaces, underlying interfaces for dynamic PPPoE logical interfaces, and PPPoE statistics

- Action**
- To display information about the properties of all PPPoE underlying interfaces associated with a dynamic PPPoE profile:  

```
user@host> show pppoe underlying-interfaces
```
  - To display information about the PPPoE properties of a specified underlying interface associated with a dynamic PPPoE profile:  

```
user@host> show pppoe underlying-interfaces interface-name
```
  - To display session-specific information about PPPoE interfaces, including whether the interface was dynamically created or statically created:  

```
user@host> show pppoe interfaces
```
  - To display information for a specified PPPoE service name table, including the assigned dynamic profile and routing instance, if configured:  

```
user@ host> show pppoe service-name-tables table-name
```
  - To display information about all active PPPoE sessions on the router:  

```
user@host > show pppoe sessions
```
  - To display information for all active PPPoE sessions established for a specified service name:

user@host > **show pppoe sessions service *service-name***

- To display information for all active PPPoE sessions established for a specified agent circuit identifier (ACI) or agent remote identifier (ARI) string:

user@host > **show pppoe sessions aci "west-ge-2/0/3"**

user@host > **show pppoe sessions ari "sunnyvale"**

- To display PPPoE control packet statistics for all PPPoE sessions:

user@host> **show pppoe statistics**

- To display PPPoE control packet statistics for a specified PPPoE underlying interface:

user@host> **show pppoe statistics *interface-name***

- To clear (reset) PPPoE control packet statistics for all PPPoE sessions:

user@host> **clear pppoe statistics**

- To clear (reset) PPPoE control packet statistics for a specified underlying Ethernet interface:

user@host> **clear pppoe statistics *underlying-interface-name***

**Related  
Documentation**

- [Junos OS Interfaces Command Reference](#)





# Dynamic PPPoE Subscriber Interfaces Examples

- Example: Configuring a Dynamic PPPoE Subscriber Interface on a Static Gigabit Ethernet VLAN Interface on page 547
- Example: Configuring a PPPoE Service Name Table for Dynamic Subscriber Interface Creation on page 549
- Evaluation Order for Matching Client Information in PPPoE Service Name Tables on page 552

## Example: Configuring a Dynamic PPPoE Subscriber Interface on a Static Gigabit Ethernet VLAN Interface

---

This example shows how to configure a dynamic PPPoE subscriber interface on a statically configured Gigabit Ethernet VLAN underlying interface. When a PPPoE subscriber logs in on the underlying interface, the router creates the dynamic PPPoE subscriber interface with the attributes specified in the dynamic profile.

In this example, the dynamic PPPoE profile, **pppoe-profile-east**, defines options for PPPoE subscribers accessing the network, and includes the predefined dynamic variables **\$junos-interface-unit**, which represents the logical unit number of the dynamic PPPoE logical interface, and **\$junos-underlying-interface**, which represents the name of the underlying Ethernet interface. The **pppoe-profile-east** dynamic profile is assigned to the underlying Ethernet VLAN interface **ge-2/0/3.1** that is configured with PPPoE (**ppp-over-ether**) encapsulation.

When the router dynamically creates the PPPoE subscriber interface on **ge-2/0/3.1** in response to a subscriber login, the values of **\$junos-interface-unit** and **\$junos-underlying-interface** are dynamically replaced with the actual logical unit number and interface name, respectively, that are supplied by the network when the PPPoE subscriber logs in.

To configure a dynamic PPPoE subscriber interface:

1. Configure a dynamic profile to define the attributes of the dynamic PPPoE subscriber interface.

```
[edit]
dynamic-profiles {
```

```
pppoe-profile-east {
  interfaces {
    pp0 {
      unit "$junos-interface-unit" {
        ppp-options {
          chap;
        }
        pppoe-options {
          underlying-interface "$junos-underlying-interface";
          server;
        }
        keepalives interval 30;
        family inet {
          filter {
            input pppoe-input-filter-east;
            output pppoe-output-filter-east precedence 20;
          }
          service {
            input {
              service-set inputService-east;
              post-service-filter postService-east;
            }
            output {
              service-set outputService-east;
            }
          }
          address 6.6.6.1/32;
          unnumbered-address lo0.0;
        }
      }
    }
  }
}
```

2. Assign the dynamic PPPoE profile to the static underlying Ethernet interface, and define PPPoE-specific attributes for the underlying interface.

```
[edit]
interfaces {
  ge-2/0/3 {
    vlan-tagging;
    unit 1 {
      encapsulation ppp-over-ether;
      vlan-id 100;
      pppoe-underlying-options {
        access-concentrator server-east;
        duplicate-protection;
        dynamic-profile pppoe-profile-east;
        max-sessions 10;
      }
    }
  }
}
```

- Related Documentation**
- Subscriber Interfaces and PPPoE Overview on page 527
  - Dynamic PPPoE Subscriber Interfaces over Static Underlying Interfaces Overview on page 531
  - Configuring a PPPoE Dynamic Profile with Additional Options on page 539
  - Configuring an Underlying Interface for Dynamic PPPoE Subscriber Interfaces on page 541

## Example: Configuring a PPPoE Service Name Table for Dynamic Subscriber Interface Creation

This example shows how to configure a PPPoE service name table to create a dynamic PPPoE subscriber interface based on the service name, agent circuit identifier (ACI), and agent remote identifier (ARI) information provided by PPPoE clients during PPPoE negotiation.

In this example, PPPoE service name table **TableDynamicPPPoE** includes an **any** service entry, **empty** service entry, and two named service entries: **Premium** and **Standard**. The PPPoE underlying interfaces configured for **TableDynamicPPPoE** are **ge-2/0/0.1** and **ge-2/0/0.2**. Only **ge-2/0/0.1** is configured for dynamic profile assignment and creation of dynamic PPPoE subscriber interfaces.

Following the configuration example, Table 49 on page 551 explains how the router evaluates the entries in **TableDynamicPPPoE** to create a dynamic PPPoE subscriber interface in a specified routing instance for each of several sample clients.

To configure a PPPoE service name table to create dynamic PPPoE subscriber interfaces:

1. Configure the PPPoE service name table.

```
protocols {
  pppoe {
    service-name-tables TableDynamicPPPoE {
      service any {
        terminate;
        max-sessions 100;
        dynamic-profile AnyProfile;
        agent-specifier {
          aci "broadway-ge-1/0/1.0" ari "london" {
            terminate;
            dynamic-profile LondonProfile;
            routing-instance LondonRI;
          }
          aci "groton-ge-4/0/3.32" ari "paris" {
            delay 5;
            dynamic-profile ParisProfile;
            routing-instance ParisRI;
          }
        }
      }
      service empty {
        drop;
      }
    }
  }
}
```

```

        agent-specifier {
            aci "dunstable-ge-1/0/0.1" ari "kanata" {
                dynamic-profile BasicPppoeProfile;
                delay 10;
            }
        }
    }
    service Premium {
        terminate;
        dynamic-profile PremiumProfile;
    }
    service Standard {
        terminate;
        max-sessions 10;
        dynamic-profile StandardProfile;
        agent-specifier {
            aci "dunstable-ge-1/0/0.1" ari "kanata" {
                dynamic-profile BasicPppoeProfile;
                delay 10;
            }
        }
    }
}

```

2. Configure the PPPoE underlying interface for the service name table.

```

interfaces {
    ge-2/0/0 {
        vlan-tagging;
        unit 1 {
            vlan-id 1;
            pppoe-underlying-options {
                dynamic-profile BasicPppoeProfile;
                service-name-table TableDynamicPPPoE;
            }
        }
        unit 2 {
            vlan-id 2;
            pppoe-underlying-options {
                service-name-table TableDynamicPPPoE;
            }
        }
    }
}

```

Table 49 on page 551 lists the service name, ACI value, and ARI value provided in several sample PPPoE client requests, and the name of the PPPoE underlying interface on which the router received each client request. The Results column describes the dynamic PPPoE subscriber interface created by the router based on *both* of the following:

- The values received from each PPPoE client during PPPoE negotiation
- The sequence in which the router evaluates the entries configured in the PPPoE service name table to find a match for the client's service name and ACI/ARI information, as

described in “Evaluation Order for Matching Client Information in PPPoE Service Name Tables” on page 552

**Table 49: Dynamic PPPoE Subscriber Interface Creation Based on PPPoE Client Request Values**

PPPoE Client	Service Name	ACI Value	ARI Value	Receiving Underlying Interface	Results
Client 1	Premium	broadway-ge-1/0/1.1	london	ge-2/0/0.1	Matches ACI/ARI pair configured for <b>any</b> service. Router creates dynamic PPPoE subscriber interface over <b>ge-2/0/0.1</b> using <b>LondonProfile</b> dynamic profile and <b>LondonRI</b> routing instance assigned to <b>any</b> service.
Client 2	Premium	dunstable-ge-1/0/1.0	toronto	ge-2/0/0.1	Matches base <b>Premium</b> service. Router creates dynamic PPPoE subscriber interface over <b>ge-2/0/0.1</b> using <b>PremiumProfile</b> dynamic profile and routing instance associated with <b>ge-2/0/0.1</b> underlying interface.
Client 3	empty	dunstable-ge-1/0/0.1	kanata	ge-2/0/0.1	Matches ACI/ARI pair configured for <b>empty</b> service and <b>Standard</b> service. Router creates dynamic PPPoE subscriber interface over <b>ge-2/0/0.1</b> after a delay of 10 seconds if no other PPPoE server responds to the client request within that time. Router uses <b>BasicPPPoEProfile</b> dynamic profile and routing instance associated with <b>ge-2/0/0.1</b> underlying interface.
Client 4	empty	slinger-ge-1/0/0.1	chicago	ge-2/0/0.2	Because receiving underlying interface <b>ge-2/0/0.2</b> is <i>not</i> associated with a dynamic profile, router does not create a dynamic PPPoE subscriber interface, and drops any PADI or PADR control packets received from this client.
Client 5	Standard	slinger-ge-1/0/0.1	chicago	ge-2/0/0.1	Matches base <b>Standard</b> service. Router creates dynamic PPPoE subscriber interface over <b>ge-2/0/0.1</b> using <b>StandardProfile</b> dynamic profile and routing instance associated with <b>ge-2/0/0.1</b> underlying interface.

**Related Documentation**

- Evaluation Order for Matching Client Information in PPPoE Service Name Tables on page 552
- Subscriber Interfaces and PPPoE Overview on page 527

- Understanding PPPoE Service Name Tables
- Configuring PPPoE Service Name Tables

## Evaluation Order for Matching Client Information in PPPoE Service Name Tables

---

When the router receives a service request from a PPPoE client, it evaluates the entries configured in the PPPoE service name table to find a match for the client's ACI/ARI information so it can take the appropriate action.

The order of evaluation is as follows:

1. The router evaluates the ACI/ARI information configured for the **any** service entry, and ignores the contents of the service name tag transmitted by the client.
2. If no match is found for the client information, the router evaluates the ACI/ARI information for the **empty** service entry and the named service entries. If an ACI/ARI pair is not configured for these service entries, the router evaluates the other attributes configured for the **empty** service and named services.
3. If there is still no match for the client information, the router evaluates the other attributes configured for the **any** service entry, and ignores both the ACI/ARI information for the **any** service and the contents of the service name tag transmitted by the client. If the **any** service is configured for the default action, **drop**, the router drops the PADR packet. If the **any** service is configured for a nondefault action (**terminate** or **delay**), the router evaluates the other attributes configured for the **any** service.

### Related Documentation

- Understanding PPPoE Service Name Tables
- Benefits of Configuring PPPoE Service Name Tables
- Configuring PPPoE Service Name Tables
- Example: Configuring a PPPoE Service Name Table for Dynamic Subscriber Interface Creation on page 549

## PART 12

# Dynamic Firewall Filters, Service Sets and HTTP Redirect for Subscriber Access

- [Dynamic Firewall Filters and Service Sets Overview on page 555](#)
- [Configuring Filters for Dynamic Profiles on page 571](#)
- [Configuring Fast Update Filters on page 581](#)
- [Configuring Service Sets in Dynamic Profiles on page 595](#)
- [Firewall Filter Examples on page 597](#)
- [Redirecting HTTP Requests Overview on page 613](#)
- [Configuring HTTP Redirect on page 615](#)
- [HTTP Redirect Examples on page 619](#)





# Dynamic Firewall Filters and Service Sets Overview

- Dynamic Firewall Filters Overview on page 555
- Classic Filters Overview on page 556
- Basic Classic Filter Syntax on page 558
- Ascend-Data-Filter Policies for Subscriber Management Overview on page 559
- Ascend-Data-Filter Attribute Fields on page 561
- Fast Update Filters Overview on page 564
- Basic Fast Update Filter Syntax on page 567
- Match Conditions and Actions in Fast Update Filters on page 568
- Dynamic Service Sets Overview on page 569

## Dynamic Firewall Filters Overview

---

Firewall filters provide rules that define whether to accept or reject packets that are transiting an interface on a router. The subscriber management feature supports two categories of firewall filters—classic filters and fast update filters.

- Classic filters are compiled at commit time and then, when a service is activated, an interface-specific clone of the filter is created and attached to a logical interface. Classic filters are static filters; they cannot contain subscriber-specific terms (also called rules). Fast update filters are similar to classic filters in many ways. However, fast update filters support subscriber-specific, rather than interface-specific, filter values.
- Fast update filters also allow individual filter terms to be incrementally added or removed from filters without requiring that the entire filter be recompiled for each modification. Fast update filters are essential for networking environments in which multiple subscribers might share the same logical interface

You configure firewall filters to determine whether to accept or reject traffic before it enters or exits an interface to which the firewall filter is applied. An *input* (or *ingress*) firewall filter is applied to packets that are entering a network. An *output* (or *egress*) firewall filter 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 with a dynamic profile. When triggered, a dynamic profile can apply a named filter or a filter specified in RADIUS to an interface.

**Related Documentation**

- Classic Filters Overview on page 556
- Fast Update Filters Overview on page 564
- Dynamically Attaching Statically Created Filters for Any Interface Type on page 572
- Dynamically Attaching Statically Created Filters for a Specific Interface Family Type on page 571
- Dynamically Attaching Filters Using RADIUS Variables on page 573

---

## Classic Filters Overview

The dynamic firewall feature supports classic filters and fast update filters. Classic filters are compiled at commit time. When a service activation takes place, the router creates an interface-specific clone of the filter and attaches the clone to the specified logical interface. Classic filters are static filters; they cannot contain subscriber-specific terms, as opposed to fast update filters, which are subscriber-specific.

This overview covers:

- Classic Filter Types on page 556
- Classic Filter Components on page 557
- Classic Filter Processing on page 557
- Guidelines for Creating and Applying Classic Filters for Subscriber Interfaces on page 558

## Classic Filter Types

The following classic 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.

## Classic Filter Components

When creating a classic filter, you first define the family address type (**inet** or **inet6**) and then you define one or more terms that specify the filtering criteria and the action to take when a match occurs.

Each term, or rule, 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 when 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.

## Classic Filter Processing

The order of the terms within a classic 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 accept or reject 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. 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.



**NOTE:** Dynamic filters do not process outbound packets that are sourced from the routing engine. To filter outbound packets that are sourced from the routing engine, you can create static outbound filters for each interface.

## Guidelines for Creating and Applying Classic 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 then 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.
- You can create family-specific **inet** and **inet6** filters.
- You can create interface-specific filters at the **unit** level that apply to any family type (**inet** or **inet6**) configured on the interface.
- You can add or remove both IPv4 and IPv6 filters with the same service activation or deactivation.
- You can remove one filter type without impacting the other type of filter. For example, you can remove IPv6 filters and leave the current IPv4 filters active.
- 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 or delete a firewall filter while subscribers on the same logical interface are bound.

### Related Documentation

- Dynamic Firewall Filters Overview on page 555
- Fast Update Filters Overview on page 564
- Dynamically Attaching Statically Created Filters for Any Interface Type on page 572
- Dynamically Attaching Statically Created Filters for a Specific Interface Family Type on page 571
- Dynamically Attaching Filters Using RADIUS Variables on page 573
- Verifying and Managing Firewall Filter Configuration on page 592

---

## Basic Classic Filter Syntax

This section provides the basic classic 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 family {
      filter {
        input {
          filter-name;
          precedence precedence;
        }
        output {
          filter-name;
          precedence precedence;
        }
      }
    }
  }
}
[edit]
firewall {
  family family {
    filter filter-name {
      [desired filter configuration]
    }
    filter filter-name {
      [desired filter configuration]
    }
  }
}

```

- Related Documentation**
- Dynamically Attaching Statically Created Filters for a Specific Interface Family Type on page 571
  - Dynamic Firewall Filters Overview on page 555

## Ascend-Data-Filter Policies for Subscriber Management Overview

Subscriber management enables you to use Ascend-Data-Filters to create policies for subscriber traffic. An Ascend-Data-Filter is a binary value that is configured on the RADIUS server. The filter contains rules that specify match conditions for traffic and an action for the router to perform (such as accept or discard the traffic). The match conditions might include the source and destination IP address or port, the protocol, the filter direction, the traffic class, and policer information.

Subscriber management uses a dynamic profile to obtain the Ascend-Data-Filter attribute (RADIUS attribute 242) from the RADIUS server and apply the policy to a subscriber session. Dynamic profiles support Ascend-Data-Filters for **inet** and **inet6** family types, and both families can be present in a dynamic profile. You include Junos OS predefined variables in the dynamic profiles — **\$junos-adf-rule-v4** for family **inet** and **\$junos-adf-rule-v6** for **inet6**. The predefined variables map the Ascend-Data-Filter rules to Junos OS functionality.

You can also configure a static Ascend-Data-Filter by manually entering the required binary data as a hexadecimal string in a dynamic profile. A statically configured

Ascend-Data-Filter in a dynamic profile takes precedence over an Ascend-Data-Filter attribute that is received from RADIUS. The static method is time-consuming to configure; it is typically used only for testing purposes.

The Ascend-Data-Filter attribute is supported in RADIUS Access-Accept and Change of Authorization (CoA) messages.

CoA updates existing filters based on the Ascend-Data-Filter Type field, as shown in the following list:

- If the Type field is 1, IPv4 rules are updated and IPv6 rules are unchanged. The opposite is true if the Type field is 3.
- If both Type 1 and 3 are specified, then all rules are updated.
- If the CoA has no Ascend-Data-Filter rules, then the existing rules are unchanged.

## Filter Naming Conventions

Each Ascend-Data-Filter has a unique name, which is assigned by the dynamic firewall daemon. The assigned names are displayed in the results of the **show subscriber extensive** and **show firewall** commands. Ascend-Data-Filters use the following naming convention.

***\_\_junos\_adf\_session#-interfacename-family-direction***

For example:

***\_\_junos\_adf\_33847-ge/1/0/4.53-init-in***

Each Ascend-Data-Filter rule maps to a single term, and the term names are simply **t0**, **t1**, **t3**. If you configure the **counter** option, the router adds a count action to each term that is created. The counter names are a combination of the the term names with **-cnt** appended. For example **t0-cnt** and **t1-cnt**.

## Using Multiple Sessions with Ascend-Data-Filters on an Interface

An interface can have multiple subscriber sessions, each session using its own Ascend-Data-Filter rules. When an Ascend-Data-Filter is applied to a subscriber session, the rules are created independently of any other filters and are added to the interface filter list. The Ascend-Data-Filter rules for the other sessions on the same interface are also added to the filter list. All packets that are processed for the interface must go through all filters, and the filters are applied according to the precedence you set.

Because the filter list can be a combination of several rules, you must consider how the multiple filters coexist. You must ensure that the filters are designed and applied correctly in order to provide the desired filtering and resulting action. For example, a session might have a filter that accepts traffic from Subscriber-A, and that discards all other traffic. However, a second session on the same interface might have a filter that accepts traffic from Subscriber-B only and discards other traffic. When the two filters are combined in the filter list, traffic from Subscriber-B is discarded by the first filter, and traffic from Subscriber-A is discarded by the second filter. As a result, no traffic is accepted on the interface because the two filters essentially cancel out each other and discard all traffic.

- Related Documentation**
- Dynamically Applying Ascend-Data-Filter Policies to Subscriber Sessions on page 577
  - Ascend-Data-Filter Attribute Fields on page 561

## Ascend-Data-Filter Attribute Fields

Table 50 on page 561 provides information about the fields used in the Ascend-Data-Filter attribute (RADIUS attribute 242) and how the fields map to Junos OS filter functions. The table lists the fields in the order in which they occur in the Ascend-Data-Filter attribute.

**Table 50: Ascend-Data-Filter Attribute Fields**

Action or Classifier	Format	Value	Junos OS Filter Function
Type	1 byte	<ul style="list-style-type: none"> <li>• 1 = IPv4</li> <li>• 3 = IPv6</li> </ul>	
Filter or forward	1 byte	<ul style="list-style-type: none"> <li>• 0 = filter</li> <li>• 1 = forward</li> </ul>	<ul style="list-style-type: none"> <li>• 0 = maps to <b>discard</b> action</li> <li>• 1 = maps to <b>accept</b> action</li> </ul>
Indirection	1 byte	<ul style="list-style-type: none"> <li>• 0 = egress</li> <li>• 1 = ingress</li> </ul>	<ul style="list-style-type: none"> <li>• 0 = adds egress terms to the output filter</li> <li>• 1 = adds ingress terms to the input filter</li> </ul>
Spare	1 byte	—	—
Source IP address	IPv4 = 4 bytes IPv6 = 16 bytes	IP address of the source interface	<ul style="list-style-type: none"> <li>• 0 = no mapping performed</li> <li>• From <b>source-address address</b> entry added to term</li> </ul>
Destination IP address	IPv4 = 4 bytes IPv6 = 16 bytes	IP address of the destination interface	<ul style="list-style-type: none"> <li>• 0 = no mapping performed</li> <li>• From <b>destination-address address</b> entry added to term</li> </ul>
Source IP prefix	1 byte	<ul style="list-style-type: none"> <li>• Type 1 = Number of leading zeros in the wildcard mask</li> <li>• Type 3 = Higher order contiguous bits of the address that make up the network portion of the address</li> </ul>	<ul style="list-style-type: none"> <li>• 0 = no mapping performed</li> <li>• From <b>source-address prefix</b> entry added to term</li> </ul>

Table 50: Ascend-Data-Filter Attribute Fields (*continued*)

Action or Classifier	Format	Value	Junos OS Filter Function
Destination IP prefix	1 byte	<ul style="list-style-type: none"> <li>Type 1 = Number of leading zeros in the wildcard mask</li> <li>Type 3 = Higher order contiguous bits of the address that make up the network portion of the address</li> </ul>	<ul style="list-style-type: none"> <li>0 = no mapping performed</li> <li>From <b>destination-address prefix</b> entry added to term</li> </ul>
Protocol	1 byte	Protocol type	<ul style="list-style-type: none"> <li>0 = no mapping performed</li> <li>IPv4 = from <b>protocol number</b> added to term</li> <li>IPv6 = from <b>next-header number</b> added to term</li> </ul>
Established	1 byte	Not implemented	Not implemented
Source port	2 bytes	Port number of the source port	From <b>source-port x - y</b> entry added to term
Destination port	2 bytes	Port number of the destination port	From <b>destination-port x - y</b> entry added to term
Source port qualifier	1 byte	<ul style="list-style-type: none"> <li>0 = no compare</li> <li>1 = less than</li> <li>2 = equal to</li> <li>3 = greater than</li> <li>4 = not equal to</li> </ul>	<ul style="list-style-type: none"> <li>0 = no mapping performed</li> <li>1 – 3 = mapped to corresponding option</li> <li>4 = mapped to <b>except</b> match option</li> </ul>
Destination port qualifier	1 byte	<ul style="list-style-type: none"> <li>0 = no compare</li> <li>1 = less than</li> <li>2 = equal to</li> <li>3 = greater than</li> <li>4 = not equal to</li> </ul>	<ul style="list-style-type: none"> <li>0 = no mapping performed</li> <li>1 – 3 = mapped to corresponding match option</li> <li>4 = mapped to <b>except</b> match option</li> </ul>
Reserved	2 bytes	Not used	Not used
Marking value	1 byte	<ul style="list-style-type: none"> <li>For IPv4 = Type of Service (ToS)</li> <li>For IPv6 = Differentiated Services Code Point (DSCP)</li> </ul>	Not implemented
Marking mask	1 byte	0 = no packet marking	Not implemented



Table 50: Ascend-Data-Filter Attribute Fields (*continued*)

Action or Classifier	Format	Value	Junos OS Filter Function
Traffic class	1–41 bytes	<ul style="list-style-type: none"> <li>0 = no traffic class (required if there is no profile)</li> <li>First byte specifies the length of the ASCII name of the traffic class</li> <li>Traffic class must be statically configured</li> <li>Name can optionally be null terminated, which consumes 1 byte</li> <li>If a name is given, it must match one of the default forwarding classes (such as best-effort) or the name of a forwarding class configured under the <b>[edit class-of-service scheduler-maps map-name]</b> stanza.</li> </ul>	Maps to the forwarding class name. The action <b>forwarding-class name</b> is added to term.
Rate-limit profile	1–41 bytes	<ul style="list-style-type: none"> <li>0 = no rate limit (required if there is no profile)</li> <li>First byte specifies the length of the ASCII, followed by the ASCII name of the profile</li> <li>Profile must be statically configured</li> <li>Name can optionally be null terminated, which consumes 1 byte</li> <li>If a name is given, it must match the name of one of the firewall policers that is configured under the <b>[edit firewall]</b> stanza.</li> </ul>	Maps to the <b>policer policer-name</b> action modifier of the same name. The action <b>policer name</b> is added to term.

**Related Documentation**

- Ascend-Data-Filter Policies for Subscriber Management Overview on page 559

## Fast Update Filters Overview

---

The dynamic firewall feature supports classic filters and fast update filters. Fast update filters support subscriber-specific filter values, as opposed to classic filters, which are interface-specific. Fast update filters allow individual filter terms, or rules, to be added or removed from filters without requiring that you recompile the filter after each modification—terms are added and removed when subscriber services are added and removed.

Using the fast update filters feature involves three distinct operations:

1. Creating the filter—You define fast update filters under the **[edit dynamic-profiles profile-name firewall family family]** hierarchy. The **dynamic-profiles** stanza enables you to use dynamic variables to create subscriber-specific configurations for the filter's match terms. See "Configuring Fast Update Filters" on page 581.
2. Associating the filter with a dynamic profile—You use the **[edit dynamic-profiles profile-name interface interface-name unit unit-number family family]** hierarchy to associate the filter with a dynamic profile. This is the same procedure used for classic filters. See "Associating Fast Update Filters with Interfaces in a Dynamic Profile" on page 591.
3. Attaching the filter to an interface—When a subscriber logs in, the dynamic profile instantiates the subscriber session and applies the properties of the profile, including the fast update filter, to the session interface. This is the same procedure used for classic filters. Also, similar to classic filters, the name of fast update filters can be provided in a user's RADIUS file.

When a dynamic profile instantiates a subscriber session and applies a fast update filter, the router verifies that the filter is not already present on the session interface. If the filter is not present, the router adds the filter. If the filter is already present on the interface, the router simply adds any new terms that are not in the existing filter. This procedure is reversed when subscriber sessions are deleted. Any terms that were added by a session are then removed when the session is deleted. The filter is deleted when the last subscriber session is deleted.



**NOTE:** You can optionally specify that a term can be added only once and cannot be modified. See "Match Conditions and Actions in Fast Update Filters" on page 568.

---

This overview covers:

- Fast Update Filter Components on page 565
- Fast Update Filter Processing on page 565
- Fast Update Filter Names on page 566
- Guidelines for Creating and Applying Fast Update Filters on page 566

## Fast Update Filter Components

When creating a fast update filter, you define one or more terms that specify the filtering criteria and the action to take when a match occurs.

Each term consists of the following components:

- **Match condition**—Specifies values or fields that the packet must contain. You can match a maximum of five fields in a fast update filter. A match condition can contain a single value or range. This differs from classic filters, in which terms can have multiple values. However, you can use additional terms to specify multiple ranges. “Fast Update Filter Match Conditions” on page 584 lists the supported match conditions for fast update filters. The order in which the terms appear in a fast update filter is not important, because the router examines the most specific term first. (Classic filters examine the terms in the order in which the terms are listed.)
- **Action**—Specifies what to do when a packet matches the match condition. If no action is specified for a term, the default action is to accept the packet. “Fast Update Filter Actions and Action Modifiers” on page 585 lists the supported actions for fast update filters.

Terms that are added to the filter during session instantiation must have a unique set of match conditions. Two terms overlap, or conflict, if a packet can match both sets of conditions—as a result, there are two different actions for the packet. You can ensure that terms are unique by using the `$junos-subscriber-ip-address` variable as the **source-address** (for an input filter) or **destination-address** (for an output filter) in the **from** statement. You must then supply the **source-address** or **destination-address** condition, as appropriate, as the first condition in the **match-order** statement.

### Related Documentation

- Fast Update Filter Actions and Action Modifiers on page 585
- Fast Update Filter Match Conditions on page 584
- Avoiding Conflicts When Terms Match on page 586

## Fast Update Filter Processing

You must use the **match-order** statement to explicitly specify the order in which the router examines filter match conditions. Also, the router examines only those conditions that you include in the **match-order** statement. When a fast update filter contains multiple terms, the router compares a packet against the terms starting with the most specific condition first. When the packet first matches a condition, the router performs the action defined in the term to either accept or reject the packet, and then 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 filter. The router continues to compare the packet to the next specified term until a match is found. If there is no match after all terms have been examined, the router silently drops the packet.

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. 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.

## Fast Update Filter Names

When a filter is attached to an interface, the router first searches for a classic filter with the specified name, and then uses the classic filter. If no classic filter exists with that name, the router then searches in the dynamic profile for a fast update filter with the specified name, and uses that filter.

If two different dynamic profiles include a fast update filter with the same name, the **match-order** specification of the two filters must be identical. If the two filters are activated on the same interface, the terms are added together.

The router includes the filter name in **show firewall** command results. The router also creates unique names for filter terms and counters for the **show firewall** command.

When a fast update filter is created by the activation of a dynamic profile, the router creates an interface-specific name for the filter. The name uses the following format, which is also used for classic filters:

**<filter-name>-<interface-name>.<subunit>-<direction>**

For example, an input filter named **httpFilter** on interface **ge-1/0/0.5** is named as follows (**in** indicates an input filter and **out** indicates an output filter):

**http-filter-ge-1/0/0.5-in**

The router creates unique names for the filter terms and counters by appending the session ID to all term and counter names. Terms that use the **only-at-create** statement have a session-id of 0. Terms and counters use the following format:

**<term-name>-<session-id>**

**<counter-name>-<session-id>**

## Guidelines for Creating and Applying Fast Update Filters

Fast update filters enable you to create subscriber-specific firewall filters and dynamically apply these filters to statically created interfaces using dynamic profiles. Individual terms can be added to, or removed from, a filter without requiring that the entire filter be recompiled.

When creating and applying fast update filters, keep the following in mind:

- This release supports dynamic application of input and output filters.
- Fast update filters must always include terms that permit DHCP traffic to pass. See “Configuring Filters to Permit Expected Traffic” on page 585.
- You can create **family inet** and **inet6** filters.

- You can add or remove both IPv4 and IPv6 filters with the same service activation or deactivation.
- You can remove one filter type without impacting the other type of filter. For example, you can remove IPv6 filters and leave the current IPv4 filters active.
- The **interface-specific** statement is required for all fast update filters.
- The **match-order** statement is required—you must explicitly state the order of the match fields in a fast update filter. See “Configuring the Match Order for Fast Update Filters” on page 582.
- The **match-order** statement uses an implied wildcard for conditions that you specify in the statement. If you specify a condition that is not also configured in the **from** specification of a filter term, the router considers that a wildcard for that condition.
- A filter term can have only a single value or range; however, you can configure multiple terms to specify multiple ranges.
- You can match a maximum of five match conditions in a filter.

#### Related Documentation

- Dynamic Firewall Filters Overview on page 555
- Classic Filters Overview on page 556
- Dynamically Attaching Statically Created Filters for Any Interface Type on page 572
- Dynamically Attaching Statically Created Filters for a Specific Interface Family Type on page 571
- Verifying and Managing Firewall Filter Configuration on page 592

## Basic Fast Update Filter Syntax

This section shows the basic fast update filter statement syntax. The first part of this syntax provides the CLI statements to associate an input and output filter with 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 family {
        filter {
          input filter-name;
          precedence precedence;
          output filter-name;
          precedence precedence;
        }
      }
    }
  }
}
[edit dynamic-profiles profile-name]
```

```
firewall {  
  family family {  
    fast-update-filter filter-name {  
      [desired filter configuration]  
    }  
    fast-update-filter filter-name {  
      [desired filter configuration]  
    }  
  }  
}
```

**Related Documentation**

- [Configuring Fast Update Filters on page 581](#)

---

## Match Conditions and Actions in Fast Update Filters

To create a fast update filter, you use the **term** statement to specify conditions that a packet must have, and to specify the action the router performs when those conditions exist in the packet.

This section covers:

- [Match Conditions on page 568](#)
- [Actions on page 569](#)
- [Adding Terms Only Once on page 569](#)

### Match Conditions

Match conditions specify characteristics that a packet must have—if the conditions exist in the packet, the router then performs the specified action. You use the **from** keyword in the **term** statement to specify match conditions for the filter. The packet must match all conditions in the **from** specification for the action to be performed, which also means that their order in the **from** specification is not important.

An individual condition in a **from** specification can contain a single value or range. You can match a maximum of five match conditions in a filter.

“Fast Update Filter Match Conditions” on page 584 lists the match conditions you can use in fast update filters.



**NOTE:** The router uses an implied wildcard for conditions that you include in the **match-order** statement. If you include a condition that is *not* configured in the **from** specification of a filter term, the router considers that a wildcard for the condition.

For example, if you include the **dscp** condition in the **match-order** statement, but do not configure a **dscp** value in the **from** specification of the filter term, the router performs the action configured in the **then** specification of the filter on all DSCP values.

---

## Actions

Actions and action modifiers specify the operation the router performs when a particular match condition exists in a packet. You use the **then** keyword in the **term** statement to specify the actions to perform on packets whose characteristics match the conditions specified in the preceding **from** specification.

Action modifiers are actions taken in addition to the specified action. You can configure any combination of action modifiers. For the action or action modifier to take effect, all conditions in the **from** specification must match. If you specify **log** as one of the actions in a term, this constitutes a termination action; whether any additional terms in the filter are processed depends on the traffic through the filter. The action modifier operations carry a default **accept** action. For example, if you specify an action modifier and do not specify an action, the specified action modifier is implemented and the packet is accepted.

“Fast Update Filter Actions and Action Modifiers” on page 585 lists the actions and action modifiers you can use in fast update filters.

## Adding Terms Only Once

You can optionally specify that a term can be added only when the fast update filter is first created, and cannot be later changed by adding or removing conditions. We recommend that you only use the **only-at-create** option for terms that do not include subscriber-specific data in their match conditions, such as common or default terms (counting the default drop packet, for instance).

### Related Documentation

- Configuring Terms for Fast Update Filters on page 583
- Fast Update Filter Match Conditions on page 584
- Fast Update Filter Actions and Action Modifiers on page 585

## Dynamic Service Sets Overview

A service set is a collection of services to be performed by an Adaptive Services (AS) or Multiservices PIC. You configure a service-set definition at the **[edit services]** hierarchy level. You can then apply the service set to one or more interfaces on the router. The service set can be applied either dynamically or statically.

To dynamically associate a service set to interfaces you include the **service-set** statement with the **input** or **output** statement at the **[edit dynamic-profiles *profile-name* interfaces *interface-name* unit *logical-unit-number* family *family* service]** hierarchy level.

To statically associate a defined service set with an interface, you include the **service-set** statement with the **input** or **output** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family *family* service]** hierarchy level.

### Related Documentation

- Associating Service Sets with Interfaces in a Dynamic Profile on page 595
- Verifying and Managing Service Sets Information on page 596

- For information about creating service sets, see “Service Set Configuration Guidelines” in the *Junos OS Services Interfaces Configuration Guide*.
- For information about statically applying service sets to interfaces, see “Applying Filters and Services to Interfaces” in the *Junos OS Services Interfaces Configuration Guide*.



## Configuring Filters for Dynamic Profiles

- Dynamically Attaching Statically Created Filters for a Specific Interface Family Type on page 571
- Dynamically Attaching Statically Created Filters for Any Interface Type on page 572
- Dynamically Attaching Filters Using RADIUS Variables on page 573
- Defining Dynamic Filter Processing Order on page 574
- Configuring Firewall Filter Bypass on page 575
- Configuring Service Packet Counting on page 576
- Dynamically Applying Ascend-Data-Filter Policies to Subscriber Sessions on page 577
- Verifying and Managing Dynamic Ascend-Data-Filter Policy Configuration on page 578

### Dynamically Attaching Statically Created Filters for a Specific Interface Family Type

You can dynamically attach statically created filters for either IPv4 (**inet**) or IPv6 (**inet6**) interface types. These filters apply only to interfaces of the specified type.

Before you can attach a statically created filter using a dynamic profile.

1. Create the filters you want to attach.

See the *Junos OS Routing Policy Configuration Guide* for detailed information about classic firewall filters and how to create them. See “Configuring Fast Update Filters” on page 581 for information about creating fast update filters.

2. Create a basic dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 391.

To dynamically attach statically created input and output filters:

1. Specify the unit family type you want to use when dynamically attaching the filters.
  - a. For IPv4 interfaces, specify the **inet** unit family.

```
[edit dynamic-profiles access-profile interfaces ge-1/1/1 unit 1]  
user@host# set family inet
```
  - b. For IPv6 interfaces, specify the **inet6** unit family.

```
[edit dynamic-profiles access-profile interfaces ge-1/1/1 unit 1]
```

```
user@host# set family inet6
```

2. 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
```

3. 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 Documentation

- Classic Filters Overview on page 556
- Fast Update Filters Overview on page 564
- Dynamically Attaching Statically Created Filters for Any Interface Type on page 572
- Dynamically Attaching Filters Using RADIUS Variables on page 573
- For information about Junos OS default groups, see the [Junos OS CLI User Guide](#)
- For information about firewall filters, see the [Junos OS Routing Policy Configuration Guide](#)

---

## Dynamically Attaching Statically Created Filters for Any Interface Type

You can dynamically attach statically created filters for any interface type. These filters apply to any interfaces that are created using the dynamic profile.

Before you can attach a statically created filter using a dynamic profile.

1. Create the filters you want to attach.

See the [Junos OS Routing Policy Configuration Guide](#) for detailed information about classic firewall filters and how to create them. See “Configuring Fast Update Filters” on page 581 for information about creating fast update filters.

2. Create a basic dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 391.

To dynamically attach statically created input and output filters for all interfaces created dynamically using the dynamic profile:

1. Access the dynamic profile, interface, and unit that you want to use when applying the static filters.

```
[edit]  
user@host# edit dynamic-profiles access-profile interfaces ge-1/1/1 unit 1
```

2. Specify the input filter for the interface unit.

```
[edit dynamic-profiles access-profile interfaces ge-1/1/1 unit 1]
```

```
user@host# set filter input static-input-filter
```

3. Specify the output filter for the interface unit.

```
[edit dynamic-profiles access-profile interfaces ge-1/1/1 unit 1]
```

```
user@host# set filter output static-output-filter
```

#### Related Documentation

- Classic Filters Overview on page 556
- Fast Update Filters Overview on page 564
- Dynamically Attaching Statically Created Filters for a Specific Interface Family Type on page 571
- Dynamically Attaching Filters Using RADIUS Variables on page 573
- For information about Junos OS default groups, see the [Junos OS CLI User Guide](#)
- For information about firewall filters, see the [Junos OS Routing Policy 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-filter
26–11	Egress-Policy-Name	\$junos-output-filter
26–106	IPv6-Ingress-Policy-Name	\$junos-input-ipv6-filter
26–107	IPv6-Egress-Policy-Name	\$junos-output-ipv6-filter

Before you can attach a filter using RADIUS.

1. Create a basic dynamic profile.  
See “Configuring a Basic Dynamic Profile” on page 391.
2. Ensure that RADIUS ingress and egress policies are configured appropriately.  
See “Configuring RADIUS Server Parameters for Subscriber Access” on page 26.

To dynamically attach IPv4 input and output filters using RADIUS:

1. Specify the dynamic profile you want to attach, the interface, the logical unit number, and family **inet**.

```
[edit]
```

```
user@host# edit dynamic-profiles myProfile interface ge-1/1/1 unit 1 family inet
```

2. Specify the IPv4 input filter variable in the dynamic profile.

```
[edit dynamic-profiles myProfile interfaces ge-1/1/1 unit 1 family inet]
user@host# set filter input $junos-input-filter
```

3. Specify the IPv4 output filter variable in the dynamic profile.

```
[edit dynamic-profiles myProfile interfaces ge-1/1/1 unit 1 family inet]
user@host# set filter output $junos-output-filter
```

To dynamically attach IPv6 input and output filters using RADIUS:

1. Specify the dynamic profile you want to attach, the interface, the logical unit number, and family **inet6**.

```
[edit]
user@host# edit dynamic-profiles myProfile interface ge-1/1/1 unit 1 family inet6
```

2. Specify the IPv6 input filter variable in the dynamic profile.

```
[edit dynamic-profiles myProfile interfaces ge-1/1/1 unit 1 family inet6]
user@host# set filter input $junos-input-ipv6-filter
```

3. Specify the IPv6 output filter variable in the dynamic profile.

```
[edit dynamic-profiles myProfile interfaces ge-1/1/1 unit 1 family inet6]
user@host# set filter output $junos-output-ipv6-filter
```

#### Related Documentation

- Classic Filters Overview on page 556
- Dynamically Attaching Statically Created Filters for Any Interface Type on page 572
- Dynamically Attaching Statically Created Filters for a Specific Interface Family Type on page 571
- For more information about Junos default groups, see the [Junos OS CLI User Guide](#)
- For more information about firewall filters, see the [Junos OS Routing Policy 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 profile-name interfaces (interface-name | demux0) unit logical-unit-number family family]` hierarchy level.

The precedence range is from 0 through 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 OS Routing Policy 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 391.

3. Attach the filters to the dynamic profile.

See “Dynamically Attaching Statically Created Filters for Any Interface Type” on page 572, “Dynamically Attaching Statically Created Filters for a Specific Interface Family Type” on page 571, or “Dynamically Attaching Filters Using RADIUS Variables” on page 573.

To define a precedence for an input and output filter:

1. Specify the input filter precedence in the dynamic profile.

```
[edit dynamic-profiles profile-name interfaces interface-name unit logical-unit-number
family family]
user@host# set filter input precedence 50
```

2. Specify the output filter precedence in the dynamic profile.

```
[edit dynamic-profiles profile-name interfaces interface-name unit logical-unit-number
family family]
user@host# set filter output precedence 5
```

#### Related Documentation

- Classic Filters Overview on page 556
- For information about firewall filters, see the [Junos OS Routing Policy Configuration Guide](#)

## Configuring Firewall Filter Bypass

You can streamline the filter process, decrease the amount of packet handling for each filter in a chain, and effectively bypass unnecessary filters by using the **service-filter-hit** match/action combination at the `[edit firewall family family-name filter filter-name term term-name]` hierarchy level.

To bypass firewall filters using the **service-filter-hit** match/action combination, you configure the **service-filter-hit** action in at least one filter in the chain and configure **service-filter-hit** match condition in any subsequent filters that you want to bypass. All packets must pass through each filter in a chain. However, after the **service-filter-hit** flag is set in a packet, the packet “bypasses” any subsequent filters that contain the **service-filter-hit** match condition and more efficiently passes (accepts) marked packets and accelerating the filter process.



**NOTE:** When using the **service-filter-hit** match/action combination, the order in which the filters are applied is important. You can ensure the order in which the filters are processed by specifying a filter precedence value for the interface. See “Defining Dynamic Filter Processing Order” on page 574 for more information about dynamic filter processing.

To bypass filter processing:

1. Specify the **service-filter-hit** action for any filters in a filter chain.

```
[edit firewall family inet filter video term 1]
user@host# set then service-filter-hit
```

When the match conditions for the filter are met, the **service-filter-hit** action is set to indicate to subsequent filters that further processing is unnecessary.

2. Specify the **service-filter-hit** match condition in any filters with a lower precedence (that is, a higher **precedence** statement value) that you want to detect **service-filter-hit** actions applied from previous filters in the chain.

```
[edit firewall family inet filter data term 1]
user@host# set from service-filter-hit
```

3. Configure the filter to pass (accept) any packet that has a **service-filter-hit** action applied from any previous filters.

```
[edit firewall family inet filter data term 1]
user@host# set then accept
```

**Related  
Documentation**

- Classic Filters Overview on page 556
- Defining Dynamic Filter Processing Order on page 574
- Example: Bypassing Firewall Filters on page 608

---

## Configuring Service Packet Counting

You can count service packets, applying them to a specific named counter (`_junos-dyn-service-counter`), for use by RADIUS, by specifying the **service-accounting** action at the `[edit firewall family family-name filter filter-name term term-name then]` hierarchy level.

Service packet counting is used by the router to provide volume statistics for subscribers on a per-service session basis. See “Configuring Per-Service Session Accounting” on page 25 for additional information, including descriptions of the RADIUS VSAs used for per-service session accounting.

To enable service packet counting:

1. Configure any match conditions that you want to count using the service accounting action. For example:

```
[edit firewall family inet filter filtername term term-name]
user@host# set from source-address address
```

2. Specify the **service-accounting** action for the filter.

```
[edit firewall family inet filter filtername term term-name]
user@host# set then service-accounting
```

When the match conditions for the filter are met, the packet is counted and applied to the well-known service counter (`_junos-dyn-service-counter`) for use by the RADIUS server. This counter provides the volume statistics for per-service accounting.

**Related  
Documentation**

- Classic Filters Overview on page 556
- Defining Dynamic Filter Processing Order on page 574
- RADIUS Accounting Statistics for Subscriber Access Overview on page 23
- Configuring Per-Service Session Accounting on page 25
- Configuring Per-Subscriber Session Accounting on page 24
- Guidelines for Configuring Standard Firewall Filters
- Guidelines for Applying Standard Firewall Filters
- Standard Firewall Filter Terminating Actions
- Standard Firewall Filter Nonterminating Actions

## Dynamically Applying Ascend-Data-Filter Policies to Subscriber Sessions

Subscriber management enables you to use dynamic profiles to dynamically apply policies that are defined in Ascend-Data-Filters (RADIUS attribute 242) to subscriber sessions. The dynamic profiles include a Junos OS predefined variable that maps the rules and actions defined in the Ascend-Data-Filter to Junos OS features. The RADIUS administrator configures the Ascend-Data-Filter on the RADIUS server in a separate operation.

Subscriber management dynamic profiles use the following Junos OS predefined variables to map Ascend-Data-Filter rules to Junos OS filter functionality.

- `$junos-adf-rule-v4`—Used for IPv4 family `inet`.
- `$junos-adf-rule-v6`—Used for IPv6 family `inet6`.

To configure a dynamic profile to dynamically apply the policy defined by an Ascend-Data-Filter to a subscriber session:

1. Specify the dynamic profile in which you want to include the Ascend-Data-Filter. Specify the interface, the logical unit number, and the family type.

[edit]

```
user@host# edit dynamic-profiles profile-name interfaces interface-name unit
logical-unit-number family family
```

2. Specify that you want to include an Ascend-Data-Filter in the dynamic profile.

```
[edit dynamic-profiles profile-name interfaces interface-name unit logical-unit-number
family family]
user@host# edit filter adf
```

3. Specify the Junos OS predefined variable that maps the Ascend-Data-Filter actions to Junos OS filter functionality. Use the variable that corresponds to the specified family type.

```
[edit dynamic-profiles profile-name interfaces interface-name unit logical-unit-number
family family filter adf]
user@host# set rule ($junos-adf-rule-v4 | $junos-adf-rule-v6)
```



**NOTE:** You can also statically configure the Ascend-Data-Filter in this step by entering the filter in hexadecimal format, rather than use a predefined variable. You might use a static filter for testing purposes.

4. (Optional) Enable the counter feature. The counter increments each time a packet matches the rule.

```
[edit dynamic-profiles profile-name interfaces interface-name unit logical-unit-number
family family filter adf]
user@host# set counter
```

5. (Optional) Specify the input precedence used to establish the order in which filters on the interface are applied. A lower precedence value equals a higher precedence. The precedence relates to other dynamic filters configured on the same interface.

```
[edit dynamic-profiles profile-name interfaces interface-name unit logical-unit-number
family family filter adf]
user@host# set input-precedence precedence
```

6. (Optional) Specify the output precedence used to establish the order in which filters on the interface are applied. A lower precedence value equals a higher precedence. The precedence relates to other dynamic filters configured on the same interface.

```
[edit dynamic-profiles profile-name interfaces interface-name unit logical-unit-number
family family filter adf]
user@host# set output-precedence precedence
```

#### Related Documentation

- Ascend-Data-Filter Policies for Subscriber Management Overview on page 559
- Ascend-Data-Filter Attribute Fields on page 561
- Verifying and Managing Dynamic Ascend-Data-Filter Policy Configuration on page 578
- Example: Configuring Dynamic Ascend-Data-Filter Support for Subscriber Access on page 600
- Example: Configuring Static Ascend-Data-Filter Support for Subscriber Access on page 603

## Verifying and Managing Dynamic Ascend-Data-Filter Policy Configuration

**Purpose** View or manage information for Ascend-Data-Filters.

**Action** • To display statistics for Ascend-Data-Filters:

```
user@host> show firewall
```



- To display firewall log information:  
user@host> **show subscribers extensive**
- To clear filter counters:  
user@host> **clear firewall all**

**Related  
Documentation**

- Ascend-Data-Filter Policies for Subscriber Management Overview on page 559
- Dynamically Applying Ascend-Data-Filter Policies to Subscriber Sessions on page 577



## Configuring Fast Update Filters

- Configuring Fast Update Filters on page 581
- Configuring the Match Order for Fast Update Filters on page 582
- Configuring Terms for Fast Update Filters on page 583
- Fast Update Filter Match Conditions on page 584
- Fast Update Filter Actions and Action Modifiers on page 585
- Configuring Filters to Permit Expected Traffic on page 585
- Avoiding Conflicts When Terms Match on page 586
- Associating Fast Update Filters with Interfaces in a Dynamic Profile on page 591
- Verifying and Managing Firewall Filter Configuration on page 592

### Configuring Fast Update Filters

---

You configure a fast update filter in a dynamic profile—this enables you to use dynamic variables in the filter configuration. After you configure fast update filters, you then use the **dynamic-profiles** syntax to associate the filter with the subscriber interface.

To configure a fast update filter for subscriber access:

1. Access the dynamic profile you want to use.

```
[edit]  
user@host# edit dynamic-profiles myProfile
```

2. Specify that you want to configure a firewall, and specify the family.

```
[edit dynamic-profiles myProfile]  
user@host# edit firewall family inet
```

3. Specify that you want to configure a fast update filter and assign a name to the filter.

```
[edit dynamic-profiles myProfile firewall family inet]  
user@host# edit fast-update-filter httpFilter
```

4. Specify the **interface-specific** statement. This statement is mandatory.

```
[edit dynamic-profiles myProfile firewall family inet fast-update-filter httpFilter]  
user@host# set interface-specific
```

5. Configure the match order to use for the filter terms.

```
[edit dynamic-profiles myProfile firewall family inet fast-update-filter httpFilter]
user@host# set match-order [source-address protocol destination-port]
```

See “Configuring the Match Order for Fast Update Filters” on page 582.

6. Specify that you want to configure a term for the filter and assign the name to the term. Configure the match conditions and actions for the term.

```
[edit dynamic-profiles myProfile firewall family inet fast-update-filter httpFilter]
user@host# edit term term1
```

```
[edit dynamic-profiles myProfile firewall family inet fast-update-filter httpFilter term
term1]
user@host# set from protocol tcp
user@host# set from source-address $junos-subscriber-ip-address
user@host# set from destination-port http
user@host# set then count http-cnt
```

See “Configuring Terms for Fast Update Filters” on page 583.

#### Related Documentation

- Configuring the Match Order for Fast Update Filters on page 582
- Configuring Terms for Fast Update Filters on page 583
- Associating Fast Update Filters with Interfaces in a Dynamic Profile on page 591
- Fast Update Filters Overview on page 564
- Dynamic Profiles Overview on page 369
- For information about firewall filters, see Guidelines for Configuring Standard Firewall Filters and Guidelines for Applying Standard Firewall Filters in the *Junos OS Firewall Filter and Policer Configuration Guide*.

---

## Configuring the Match Order for Fast Update Filters

You must include the **match-order** statement to explicitly specify the order in which router examines the match conditions. The router examines only those match conditions that you include in the statement. You can match a maximum of five conditions.



**NOTE:** If the **match-order** statement contains a condition that is not specified in the **from** statement of a term, the router considers that a wildcard for that condition.

If you use the same fast update filter in multiple dynamic profiles, you must configure the same match order for all profiles.

To configure the order in which the router examines the match conditions of a fast update filter:

1. Access the fast update filter:

```
[edit dynamic-profiles myProfile]
```

```
user@host# edit firewall family inet fast-update-filter httpFilter
```

2. Specify the mandatory **interface-specific** statement.

```
[edit dynamic-profiles myProfile firewall family inet fast-update-filter httpFilter]
user@host# set interface-specific
```

3. Configure the match order for the match conditions in the filter. Use brackets to enclose multiple match conditions.

```
[edit dynamic-profiles myProfile firewall family inet fast-update-filter httpFilter]
user@host# set match-order [source-address protocol destination-port]
```

#### Related Documentation

- Configuring Fast Update Filters on page 581
- Configuring Terms for Fast Update Filters on page 583
- Fast Update Filters Overview on page 564
- Dynamic Profiles Overview on page 369
- Fast Update Filter Match Conditions on page 584
- For information about firewall filters, see the *Junos OS Routing Policy Configuration Guide*

## Configuring Terms for Fast Update Filters

A fast update filter consists of one or more terms. A term is made up of one or more match conditions and the action to take when a packet matches the specified conditions.

To configure a term for a fast update filter:

1. Access the fast update filter.

```
[edit dynamic-profiles myProfile]
user@host# edit firewall family inet fast-update-filter httpFilter
```

2. Create the new term and assign a name to the term.

```
[edit dynamic-profiles myProfile firewall family inet fast-update-filter httpFilter]
user@host# set term term1
```

3. Configure the match condition for the term. See “Fast Update Filter Match Conditions” on page 584 for the supported match conditions for fast update filters.

```
[edit dynamic-profiles myProfile firewall family inet fast-update-filter httpFilter]
user@host# set from protocol tcp
user@host# set from source-address $junos-subscriber-ip-address
user@host# set from destination-port http
```

4. Configure the action that the router takes when the match conditions are met. See “Fast Update Filter Actions and Action Modifiers” on page 585 for the supported actions for fast update filters.

```
[edit dynamic-profiles myProfile firewall family inet fast-update-filter httpFilter]
user@host# set then accept
```

5. (Optional) Configure the action modifiers that you want the router to take when the match conditions are met. See “Fast Update Filter Actions and Action Modifiers” on page 585 for the supported action-modifiers for fast update filters.

```
[edit dynamic-profiles myProfile firewall family inet fast-update-filter httpFilter]
user@host# set then count http-cnt
```

6. (Optional) Configure the term to be added only once, when the fast update filter is first created.

```
[edit dynamic-profiles myProfile firewall family inet fast-update-filter httpFilter]
user@host# set only-at-create
```

#### Related Documentation

- Configuring Fast Update Filters on page 581
- Configuring the Match Order for Fast Update Filters on page 582
- Fast Update Filters Overview on page 564
- Fast Update Filter Match Conditions on page 584
- Fast Update Filter Actions and Action Modifiers on page 585
- For additional information about firewall filter terms, see the following topics in the [Junos OS Firewall Filter and Policier Configuration Guide](#)
  - Stateless Firewall Filter Overview
  - Stateless Firewall Filter Components

## Fast Update Filter Match Conditions

Table 51: Fast Update Filter Match Conditions

Match Condition	Description
<b>destination-address</b> <i>prefix</i>	IP destination address field.
<b>destination-port</b> <i>number</i>	TCP or UDP destination port field. Can be a single number, a single range, or one of the standard port synonyms.
<b>dscp</b> <i>number</i>	Differentiated services code point. Can be a single number, a single range, or the standard synonyms. IPv4 only.
<b>match-terms</b> <i>string-of-conditions</i>	Series of match conditions. Enclose the string within quotation marks and use semicolons to separate entries. For example, <b>match-terms "protocol tcp; destination-port http"</b> ; Dynamic profile variables are not allowed in the string.
<b>protocol</b> <i>number</i>	IP protocol field. Can be a single number, a single range, or one of the standard protocol synonyms. IPv4 only.
<b>source-address</b> <i>prefix</i>	IP source address field.
<b>source-port</b> <i>number</i>	TCP or UDP source port field. Can be a single number, a single range, or one of the standard protocol synonyms.

## Fast Update Filter Actions and Action Modifiers

Table 52: Fast Update Filter Actions and Action Modifiers

Action or Action Modifier	Description
<b>Actions</b>	
<b>accept</b>	Accept the packet.
<b>action-terms</b> <i>string-of-actions</i>	A series of multiple actions or action modifiers. Enclose the string within quotation marks and use semicolons to separate entries. For example, <b>action-terms</b> "log; count http-cnt";. Dynamic profile variables are not allowed in the string.
<b>discard</b>	Drop the packet silently, without sending an Internet Control Message Protocol (ICMP) message.
<b>ignore-term</b>	Do not add this term to the filter. All match conditions and actions are ignored.
<b>port-mirror</b>	Port mirror packets.
<b>routing-instance</b> <i>routing-instance</i>	Forward packets to specified routing instance.
<b>Action Modifiers</b>	
<b>count</b> <i>counter-name</i>	Increment the specified counter.
<b>forwarding-class</b> <i>class</i>	Classify the packet into one of the following forwarding classes: <b>as</b> , <b>assured-forwarding</b> , <b>best-effort</b> , <b>expedited-forwarding</b> , or <b>network-control</b> .
<b>log</b>	Log the packet header information.
<b>loss-priority</b> (high   medium-high   medium-low   low)	Set the loss priority level for packets.
<b>policer</b> <i>policer-name</i>	Rate-limit packets based on the specified policer.

## Configuring Filters to Permit Expected Traffic

You must explicitly configure your firewall filter to permit expected traffic, such as DHCP traffic, to pass. Otherwise, the expected traffic is denied when the filter is applied to the interface. This requirement applies to both classic and fast update filters.

The following example shows a fast update filter that might be used to accept DHCP traffic. The actual filter you use depends on the expected traffic in your network.

In the example, the term **allow-dhcp** accepts all DHCP traffic from all source addresses. The term also includes the **only-at-create** option to specify that the term is applied only

when the filter is first applied. The term **sub-allow-dhcp** includes the Junos OS predefined variable **\$junos-subscriber-ip-address**, which permits all subscriber-specific DHCP traffic.

The **match-order** statement configuration lists the conditions from most-specific to least-specific, as recommended in “Configuring the Match Order for Fast Update Filters” on page 582. Because this filter is designed to permit ingress DHCP traffic, the **source-address** condition is listed first.

```
firewall {
  family inet {
    fast-update-filter psf1 {
      interface-specific;
      match-order [ source-address destination-address protocol destination-port ];
      term allow-dhcp {
        only-at-create;
        from {
          source-address 0.0.0.0/32;
          destination-address 255.255.255.255/32;
          destination-port 67;
          protocol udp;
        }
        then accept;
      }
      term sub-allow-dhcp {
        from {
          source-address $junos-subscriber-ip-address;
          destination-address 192.168.1.2/32;
          destination-port 67;
          protocol udp;
        }
        then accept;
      }
    }
  }
}
```

- Related Documentation**
- [Configuring the Match Order for Fast Update Filters on page 582](#)
  - [Configuring Terms for Fast Update Filters on page 583](#)

---

## Avoiding Conflicts When Terms Match

A fast update filter can contain multiple terms, each with a variety of match conditions. However, when you configure multiple terms in a filter, you must ensure that the terms do not overlap, or conflict with each other. Two terms are considered to overlap when it is possible for a packet to match all conditions of both terms. Because each term specifies a different action for matches, the router cannot determine which action to take. When terms overlap, a conflict error occurs and the session fails when the dynamic profile attempts to apply the filter. The error log indicates the overlapping terms.



## How the Router Evaluates Terms in a Filter

The router creates a table of match conditions when examining terms. The table, which is similar to a routing table, is based on the conditions included in the **match-order** statement. When the router receives a packet, the router examines the packet's contents in the sequence specified in the **match-order** statement.

For example, using the sample configuration in the following Match-Order Example, the router first examines the packet's **source-address**, then the **destination-address**, and finally the **destination-port**. As shown in the following table, the two terms in the filter do not overlap because each term has a different **destination-port** specification. The router then takes the appropriate filter action for the term that matches the **destination-port** value of the packet.

Term	source-address	destination-address	destination-port	Action
t55	subscriber's address	3.1.1.2/32	http	count t55_cntr accept
t999	subscriber's address	3.1.1.2/32	https	count t999_cntr accept

### Match-Order Example

```

firewall {
  family inet {
    fast-update-filter psf1 {
      interface-specific;
      match-order [ source-address destination-address destination-port ];
      term t55 {
        from {
          source-address $junos-subscriber-ip-address;
          destination-address 3.1.1.2/32;
          destination-port http;
        }
        then {
          count t55_cntr;
          accept;
        }
      }
      term t999 {
        from {
          source-address $junos-subscriber-ip-address;
          destination-address 3.1.1.2/32;
          destination-port https;
        }
        then {
          count t999_cntr;
          accept;
        }
      }
    }
  }
}

```

}

## Using Implied Wildcards

This section shows an example of how you might use an implied wildcard specification in the match configuration. A condition in the **match-order** statement is an implied wildcard when that condition is not configured in the **from** specification of a term in the filter.



**NOTE:** When you use ranges (for example, a range of values or a wildcard) in terms, the ranges must not overlap—overlapping ranges create a conflict error. However, you can configure a range in one term and an exact match in another term. For example, in the following filter table, the wildcard destination port value in term **t3** does not overlap the destination port specifications in terms **t55** and **t999** because the **http** and **https** values are exact matches.

In the Implied Wildcard Example configuration, the router views the **destination-port** condition in the **match-order** statement as an implied wildcard for term **t3**, because there is no **destination-port** value configured in that term. As a result, the wildcard specifies that for term **t3** any **destination-port** value is accepted. The filter table appears as follows:

Term	source-address	destination-address	destination-port	Action
t3	subscriber's address	3.1.1.2/32	any (wildcard)	count t3_cntr accept
t55	subscriber's address	3.1.1.2/32	http	count t55_cntr accept
t999	subscriber's address	3.1.1.2/32	https	count t999_cntr accept

In the following filter configuration, traffic with a destination port of **http** matches term **t55** and traffic with a destination port of **https** matches term **t999**. Traffic with a destination port other than **http** or **https** matches term **t3**, which is the implied wildcard.

### Implied Wildcard Example

```
firewall {
  family inet {
    fast-update-filter psf1 {
      interface-specific;
      match-order [ source-address destination-address dscp protocol destination-port ];
      term t3 {
        from {
          source-address $junos-subscriber-ip-address;
          destination-address 3.1.1.2/32;
        }
        then {
```

```

        count t3_cntr;
        accept;
    }
}
term t55 {
    from {
        source-address $junos-subscriber-ip-address;
        destination-address 3.1.1.2/32;
        destination-port http;
    }
    then {
        count t55_cntr;
        accept;
    }
}
term t999 {
    from {
        source-address $junos-subscriber-ip-address;
        destination-address 3.1.1.2/32;
        destination-port https;
    }
    then {
        count t999_cntr;
        accept;
    }
}
}
}
```

Conflict Caused by Overlapping Ranges

This section shows two examples of overlapping ranges in terms. When you use ranges (such as a wildcard or a range of values) in terms, the ranges must not overlap—overlapping ranges create a conflict error and the session fails.

In the following filter configuration, the **destination-port** ranges in the two terms overlap. Ports in the range from 50 through 80 match both term **src0** and term **src1**, which each specify different actions to take.



**NOTE:** You can configure a range in one term and an exact match in another term. See the section, *Using Implied Wildcards*, for an example that uses a wildcard for a match condition in one term and an exact match for the condition in a second term.

Term	source-address	destination-address	destination-port	Action
src0	subscriber's address	10.1.1.2/32	0–80	count c1_cntr accept

Term	source-address	destination-address	destination-port	Action
src1	subscriber's address	10.1.1.2/32	50–100	count c2_cntr accept

### Overlapping Ranges Example 1

```

firewall {
  family inet {
    fast-update-filter fuf-src {
      interface-specific;
      match-order [ source-address destination-address destination-port ];
      term src0 {
        from {
          source-address $junos-subscriber-ip-address;
          destination-address 10.1.1.2/32;
          destination-port 0–80;
        }
        then {
          count c1_cntr;
          accept;
        }
      }
      term src1 {
        from {
          source-address $junos-subscriber-ip-address;
          destination-address 10.1.1.2/32;
          destination-port 50–100;
        }
        then {
          count c2_cntr;
          accept;
        }
      }
    }
  }
}

```

In this filter configuration, the **protocol** specification in terms **src21** and **src22** use the implied wildcard, which configures a range for each term. Because overlapping ranges are not allowed, a conflict error results.

Term	source-address	destination-address	protocol	destination-port	Action
src20	subscriber's address	10.1.1.2/32	udp	any (wildcard)	count c20_cntr accept
src21	subscriber's address	10.1.1.2/32	any (wildcard)	http	count c21_cntr accept
src21	subscriber's address	10.1.1.2/32	any (wildcard)	https	count c22_cntr accept

### Overlapping Ranges Example 2

```

firewall {
  family inet {
    fast-update-filter fuf-src2 {
      interface-specific;
      match-order [ source-address destination-address protocol destination-port ];
      term src20 {
        from {
          source-address $junos-subscriber-ip-address;
          destination-address 10.1.1.2/32;
          protocol udp;
        }
        then {
          count c20_cntr;
          accept;
        }
      }
      term src21 {
        from {
          source-address $junos-subscriber-ip-address;
          destination-address 10.1.1.2/32;
          destination-port http;
        }
        then {
          count c21_cntr;
          accept;
        }
      }
      term src22 {
        from {
          source-address $junos-subscriber-ip-address;
          destination-address 10.1.1.2/32;
          destination-port https;
        }
        then {
          count c22_cntr;
          accept;
        }
      }
    }
  }
}

```

### Related Documentation

- [Configuring Fast Update Filters on page 581](#)
- [Configuring Terms for Fast Update Filters on page 583](#)
- [Configuring the Match Order for Fast Update Filters on page 582](#)

## Associating Fast Update Filters with Interfaces in a Dynamic Profile

After you configure the fast update filter, you reference the filter in the **interfaces** stanza of a dynamic profile. When the dynamic profile instantiates a subscriber session, the router applies the terms of the filter to the interface.

To apply a fast update filter to an interface in a dynamic profile:

1. Access the dynamic profile you want to use.

```
[edit]
user@host# edit dynamic-profiles myProfile
```

2. Specify the interface for the dynamic profile—use the dynamic interface variable.

```
[edit dynamic-profiles myProfile]
user@host# edit interfaces $junos-interface-ifd-name
```

3. Specify the underlying interface—use the unit number variable.

```
[edit dynamic-profiles myProfile interfaces "$junos-interface-ifd-name"]
user@host# edit unit $junos-underlying-interface-unit
```

4. Specify the family. Use `inet` if you are using IPv4 filters or `inet6` for IPv6 filters.

```
[edit dynamic-profiles myProfile interfaces "$junos-interface-ifd-name" unit
"$junos-underlying-interface-unit"]
user@host# edit family inet
```

5. Specify the filters that you want to apply to the interface.

```
[edit dynamic-profiles myProfile interfaces "$junos-interface-ifd-name" unit
"$junos-underlying-interface-unit" family inet]
user@host# set filter input httpFilter
user@host# set filter output myOutFilter
```

#### Related Documentation

- Dynamic Profiles Overview on page 369
- Configuring Static Subscriber Interfaces in Dynamic Profiles on page 439
- Associating Dynamic Profiles with Statically Created Interfaces on page 441
- Fast Update Filters Overview on page 564
- For information about firewall filters, see Guidelines for Configuring Standard Firewall Filters and Guidelines for Applying Standard Firewall Filters in the *Junos OS Firewall Filter and Policer Configuration Guide*.

---

## Verifying and Managing Firewall Filter Configuration

**Purpose** View or manage information for firewall filters:



**NOTE:** The router creates unique names for fast update filters and for filter terms and counters. See *Naming Fast Update Filters* in “Fast Update Filters Overview” on page 564 for information.

**Action** • To display statistics for firewall filters:

```
user@host> show firewall
```

- To display firewall log information:

```
user@host> show firewall log
```

- To clear filter counters:

```
user@host> clear firewall all
```

**Related  
Documentation**

- Classic Filters Overview on page 556
- Fast Update Filters Overview on page 564
- *[Junos OS Routing Protocols and Policies Command Reference](#)*





# Configuring Service Sets in Dynamic Profiles

- Associating Service Sets with Interfaces in a Dynamic Profile on page 595
- Verifying and Managing Service Sets Information on page 596

## Associating Service Sets with Interfaces in a Dynamic Profile

---

After you configure a service set, you use a dynamic profile to dynamically associate the service set with interfaces. You reference the filter in the **interfaces** stanza of a dynamic profile. When the dynamic profile instantiates a subscriber session, the router applies the terms of the filter to the interface.

To apply a service set to an interface in a dynamic profile:

1. Access the dynamic profile you want to use.

```
[edit]
user@host# edit dynamic-profiles myProfile
```

2. Specify the interface for the dynamic profile—use the dynamic interface variable.

```
[edit dynamic-profiles myProfile]
user@host# edit interfaces $junos-interface-ifd-name
```

3. Specify the underlying interface—use the unit number variable.

```
[edit dynamic-profiles myProfile interfaces "$junos-interface-ifd-name"]
user@host# edit unit $junos-underlying-interface-unit
```

4. Specify the family. Dynamic service sets are supported only on **family inet** (IPv4).

```
[edit dynamic-profiles myProfile interfaces "$junos-interface-ifd-name" unit
"$junos-underlying-interface-unit"]
user@host# edit family inet
```

5. Specify the input and output service sets that you want to apply to the interface.

```
[edit dynamic-profiles myProfile interfaces "$junos-interface-ifd-name" unit
"$junos-underlying-interface-unit" family inet]
user@host# set service input service-set inputService_200
user@host# set service input post-service-filter postService_15
user@host# set service output service-set outputService_320
```

- Related Documentation**
- Dynamic Service Sets Overview on page 569
  - Verifying and Managing Service Sets Information on page 596
  - For information about creating service sets, see “Service Set Configuration Guidelines” in the *Junos OS Services Interfaces Configuration Guide*.
  - For information about statically applying service sets to interfaces, see Applying Filters and Services to Interfaces in the *Junos OS Services Interfaces Configuration Guide*.

---

## Verifying and Managing Service Sets Information

---

**Purpose** View information for service sets:

- Action**
- To display summary information for service sets:  
`user@host> show services service-sets summary`
  - To display interface-specific information for service sets:  
`user@host> show services service-sets summary interface interface-name`

- Related Documentation**
- Dynamic Service Sets Overview on page 569
  - Associating Service Sets with Interfaces in a Dynamic Profile on page 595
  - *Junos OS System Basics and Services Command Reference*

# Firewall Filter Examples

- Examples: Configuring Static Filters on page 597
- Example: Configuring Dynamic Ascend-Data-Filter Support for Subscriber Access on page 600
- Example: Configuring Static Ascend-Data-Filter Support for Subscriber Access on page 603
- Example: Configuring Fast Update Filters for Subscriber Access on page 607
- Example: Bypassing Firewall Filters on page 608

## Examples: Configuring Static Filters

---

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 Documentation**
- Dynamically Attaching Statically Created Filters for Any Interface Type on page 572
  - Dynamically Attaching Statically Created Filters for a Specific Interface Family Type on page 571

## Example: Configuring Dynamic Ascend-Data-Filter Support for Subscriber Access

---

This example shows how to configure support for dynamic Ascend-Data-Filter policies.

- Requirements on page 600
- Overview on page 600
- Configuration on page 600
- Verification on page 601

### Requirements

- Ensure that the Ascend-Data-Filter has been configured on the RADIUS server.
- Create the dynamic profile. See “Dynamic Profiles Overview” on page 369.
- Configure RADIUS support. See “Configuring RADIUS Server Parameters for Subscriber Access” on page 26.

### Overview

Ascend-Data-Filters are configured on a RADIUS server, and contain rules that create policies. Subscriber management uses a dynamic profile to obtain the Ascend-Data-Filter attribute (RADIUS attribute 242) from the RADIUS server and apply the policy to a subscriber session.

- Specify the dynamic profile to use to apply the Ascend-Data-Filter policy to the subscriber session.
- Specify the Junos OS predefined variable that maps the Ascend-Data-Filter rules to Junos OS filter functionality.
- Configure optional settings, which include counting the rule usage and setting the precedence order for the filter.

### Configuration

#### Step-by-Step Procedure

To configure dynamic Ascend-Data-Filter support:

1. Specify the dynamic profile in which you want to include the Ascend-Data-Filter, and configure the interface, the logical unit number, and the family type.  
  
[edit]  
user@host# **edit dynamic-profiles adf-profile-v4 interfaces**  
          **\$junos-interface-ifd-name unit \$junos-underlying-interface-unit family inet**
2. Specify that you want to include an Ascend-Data-Filter in the dynamic profile and provide the Junos OS predefined variable as the rule that maps the Ascend-Data-Filter actions to Junos OS filter functionality.

```
[edit dynamic-profiles adf-profile-v4 interfaces "$junos-interface-ifd-name" unit
"$junos-underlying-interface-unit" family inet]
user@host# set filter adf rule $junos-adf-rule-v4
```

3. Enable the counter for the rule.

```
[edit dynamic-profiles adf-profile-v4 interfaces "$junos-interface-ifd-name" unit
"$junos-underlying-interface-unit" family inet]
user@host# set filter adf counter
```

4. Specify the precedence for received packets on the interface.

```
[edit dynamic-profiles adf-profile-v4 interfaces "$junos-interface-ifd-name" unit
"$junos-underlying-interface-unit" family inet]
user@host# set filter adf input-precedence 75
```

5. Specify the precedence for transmitted packets on the interface.

```
[edit dynamic-profiles adf-profile-v4 interfaces "$junos-interface-ifd-name" unit
"$junos-underlying-interface-unit" family inet]
user@host# set filter adf output-precedence 80
```

**Results** From configuration mode, confirm your configuration by entering the **show dynamic-profiles** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show dynamic-profiles
...
adf-profile-v4 {
  interfaces {
    "$junos-interface-ifd-name" {
      unit "$junos-underlying-interface-unit" {
        family inet {
          filter {
            adf {
              rule "$junos-adf-rule-v4";
              counter;
              input-precedence 75;
              output-precedence 80;
            }
          }
        }
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying that Dynamic Ascend-Data-Filter Rules Are Applied to Subscriber Sessions on page 601
- Verifying Dynamic Ascend-Data-Filter Usage on page 602

### Verifying that Dynamic Ascend-Data-Filter Rules Are Applied to Subscriber Sessions

**Purpose** Verify that the Ascend-Data-Filter rules were attached to the subscriber.

**Action** From operational mode, enter the **show subscribers extensive** command.

```
user@host>show subscribers extensive
Type: DHCP
User Name: user1-adf
IP Address: 192.168.1.10
IP Netmask: 255.255.255.0
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.0
Interface type: Static
Dynamic Profile Name: adf-profile-v4
MAC Address: 00:10:94:00:00:01
State: Active
Radius Accounting ID: 5
Login Time: 2010-08-12 14:06:27 PDT
ADF IPv4 Input Filter Name: __junos_adf_5-ge-1/0/0.0-inet-in
Rule 0: 010101000000000000d87f920000180000000000000000000000
      from {
        destination-address 216.127.146.0/24;
      }
      then {
        accept;
      }
Rule 1: 0100010000000000000000000000000000000000060000000001900020000
      from {
        protocol 6;
        destination-port 25;
      }
      then {
        discard;
      }
Rule 2: 01010100000000000000000000000000000000000000000000000000000
      then {
        accept;
      }
```

**Meaning** The output shows the information for the dynamic profile, including Ascend-Data-Filter rules. Verify the following information:

- The User Name field indicates the correct subscriber.
- The Dynamic Profile Name field is correct for the subscriber.
- The correct Ascend-Data-Filter rules are applied to the subscriber. The display shows the rules that are configured on the RADIUS server.

---

### Verifying Dynamic Ascend-Data-Filter Usage

---

**Purpose** Verify usage of the dynamic Ascend-Data-Filter. Counter statistics are displayed when the **counter** option is configured for the **adf** command in the dynamic profile.

**Action** From operational mode, enter the **show firewall** command.

```
user@host> show firewall
```



```

Filter: __junos_adf_5-ge-1/0/0.0-inet-in
Counters:
Name                Bytes      Packets
t0-cnt              32758      22
t1-cnt              22199      15
t2-cnt              21723      14

```

**Meaning** The output shows the name of the filter and lists the counter activity. If the **counter** option is not configured, the output displays only the filter name.

**Related Documentation**

- Ascend-Data-Filter Policies for Subscriber Management Overview on page 559
- Dynamically Applying Ascend-Data-Filter Policies to Subscriber Sessions on page 577

## Example: Configuring Static Ascend-Data-Filter Support for Subscriber Access

This example shows how to configure support for static Ascend-Data-Filter policies. In a static configuration, you manually configure the Ascend-Data-Filter as part of the dynamic profile configuration. This procedure differs from dynamic configuration, in which the Ascend-Data-Filter is defined on the RADIUS server and then subscriber management uses a predefined variable to map the Ascend-Data-Filter rules to Junos OS filter functionality. Because creating a static Ascend-Data-Filter configuration can be labor-intensive, you might typically use this method for testing purposes.

- Requirements on page 603
- Overview on page 603
- Configuration on page 604
- Verification on page 605

### Requirements

- Create the dynamic profile. See “Dynamic Profiles Overview” on page 369.
- Configure RADIUS support. See “Configuring RADIUS Server Parameters for Subscriber Access” on page 26.

### Overview

Ascend-Data-Filters contain rules that create policies. Subscriber management uses a dynamic profile to apply the policy to a subscriber session. You manually configure the Ascend-Data-Filter as part of the dynamic policy.

- Specify the dynamic profile to use to apply the Ascend-Data-Filter policy to the subscriber session.
- Configure the Ascend-Data-Filter.
- Configure optional settings, which include counting the rule usage and setting the precedence for received and transmitted traffic.

## Configuration

### Step-by-Step Procedure

To configure static Ascend-Data-Filter support:

1. Specify the dynamic profile in which you want to create the Ascend-Data-Filter, and configure the interface, the logical unit number, and the family type.  
  

```
[edit]
user@host# edit dynamic-profiles adf-profile-v4 interfaces
$junos-interface-ifd-name unit $junos-underlying-interface-unit family inet
```
2. Configure the Ascend-Data-Filter. Enclose the filter values within quotation marks. You can configure multiple Ascend-Data-Filter rules in the same dynamic profile.  
  

```
[edit dynamic-profiles adf-profile-v4 interfaces "$junos-interface-ifd-name" unit
"$junos-underlying-interface-unit" family inet]
user@host# set filter adf rule "01000100 0A020100 00000000 18000000
00000000 00000000"
```
3. Enable the counter for the rule.  
  

```
[edit dynamic-profiles adf-profile-v4 interfaces "$junos-interface-ifd-name" unit
"$junos-underlying-interface-unit" family inet]
user@host# set filter adf counter
```
4. Specify the precedence for received packets on the interface.  
  

```
[edit dynamic-profiles adf-profile-v4 interfaces "$junos-interface-ifd-name" unit
"$junos-underlying-interface-unit" family inet]
user@host# set filter adf input-precedence 80
```
5. Specify the precedence for transmitted packets on the interface.  
  

```
[edit dynamic-profiles adf-profile-v4 interfaces "$junos-interface-ifd-name" unit
"$junos-underlying-interface-unit" family inet]
user@host# set filter adf output precedence 85
```

**Results** From configuration mode, confirm your configuration by entering the **show dynamic-profiles** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show dynamic-profiles
...
adf-profile-v4 {
  interfaces {
    "$junos-interface-ifd-name" {
      unit "$junos-underlying-interface-unit" {
        family inet {
          filter {
            adf {
              rule "01000100 0A020100 00000000 18000000 00000000 00000000";
              counter;
              input-precedence 80;
              output-precedence 85;
            }
          }
        }
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

**Results** The Ascend-Data-Filter rule defined in Step 2 of the procedure configures an input policy that filters all packets from network 10.2.1.0 with wildcard mask 255.255.255.0 to any destination.

Table 53 on page 605 lists the values specified in the Ascend-Data-Filter rule.

**Table 53: Ascend-Data-Filter Rule**

Action or Classifier	Hex Value	Junos OS Filter Function
Type	01	IPv4
Forward	00	Forward
Indirection	01	Ingress
Spare	00	None
Source IP address	0a020100	10.2.1.0
Destination IP address	00000000	Any
Source IP mask	18	24 (255.255.255.0)
Destination IP mask	00	0 (0.0.0.0)
Protocol	00	None
Established	00	None
Source port	0000	None
Destination port	0000	None
Source port qualifier	00	None
Destination port qualifier	00	None
Reserved	0000	None

## Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying that Static Ascend-Data-Filter Rules are Applied to Subscriber Sessions on page 606
- Verifying Static Ascend-Data-Filter Usage on page 606

### Verifying that Static Ascend-Data-Filter Rules are Applied to Subscriber Sessions

**Purpose** Verify that the Ascend-Data-Filter rules you manually configured were attached to the subscriber.

**Action** From operational mode, enter the **show subscribers extensive** command.

```
user@host>show subscriber extensive
Type: DHCP
User Name: user1-adf
IP Address: 192.168.1.10
IP Netmask: 255.255.255.0
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.0
Interface type: Static
Dynamic Profile Name: adf-profile-v4
MAC Address: 00:10:94:00:00:01
State: Active
Radius Accounting ID: 5
Login Time: 2010-08-12 14:06:27 PDT
ADF IPv4 Input Filter Name: __junos_adf_5-ge-1/0/0.0-inet-in
Rule 0: 010001000A020100000000001800000000000000000000000000000000000000
      from {
        destination-address 10.2.1.0/24;
      }
      then {
        accept;
      }
```

**Meaning** The output shows the information for the dynamic profile, including Ascend-Data-Filter rules. Verify the following information:

- The User Name field indicates the correct subscriber.
- The Dynamic Profile Name field is correct for the subscriber.
- The correct static Ascend-Data-Filter rule is applied to the subscriber.

### Verifying Static Ascend-Data-Filter Usage

**Purpose** Verify usage of the static Ascend-Data-Filter. Counter statistics are displayed when the **counter** option is configured for the **adf** command in the dynamic profile.

**Action** From operational mode, enter the **show firewall** command.

```
user@host> show firewall

Filter: __junos_adf_5-ge-1/0/0.0-inet-in
Counters:
Name          Bytes      Packets
t0-cnt        32758      22
```

**Meaning** The output shows the name of the filter and the lists counter activity. If the **counter** option is not configured, the output displays only the filter name.

- Related Documentation**
- Ascend-Data-Filter Policies for Subscriber Management Overview on page 559
  - Dynamically Applying Ascend-Data-Filter Policies to Subscriber Sessions on page 577

## Example: Configuring Fast Update Filters for Subscriber Access

This example shows you how to configure a fast update filter that is an input filter that counts the HTTP and non-HTTP packets from a subscriber. In the example, you use the firewall stanza to create the filter and the interfaces stanza to attach the filter.

```
[edit dynamic-profiles myProfile]
firewall {
  family inet {
    fast-update-filter httpFilter {
      interface-specific;
      match-order [source-address protocol destination-port];
      term term1 {
        from {
          protocol tcp;
          source-address $junos-subscriber-ip-address;
          destination-port http;
        }
        then {
          count http-cnt;
        }
      }
      term term2 {
        from {
          protocol tcp;
          source-address $junos-subscriber-ip-address;
        }
        then {
          count non-http-cnt;
        }
      }
    }
  }
}
interfaces {
  "$junos-interface-ifd-name" {
    unit "$junos-underlying-interface-unit" {
      family inet {
        filter {
          input httpFilter;
        }
      }
    }
  }
}
```

- Related Documentation**
- Configuring Fast Update Filters on page 581

## Example: Bypassing Firewall Filters

This example describes how to configure multiple filters using the **service-filter-hit** match/action combination and contains the following sections:

- Before You Begin on page 608
- Filter Bypass Overview on page 608
- Configuring Filter Bypass on page 609

### Before You Begin

When using the **service-filter-hit** match/action combination, keep the following in mind:

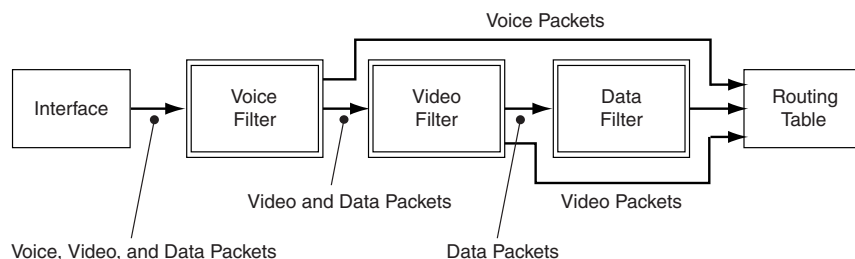
- The order in which the filters are applied is important. You can ensure the order in which the filters are processed by specifying a filter precedence value for the interface. See “Defining Dynamic Filter Processing Order” on page 574 for more information about dynamic filter processing and how to use the **precedence** statement.
- The following example uses policers to further define the match conditions each filter uses. These filters are not described here. To better understand how to configure policers, see “Statement Hierarchy for Configuring Policers” in the *Junos OS Routing Policy Configuration Guide*.

### Filter Bypass Overview

Packets must pass through each filter in a chain. However, if you create a chain of filters to process different types of packets (for example, voice, video, and data packets), you can streamline the filter process, decreasing the amount of packet handling for each filter in the chain, effectively bypassing unnecessary filters, by using the **service-filter-hit** match/action combination at the `[edit firewall family family-name filter filter-name term term-name]` hierarchy level.

Figure 12 on page 608 shows the logical processing flow through a chain of three filters (voice, video, and data) where only processing for a specific data type is desired. This configuration example shows an ingress filter flow. Though subsequent ingress filters in a chain can detect whether the **service-filter-hit** action is set, egress filters do not. To bypass egress filters, you must also configure the **service-filter-hit** match/action combination on those filters.

**Figure 12: Logical Flow Example for Filter Bypass Processing**



9017470

## Configuring Filter Bypass

- Configuring the Voice Filter on page 609
- Configuring the Video Filter on page 609
- Configuring the Data Filter on page 610

### CLI Quick Configuration

To quickly configure this example:

```
[edit]
set firewall filter voice term T1 from address 1.1.1.1/32
set firewall filter voice term T1 from source-port 5004-5005
set firewall filter voice term T1 then forwarding-class assured-forwarding service-filter-hit
  accept
set firewall filter voice term default then accept
set firewall filter video term T1 from service-filter-hit
set firewall filter video term T1 then accept
set firewall filter video term T2 from source-address 10.10.10.10/32
set firewall filter video term T2 then policer video-policer service-filter-hit accept
set firewall filter video term default then accept
set firewall filter data term T1 from service-filter-hit
set firewall filter data term T1 then accept
set firewall filter data term T2 then policer data-policer service-filter-hit accept
```

### Configuring the Voice Filter

#### Step-by-Step Procedure

To configure the voice filter for the logical flow in Figure 12 on page 608:

1. Configure the filter to apply the assured forwarding class and set the **service-filter-hit** action for traffic from a specific address and port range (over which voice traffic is expected).

```
[edit]
set firewall filter voice term T1 from address 1.1.1.1/32
set firewall filter voice term T1 from source-port 5004-5005
set firewall filter voice term T1 then forwarding-class assured-forwarding
  service-filter-hit accept
```

2. Configure the filter default action to pass (accept) packet traffic from any other address or port range.

```
[edit]
set firewall filter voice term default then accept
```

### Configuring the Video Filter

#### Step-by-Step Procedure

To configure the video filter for the logical flow in Figure 12 on page 608:

1. Configure the filter to pass (accept) incoming packets that are tagged by the **service-filter-hit** action.

```
[edit]
set firewall filter video term T1 from service-filter-hit
set firewall filter video term T1 then accept
```

2. Configure the filter to apply a video policer and set the **service-filter-hit** action for traffic from a specific address (over which video traffic is expected).

```
[edit]
set firewall filter video term T2 from source-address 10.10.10.10/32
set firewall filter video term T2 then policer video-policer service-filter-hit accept
```

3. Configure the filter default action to pass (accept) packet traffic from any other address or port range.

```
[edit]
set firewall filter video term default then accept
```

---

### Configuring the Data Filter

#### Step-by-Step Procedure

To configure the data filter for the logical flow in Figure 12 on page 608:

1. Configure the filter to pass (accept) incoming packets that are tagged by the **service-filter-hit** action.

```
[edit]
set firewall filter data term T1 from service-filter-hit
set firewall filter data term T1 then accept
```

2. Configure the filter to apply a data policer and set the **service-filter-hit** action for traffic from a specific address (over which video traffic is expected).

```
[edit]
set firewall filter data term T2 then policer data-policer service-filter-hit accept
```

**Results** Display the results of the configuration:

```
[edit firewall]
user@host# show
filter voice {
  term T1 {
    from {
      address {
        1.1.1.1/32;
      }
      source-port 5004-5005;
    }
    then {
      forwarding-class assured-forwarding;
      service-filter-hit;
      accept;
    }
  }
  term default {
    then accept;
  }
}
filter video {
  term T1 {
    from {
      service-filter-hit;
    }
    then accept;
  }
  term T2 {
```



```
    from {
      source-address {
        10.10.10.10/32;
      }
    }
    then {
      policer video_policer;
      service-filter-hit;
      accept;
    }
  }
  term default {
    then accept;
  }
}
filter data {
  term T1 {
    from {
      service-filter-hit;
    }
    then accept;
  }
  term T2 {
    then {
      policer data_policer;
      service-filter-hit;
      accept;
    }
  }
}
```

**Related  
Documentation**

- [Classic Filters Overview on page 556](#)
- [Defining Dynamic Filter Processing Order on page 574](#)
- [Statement Hierarchy for Configuring Policers](#)
- [Configuring Firewall Filter Bypass on page 575](#)



# Redirecting HTTP Requests Overview

- Redirecting HTTP Requests on page 613

## Redirecting HTTP Requests

---

HTTP request traffic from subscribers is aggregated from access networks onto a Broadband and Remote Access Server (B-RAS) router, where HTTP traffic can be intercepted and redirected to a captive portal. A captive portal provides authentication and authorization services for redirected subscribers before granting access to protected servers outside of a walled garden. A walled garden defines a group of servers where access is provided to subscribers without reauthorization through a captive portal. You can use a captive portal page as the initial page a subscriber sees after logging in to a subscriber session and as a page used to receive and manage HTTP requests to unauthorized Web resources.

The HTTP redirect service implements a data handler and a control handler and registers them with service rules applicable to the HTTP applications. These rules are parsed by the captive-portal-content-delivery daemon on the routing engine. The data handler applies the rules to HTTP data flows and handles rewriting the IP destination address or sending an HTTP 302 response with a preconfigured redirect URL. In addition, the control handler maintains a connection with the captive-portal-content-delivery daemon on the routing engine to learn configuration changes, such as the redirect URL and the rewrite IP destination and port pair. To achieve faster performance, the control handler maintains a cache of relevant configured entities, such as URLs on Multiservices DPC.

Packet flow differs depending on the following configurations:

- Walled garden as a service filter—HTTP traffic destined to servers within the walled garden does not flow to Multiservices DPC. However, any HTTP traffic destined outside of the walled garden flows to the Multiservices DPC.
- Walled garden as an HTTP policy term—All HTTP traffic flows to the Multiservices DPC. The HTTP service handler determines whether traffic is allowed to go to a walled garden.
- HTTP request packet—If the flow is destined to servers within the walled garden, no action is taken.

You can implement HTTP redirect requests using either a remote server or a local server.

An HTTP redirect service can be attached to either a static or dynamic interface. For dynamic subscriber management, HTTP services can be attached dynamically at subscriber login or by using a change of authorization (CoA).

**Related  
Documentation**

- [Configuring a Basic Dynamic Profile on page 391](#)
- [Configuring a Dynamic Profile for Various Levels of Services on page 397](#)
- [Junos OS Predefined Variables on page 372](#)
- [Associating Service Sets with Interfaces in a Dynamic Profile on page 595](#)

# Configuring HTTP Redirect

- Configuring HTTP Redirect Services on page 615
- Verifying HTTP Redirect Requests on page 618

## Configuring HTTP Redirect Services

---

You can configure a walled garden with services and policies.

To configure the HTTP redirect service:

1. Configure the packet and installation.

```
[edit chassis]
fpc 1 {
  pic 0 {
    adaptive-services {
      service-package {
        extension-provider {
          control-cores 1;
          data-cores 7;
          object-cache-size 1024;
          policy-db-size 64;
          package jservices-cpcd;
          syslog {
            daemon any;
            external any;
          }
        }
      }
    }
  }
}
```

2. Configure the units and assign the VLAN IDs.

```
[edit interfaces]
ge-0/0/1 {
  vlan-tagging;
  unit 1 {
    vlan-id 100;
    family inet {
      address 100.20.1.1/24;
    }
  }
}
```

```
    }  
  }
```

3. Configure the policy options.

```
  policy-options {  
    prefix-list google {  
      74.125.19.0/24;  
    }  
  }
```

4. Configure the service options.

```
  firewall {  
    family inet {  
      service-filter walled {  
        term google {  
          from {  
            destination-prefix-list {  
              google;  
            }  
          }  
          then skip;  
        }  
        term http {  
          from {  
            destination-port [ 80 8080 443 ];  
          }  
          then service;  
        }  
        term skip {  
          then skip;  
        }  
      }  
      service-filter fromSRC {  
        term SRC {  
          from {  
            source-address {  
              10.1.2.3/32;  
            }  
            source-port 8800;  
          }  
          then service;  
        }  
        term skip {  
          then skip;  
        }  
      }  
      service-filter test {  
        term t1 {  
          from {  
            protocol icmp;  
          }  
          then service;  
        }  
      }  
    }  
  }
```

```
}

```

5. Configure the captive portal content delivery services.

```
services {
  captive-portal-content-delivery {
    rule test {
      match-direction input;
      term t1 {
        then {
          rewrite;
        }
      }
    }
    profile ipda-rewrite {
      cpcdd-rules test;
      ipda-rewrite-options {
        destination-address 10.1.2.3;
        destination-port 8800;
      }
    }
    traceoptions {
      file cpcdd;
      flag all;
    }
  }
  service-set sset1 {
    captive-portal-content-delivery-profile ipda-rewrite;
    interface-service {
      service-interface ms-1/0/0;
    }
  }
  stateful-firewall {
    rule Rule1 {
      match-direction input-output;
      term 1 {
        from {
          applications [ junos-icmp-all junos-dhcp-server junos-tftp junos-http ];
        }
        then {
          accept;
        }
      }
      term 2 {
        from {
          applications SRC;
        }
        then {
          accept;
        }
      }
    }
  }
}
```

6. Configure the applications.

```
applications {  
  application SRC {  
    protocol tcp;  
    destination-port 8800;  
  }  
}
```

**Related Documentation**

- [Redirecting HTTP Requests on page 613](#)

---

## Verifying HTTP Redirect Requests

---

**Purpose** View information and statistics for the HTTP redirect configuration.

**Action**

- To display services statistics:

```
user@host> show services captive-portal-content-delivery statistics
```

- To display services flows:

```
user@host> show services captive-portal-content-delivery flows
```

- To clear services statistics:

```
user@host> clear services captive-portal-content-delivery statistics
```



# HTTP Redirect Examples

- Example: Walled Garden as a Service Filter on page 619
- Example: Walled Garden as an HTTP Service Rule on page 620
- Example: HTTP Service Within a Service Set on page 620
- Example: HTTP Service Attached to a Static Interface on page 621
- Example: HTTP Service Attached to a Dynamic Interface on page 621

## Example: Walled Garden as a Service Filter

---

Service filters are configured under the firewall and are not specific to captive portal content delivery. The following example shows a walled garden with one server, which is the captive portal:

```
[edit firewall family inet]
root@host# show
service-filter walled {
  term 1 {
    from {
      destination-address {
        100.20.2.3/32; ## this is the address of captive portal
      }
      destination-port 80;
    }
    then skip; ## skip service DPC for http traffic
    ## destined to captive portal
  }
}
```

The following example shows a walled garden within a subnet:

```
service-filter walled-net {
  term 2 {
    from {
      destination-prefix-list {
        100.20.2.0/24; ## '100.20.2.0/24' is not defined
      }
    }
    then skip;
  }
}
```

## Example: Walled Garden as an HTTP Service Rule

---

HTTP service rule configuration resides under the services hierarchy and uses the captive portal and content delivery (cpd) service. The following example shows a walled garden configured as an HTTP service rule:

```
[edit services captive-portal-content-delivery]
rule walled-garden {
  match-direction input-output
  term 1 {
    from {
      destination-address 100.20.2.3/32; ## captive portal
      destination-port 80;
    }
    then {
      accept;
    }
  }
}
```

When a remote HTTP redirect server is used, you need to configure an HTTP service rule to rewrite the IP-DA of incoming HTTP requests on the service router so that the requests reach the remote HTTP redirect server before being redirected to a captive portal. If the destination port is not specified, the default behavior is determined by the rewrite configuration. If no rewrite configuration is available, the destination port is not rewritten. The following example shows a configuration for IP-DA rewrite:

```
[edit services captive-portal-content-delivery]
rule ipda-rewrite {
  match-direction input-output;
  term 1 {
    from {
      applications junos-http;
    }
    then {
      rewrite destination-address 100.20.2.10; # this is the remote
      # redirect server.
    }
  }
}
```

## Example: HTTP Service Within a Service Set

---

To become part of a service set, you must configure an HTTP service rule under a service set. In the following example, you can use http-service as an option in the service order configuration:

```
[edit services]
service-set http-redirect-walled {
  cpd-rules walled-garden;
  cpd-rules redirect;
}
```

You can also put rules in a rule set and then configure the service set as in the following example:

```
[edit services]
service-set http-redirect-walled {
  cpcd-rule-sets redirect-with-walled-garden;
}
```

## Example: HTTP Service Attached to a Static Interface

The following example shows an HTTP service set attached to a static interface:

```
[edit interfaces ge-1/0/1]
root@hostr# show
unit 0 {
  family inet {
    service {
      input {
        service-set http-redirect-walled;
      }
      output {
        service-set http-redirect-walled;
      }
    }
  }
  address 10.1.3.2/24;
}
```

The following example uses a service filter as a walled garden by configuring the service set and then attaching it:

```
[edit services]
service-set http-redirect {
  cpcd-rules redirect;
}

[edit interfaces ge-1/0/1]
unit 0 {
  family inet {
    service {
      input {
        service-set http-redirect service-filter walled;
      }
      output {
        service-set http-redirect;
      }
    }
  }
  address 10.1.3.2/24;
}
```

## Example: HTTP Service Attached to a Dynamic Interface

A dynamic service attachment uses a dynamic profile. In the following dynamic profile example, the name of the service set can be populated dynamically for each subscriber

at instantiation time. This dynamic profile encapsulates a service attachment point associated with a statically preprovisioned service set sset-1.

```
dynamic-profiles {
  profile prof-2 { # parameterized service attachment
    interfaces {
      $junos-interface-ifd-name {
        unit $junos-interface-unit {
          family inet {
            service {
              input {
                service-set $junos-service-set service-filter $junos-service-filter;
                post-input-filter $junos-post-input-filter ;
              }
              output {
                service-set $junos-service-set;
              }
            }
          }
        }
      }
    }
  }
}
```

To handle scalability more efficiently, in the following example the name of the service set can be populated dynamically for each subscriber at instantiation time.

```
dynamic-profiles {
  profile prof-2 { # parameterized service attachment
    interfaces {
      $junos-interface-ifd-name {
        unit $junos-interface-unit {
          family inet {
            service {
              input {
                service-set $junos-service-set service-filter $junos-service-filter;
                post-input-filter $junos-post-input-filter ;
              }
              output {
                service-set $junos-service-set;
              }
            }
          }
        }
      }
    }
  }
}
```

## PART 13

# Subscriber Secure Policy Traffic Mirroring

- Subscriber Secure Policy Overview on page 625
- Configuring RADIUS-Flow-Tap Service Support for Subscriber Secure Policy Mirroring on page 631
- Configuring RADIUS-Initiated Subscriber Secure Policy Traffic Mirroring on page 635
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring on page 641
- Subscriber Secure Policy Mirroring and SNMP Traps on page 645
- Subscriber Secure Policy Mirroring Examples on page 649



# Subscriber Secure Policy Overview

- Subscriber Secure Policy Overview on page 625
- Subscriber Secure Policy and L2TP LAC Subscribers on page 627
- Subscriber Secure Policy Licensing Requirements on page 628
- Subscriber Secure Policy Traffic Mirroring Architecture on page 628

## Subscriber Secure Policy Overview

---

Subscriber secure policy enables you to configure traffic mirroring on a per-subscriber basis. Subscriber secure policy mirroring can be based on information provided by either RADIUS or Dynamic Tasking Control Protocol (DTCP), and can mirror both IPv4 or IPv6 traffic.

Configuration of subscriber secure policy mirroring is independent of the actual mirroring session—you can configure the mirroring parameters at any time. Also, you can use a single RADIUS or DTCP 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.

After subscriber secure policy is triggered, both the subscriber 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. The actual mirroring operation is transparent to subscribers whose traffic is being mirrored. 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.



**NOTE:** If both RADIUS-initiated and DTCP-initiated mirroring are configured for the same subscriber prior to login, the RADIUS-initiated configuration takes precedence. If both mirroring methods are configured for in-session mirroring, the first method that is triggered is used, and the other method is ignored.

---

Subscriber secure policy also supports the use of SNMPv3 traps to report mirroring information to an external device. The traps map to messages defined in the *Lawfully*

*Authorized Electronic Surveillance (LAES) for IP Network Access, American National Standard for Telecommunications.*

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. Subscriber secure policy mirroring is particularly useful for large networks, in which you can use a single RADIUS or DTCP server to provision the mirroring operation.

The following list provides information about RADIUS-initiated and DTCP-initiated mirroring::

- 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. 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 login—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.
- DTCP-initiated mirroring creates secure policies based on DTCP attributes to mirror traffic for the subscriber. The attributes in a DTCP ADD message trigger the router to start mirroring traffic and specify the interface on which the mirroring takes place. The following list describes the types of DTCP-initiated mirroring:
  - Subscriber login—If the DTCP ADD message with the trigger has been previously received, the subscriber traffic on the specified interface is then mirrored when the subscriber logs in.
  - In-session—If the subscriber is already logged in, the mirroring operation starts when the trigger is received in the DTCP ADD message.

## Subscriber Secure Policy Terms

Table 54 on page 626 defines terms that are used in the discussion of subscriber secure policy.

**Table 54: Subscriber Secure Policy Terms**

Term	Definition
DTCP	Dynamic Tasking Control Protocol.



Table 54: 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. Subscriber secure policy mirrors both IPv4 and IPv6 traffic.
Mirror trigger	RADIUS or DTCP 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	System on which the subscriber secure policy service (and the radius-flow-tap service) is configured.

**Related  
Documentation**

- Subscriber Secure Policy Traffic Mirroring Architecture on page 628
- RADIUS Attributes Used for Subscriber Secure Policy on page 636
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 635
- SNMP Traps for Subscriber Secure Policy LAES Compliance on page 645
- Subscriber Secure Policy Licensing Requirements on page 628

## Subscriber Secure Policy and L2TP LAC Subscribers

RADIUS-initiated per-subscriber traffic mirroring can be applied to subscribers whose traffic is tunneled with L2TP. Both subscriber ingress traffic (from the subscriber into the tunnel) and subscriber egress traffic (from the tunnel to the subscriber) are mirrored at the (subscriber-facing) ingress interface on the LAC. The ingress traffic is mirrored after PPPoE decapsulation and before L2TP encapsulation. The egress traffic is mirrored after L2TP decapsulation. The mirrored packet includes the complete HDLC frame sent to the LNS rather than only the IP datagram.

**Related  
Documentation**

- Subscriber Secure Policy Overview on page 625
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 635
- RADIUS Attributes Used for Subscriber Secure Policy on page 636

## Subscriber Secure Policy Licensing Requirements

To enable and use subscriber secure policy, you must install and properly configure the Subscriber Secure Policy license.

- Related Documentation**
- For information about installing and managing Junos licenses, see the “Installing and Managing Junos Licenses” chapter of the *Junos OS Installation and Upgrade Guide*

## 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 13 on page 628 illustrates the RADIUS-initiated subscriber secure policy mirroring environment (in DTCP-initiated mirroring, the DTCP client performs the mirroring-related operations shown for the RADIUS server in the figure).

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 55 on page 629 describes the configuration sequence. Table 56 on page 629 and Table 57 on page 629 describe the sequence of events that occur during mirroring operations.

**Figure 13: RADIUS-Initiated Subscriber Secure Policy Architecture**

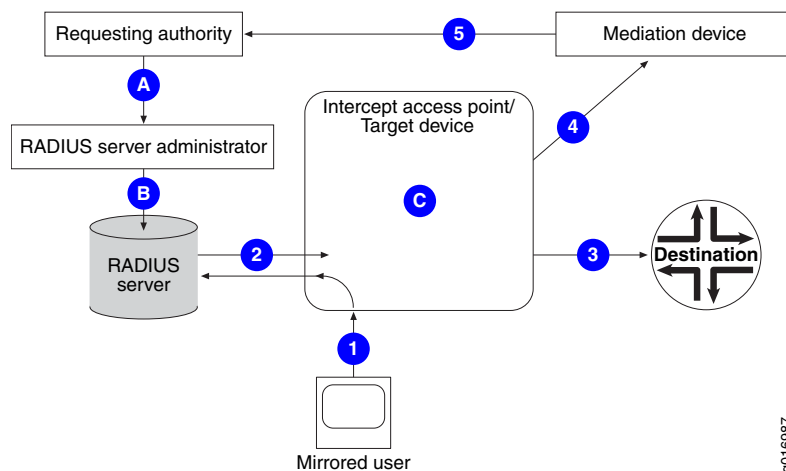


Table 55 on page 629 lists the high-level steps that are required to configure the subscriber secure policy traffic mirroring environment.

**Table 55: Subscriber Secure Policy Configuration Steps**

Step	Description
<b>A</b>	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>B</b>	<ul style="list-style-type: none"> <li>For RADIUS-initiated mirroring, the RADIUS server administrator configures the subscriber RADIUS record to include the mirroring-related RADIUS attributes and VSAs.</li> <li>For DTCP-initiated mirroring, the DTCP server administrator configures the DTCP ADD message to include the DTCP mirroring-related attributes.</li> </ul>
<b>C</b>	The Juniper Networks router administrator configures the subscriber secure policy service on the router, including the radius-flow-tap service configuration, RADIUS or DTCP server information, and mediation device information.

### RADIUS-Initiated Traffic Mirroring Process

Table 56 on page 629 shows the process for a RADIUS-initiated subscriber login mirroring operation, which is initiated when the mirrored subscriber logs in. Table 57 on page 629 shows the procedure for a RADIUS-initiated in-session mirroring operation, in which the subscriber is already logged in.

**Table 56: RADIUS-Initiated Mirroring at Subscriber Login**

Step	Description
<b>1</b>	The subscriber logs in, requesting authentication by the RADIUS server.
<b>2</b>	<ul style="list-style-type: none"> <li>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).</li> <li>The mirroring trigger in the RADIUS Access-Accept message initiates the mirroring operation.</li> <li>The intercept access point creates the subscriber secure policy based on the mirroring VSAs and begins mirroring the subscriber's traffic.</li> </ul>
<b>3</b>	The intercept access point sends the original subscriber traffic to its intended destination.
<b>4</b>	The intercept access point sends the mirrored subscriber traffic to the mediation device.
<b>5</b>	The mediation device provides information about the mirrored traffic to the requesting authority.

**Table 57: RADIUS-Initiated Mirroring for Current Subscriber**

Step	Description
<b>1</b>	The subscriber logs in, requesting authentication by the RADIUS server. The RADIUS server authenticates the subscriber (no mirroring activity occurs).

Table 57: RADIUS-Initiated Mirroring for Current Subscriber (*continued*)

Step	Description
2	<ul style="list-style-type: none"> <li>Subscriber-based mirroring is later requested by the requesting authority and then enabled on the RADIUS server.</li> <li>The RADIUS server sends a CoA message containing the mirroring-related RADIUS attributes and VSAs to the router (intercept access point).</li> <li>The mirroring trigger in the RADIUS CoA message initiates the mirroring operation.</li> <li>The intercept access point creates the subscriber secure policy based on the mirroring VSAs and immediately begins mirroring subscriber traffic.</li> </ul>
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.

### DTCP-Initiated Traffic Mirroring Process

Table 58 on page 630 shows the process for a DTCP-initiated mirroring operation.

Table 58: DTCP-Initiated Traffic Mirroring

Step	Description
1	<ul style="list-style-type: none"> <li>The DTCP client sends the ADD message containing the mirroring-related attributes to the router, which functions as the intercept access point and the DTCP server. <ul style="list-style-type: none"> <li>If the DTCP ADD is received before the subscriber logs in, the traffic mirroring begins when the subscriber subsequently logs in.</li> <li>If the DTCP ADD is received after the subscriber has logged in, the traffic mirroring begins when the ADD is received.</li> </ul> </li> <li>The intercept access point creates the subscriber secure policy based on the mirroring attributes, then begins mirroring traffic for subscribers currently logged in, and mirrors traffic for subscribers that log in in the future.</li> </ul>
2	The intercept access point sends the original subscriber traffic to its intended destination.
3	The intercept access point sends the mirrored subscriber traffic to the mediation device.
4	The mediation device provides information about the mirrored traffic to the requesting authority.

#### Related Documentation

- Subscriber Secure Policy Overview on page 625
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 635

# Configuring RADIUS-Flow-Tap Service Support for Subscriber Secure Policy Mirroring

- Guidelines for Configuring Subscriber Secure Policy Mirroring on the RADIUS-Flow-Tap Service on page 631
- Configuring RADIUS-Flow-Tap Service Support for Subscriber Secure Policy Mirroring on page 632

## Guidelines for Configuring Subscriber Secure Policy Mirroring on the RADIUS-Flow-Tap Service

---

The subscriber secure policy service runs on the radius-flow-tap service infrastructure. When configuring subscriber secure policy mirroring, consider the following guidelines regarding the relationship between subscriber secure policy service and the radius-flow-tap service:

- Subscriber secure policy inherits the limitations of the flow-tap service. For example, the radius-flow-tap service 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 radius-flow-tap service on the router. Both subscriber secure policy RADIUS-initiated mirroring and DTCP-initiated mirroring use the radius-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 radius-flow-tap service configuration while a subscriber secure policy mirroring session is active on the service.

### Related Documentation

- Subscriber Secure Policy Overview on page 625
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 635
- Configuring RADIUS-Flow-Tap Service Support for Subscriber Secure Policy Mirroring on page 632

## Configuring RADIUS-Flow-Tap Service Support for Subscriber Secure Policy Mirroring

Subscriber secure policy runs on the radius-flow-tap service. This topic describes the steps to configure radius-flow-tap support for RADIUS-initiated and DTCP-initiated subscriber secure policy mirroring.

To configure the radius-flow-tap service to support subscriber secure policy mirroring:

1. At the [edit chassis] hierarchy level, allocate a pool of tunnel interfaces for the radius-flow-tap service to 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 slot-number pic number tunnel-services bandwidth bandwidth**

2. At the [edit interfaces] hierarchy level, configure the tunnel interfaces, including the family.

[edit interfaces]

user@host# **set interface-name family family**

3. At the [edit services] hierarchy level, assign the tunnel interfaces that the radius-flow-tap service uses for subscriber secure policy mirroring.

[edit services]

user@host# **set radius-flow-tap interfaces interface-name**



**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.

4. At the [edit services] hierarchy level, specify the source IP address that the radius-flow-tap service uses for 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 ipv4-address**

5. (Optional) At the [edit services] hierarchy level, 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 class-name
```

**Related  
Documentation**

- Subscriber Secure Policy Overview on page 625
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 635
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview on page 641
- Guidelines for Configuring Subscriber Secure Policy Mirroring on the RADIUS-Flow-Tap Service on page 631





# Configuring RADIUS-Initiated Subscriber Secure Policy Traffic Mirroring

- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 635
- RADIUS Attributes Used for Subscriber Secure Policy on page 636
- Configuring RADIUS Server Support for Subscriber Secure Policy Mirroring on page 639
- Subscriber Secure Policy Mirroring Session Termination on page 639

## Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview

---

You can configure RADIUS-initiated subscriber secure policy mirroring to mirror the traffic of a particular subscriber.



**NOTE:** Subscriber secure policy RADIUS-initiated mirroring runs on the radius-flow-tap service infrastructure. To configure the subscriber secure policy service, you must have the same privileges that are required to configure the radius-flow-tap service.

To configure the subscriber secure policy service:

1. Configure the radius-flow-tap service support for secure subscriber policy. 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 RADIUS-Flow-Tap Service Support for Subscriber Secure Policy Mirroring” on page 632.

2. 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 639.

See “Using RADIUS Dynamic Requests for Subscriber Access Management” on page 34.

3. 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 636 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.

4. (Optional) Configure SNMPv3 trap support to report mirroring information to an external device.

See “Configuring SNMPv3 Traps for Subscriber Secure Policy Mirroring” on page 646.

5. You can terminate an active subscriber mirroring session at any time.

See “Subscriber Secure Policy Mirroring Session Termination” on page 639.



**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 Gbps of actual user data.

---

**Related Documentation**

- RADIUS Attributes Used for Subscriber Secure Policy on page 636
- Subscriber Secure Policy Mirroring and SNMP Traps on page 645
- Subscriber Secure Policy Mirroring Session Termination on page 639
- Example: Subscriber Secure Policy Mirroring Using RADIUS on page 649

---

## 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 59 on page 637 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 60 on page 637 must be included in the mirrored subscriber's RADIUS record.

## RADIUS Attributes Used as Traffic Mirroring Triggers

Table 59 on page 637 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 59: 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 60 on page 637 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).

**Table 60: RADIUS-Based Mirroring Attributes**

Attribute Number	Attribute Name	Description	Value
[26-58]	LI-Action	Traffic mirroring action	<ul style="list-style-type: none"> <li>0 = stop mirroring</li> <li>1 = start mirroring</li> <li>2 = no action</li> </ul>
[26-59]	Med-Dev-Handle	Identifier that associates mirrored traffic to a specific subscriber.	Salt-encrypted string
[26-60]	Med-Ip-Address	IP address of mediation device to which mirrored traffic is forwarded	Salt-encrypted IP address

Table 60: RADIUS-Based Mirroring Attributes (*continued*)

Attribute Number	Attribute Name	Description	Value
[26-61]	Med-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 369 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 61 on page 638.

Table 61: 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
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 Documentation

- Subscriber Secure Policy Overview on page 625
- Subscriber Secure Policy Traffic Mirroring Architecture on page 628
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 635
- Dynamic Profiles Overview on page 369
- Example: Subscriber Secure Policy Mirroring Using RADIUS on page 649

- Example: Subscriber Secure Policy Dynamic Profile on page 403

## 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 profile-name
```

2. Specify RADIUS as the authentication method.

```
[edit access profile profile-name]
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 profile-name]
user@host# set radius authentication-server ip-address
```

4. Specify the secret to use when communicating with the RADIUS server.

```
[edit access profile profile-name]
user@host# set radius-server server-address secret password
```

5. Specify other optional RADIUS configuration settings as needed, such as accounting support.

### Related Documentation

- Subscriber Secure Policy Overview on page 625
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 635
- RADIUS Attributes Used for Subscriber Secure Policy on page 636

## Subscriber Secure Policy Mirroring Session Termination

This topic describes how subscriber secure policy mirroring operations are terminated.

Mirroring sessions are terminated by the following actions:

- RADIUS CoA message receipt—RADIUS-initiated mirroring is terminated upon receipt of a CoA message with the VSA 26-58 (LI-Action) value of 0. The RADIUS administrator configures the LI-Action of 0 in the mirrored subscriber's RADIUS record.
- DTCP DELETE message receipt—DTCP-initiated mirroring is terminated upon receipt of a DTCP DELETE message. The DTCP administrator configures the DELETE message to include the same mirroring attributes that are used in the ADD message to initiate mirroring.

- Subscriber logout—Both RADIUS and DTCP mirroring for a subscriber are terminated when the mirrored subscriber logs out.
- Session timeout—Both RADIUS and DTCP mirroring for a subscriber are terminated when the current subscriber session times out.
- Session disconnect—Both RADIUS and DTCP mirroring for a subscriber are terminated when the current subscriber session is disconnected.

**Related  
Documentation**

- Subscriber Secure Policy Overview on page 625
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 635
- RADIUS Attributes Used for Subscriber Secure Policy on page 636
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview on page 641
- DTCP Attributes Used for Subscriber Secure Policy on page 644

# Configuring DTCP-Initiated Subscriber Secure Policy Mirroring

- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview on page 641
- Configuring DTCP Support for Subscriber Secure Policy Mirroring on page 642
- DTCP Attributes Used for Subscriber Secure Policy on page 644

## Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview

---

You can configure DTCP-initiated subscriber secure policy mirroring to mirror subscriber traffic.



**NOTE:** DTCP-initiated subscriber secure policy mirroring runs on the radius-flow-tap service infrastructure. To configure the subscriber secure policy service, you must have the same privileges that are required to configure the radius-flow-tap service.

To configure DTCP-initiated subscriber secure policy service:

1. Configure the radius-flow-tap service support for secure subscriber policy. 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 RADIUS-Flow-Tap Service Support for Subscriber Secure Policy Mirroring” on page 632.
2. Configure the DTCP support for subscriber secure policy. This support includes configuring the DTCP-over-SSH service that provides an extra level of security for DTCP transactions.  
  
See “Configuring DTCP Support for Subscriber Secure Policy Mirroring” on page 642.
3. Ensure that the following support is also configured:
  - The DTCP ADD message of the mirrored interface must include the DTCP attributes required for subscriber secure policy mirroring. See “DTCP Attributes Used for

Subscriber Secure Policy” on page 644 for descriptions of the supported attributes used in DTCP 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.

4. (Optional) Configure SNMPv3 trap support to capture and report mirroring information to an external device.

See “Configuring SNMPv3 Traps for Subscriber Secure Policy Mirroring” on page 646.

5. You can terminate an active subscriber mirroring session at any time.

See “Subscriber Secure Policy Mirroring Session Termination” on page 639.



**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 Gbps of actual user data.

---

**Related  
Documentation**

- DTCP Attributes Used for Subscriber Secure Policy on page 644
- Subscriber Secure Policy Mirroring and SNMP Traps on page 645
- Subscriber Secure Policy Mirroring Session Termination on page 639
- Example: Subscriber Secure Policy Mirroring Using DTCP on page 651

---

## Configuring DTCP Support for Subscriber Secure Policy Mirroring

---

This topic describes the steps to enable DTCP support for subscriber secure policy mirroring. The DTCP-initiated subscriber secure policy feature requires that you configure the DTCP-over-SSH feature for the radius-flow-tap service.

To enable the DTCP-over-SSH flow-tap service to support subscriber secure policy mirroring:

1. Create the login class and configure **flow-tap-operation** permissions for the class.
  - a. At the **[edit system]** hierarchy level, specify that you want to configure login properties.

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

- b. Create and name the class.

```
[edit system login]
user@host# edit class class-name
```



- c. Configure the **flow-tap-operation** permission for the class.

```
[edit system login class class-name]
user@host# set permissions flow-tap-operation
```

2. Create the user login account for the subscriber whose traffic will be mirrored.

- a. At the **[edit system login]** hierarchy, create the user account.

```
[edit system login]
user@host# edit user username
```

- b. Configure the user ID.

```
[edit system login user username]
user@host# set uid uid-value
```

- c. Configure the class for the user account.

```
[edit system login user username]
user@host# set class class-name
```

- d. Configure the authentication for the user account.

```
[edit system login user username]
user@host# set authentication encrypted-password password
```

3. Configure DTCP sessions to run over SSH in support of the flow-tap service.

- a. At the **[edit system services]** hierarchy, configure the flow-tap-dtcp service.

```
[edit system services]
user@host# edit flow-tap-dtcp
```

- b. Configure SSH support for DTCP.

```
[edit system services flow-tap-dtcp]
user@host# set ssh
```

- c. (Optional) Configure maximum number of established connections allowed for the DTCP service.

```
[edit system services flow-tap-service ssh]
user@host# set connection-limit limit
```

- d. (Optional) Configure the maximum number of connection attempts allowed per minute for DTCP.

```
[edit system services flow-tap-service ssh]
user@host# set rate-limit limit
```

#### Related Documentation

- Subscriber Secure Policy Overview on page 625
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 635
- Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview on page 641
- Subscriber Secure Policy Mirroring Session Termination on page 639
- Configuring DTCP-over-SSH Service for the Flow-Tap Application
- Example: Subscriber Secure Policy Mirroring Using DTCP on page 651

## DTCP Attributes Used for Subscriber Secure Policy

DTCP-initiated subscriber secure policy mirroring is triggered by a DTCP attribute that identifies the subscriber interface on which traffic is to be mirrored. The traffic mirroring session starts when the router (intercept access point) receives a DTCP ADD message that contains the trigger and other DTCP attributes that provide mirroring-related information, and then applies the subscriber secure policy configuration to the appropriate interface. The DTCP ADD message can be sent either before or after subscribers log on through the interface.

Table 62 on page 644 lists the mirroring trigger and the other DTCP attributes that the DTCP server administrator must include in the DTCP ADD message.

### DTCP Traffic Mirroring Attributes

Table 62 on page 644 lists the DTCP attributes that trigger traffic mirroring and provide mirroring-related information.

**Table 62: DTCP Mirroring Attributes**

Attribute Name	DTCP Message Semantic	Description
Interface-ID	X-Interface-Id	Mirroring trigger. The interface description string on which traffic mirroring is performed (for example, <b>ge-0/0/0.1</b> or <b>demux0.107472834</b> ).
Mediation Device IP Address	X-JTap-Cdest-Source-Address	IPv4 address of the mediation device to which the router sends intercepted traffic.
Mediation Device UDP Port	X-JTap-Cdest-Port	UDP port of the mediation device.
Intercept ID (also known as the Mirror ID)	X-MD-Intercept-Id	Identifier that the mediation device uses to correlate traffic from a particular subscriber.

## CHAPTER 59

# Subscriber Secure Policy Mirroring and SNMP Traps

- Subscriber Secure Policy Mirroring and SNMP Traps on page 645
- SNMP Traps for Subscriber Secure Policy LAES Compliance on page 645
- Configuring SNMPv3 Traps for Subscriber Secure Policy Mirroring on page 646

## Subscriber Secure Policy Mirroring and SNMP Traps

---

Subscriber secure policy supports the use of SNMPv3 traps to report traffic mirroring information. Using SNMPv3 provides secure traps that are visible only to authorized individuals on the intended secure mediation device. The traps help support compliance with the Communications Assistance for Law Enforcement Act (CALEA), which defines electronic surveillance guidelines for telecommunications companies.

The supported SNMPv3 traps map to messages defined by the *Lawfully Authorized Electronic Surveillance (LAES) for IP Network Access, American National Standard For Telecommunications*. “SNMP Traps for Subscriber Secure Policy LAES Compliance” on page 645 describes the supported SNMPv3 traps and their related LAES messages.

### Related Documentation

- Subscriber Secure Policy Overview on page 625
- Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 635
- SNMP Traps for Subscriber Secure Policy LAES Compliance on page 645
- Example: SNMPv3 Traps Configuration for Subscriber Secure Policy Mirroring on page 655

## SNMP Traps for Subscriber Secure Policy LAES Compliance

---

Table 63 on page 646 describes the SNMPv3 traps that subscriber secure policy mirroring uses to provide information that maps to messages defined in the *Lawfully Authorized Electronic Surveillance (LAES) for IP Network Access, American National Standard for Telecommunications*. These messages enable subscriber secure policy to comply with the *Communications Assistance for Law Enforcement Act (CALEA)*. The Juniper Packet Mirroring MIB, **jnx-js-packet-mirror.mib** provides the SNMP trap.

Table 63: Subscriber Secure Policy SNMPv3 Traps for LAES Messages

SNMPv3 Trap	LAES Message	Description
<code>jnxPacketMirrorLiSubscriberLoggedIn</code>	<ul style="list-style-type: none"> <li><code>access-attempt</code> (implied)</li> <li><code>access-session-accept</code></li> <li><code>packet-data-session-start</code></li> </ul>	A subscriber, who is identified to have a mirrored service that is activated at login, has successfully logged in.
<code>jnxPacketMirrorSessionLiSubscriberLogInFailed</code>	<ul style="list-style-type: none"> <li><code>access-attempt</code> (implied)</li> <li><code>access-failed</code> (all termination reasons except authentication-reject)</li> <li><code>access-reject</code> (termination reason is authentication-reject)</li> </ul>	A subscriber, who is identified to have a mirrored service that is activated at login, has failed to log in.
<code>jnxPacketMirrorInterfaceLiSubscriberLoggedOut</code>	<ul style="list-style-type: none"> <li><code>access-session-end</code></li> <li><code>packet-data-session-end</code></li> </ul>	A subscriber, who had an active mirrored service, has logged out.
<code>jnxPacketMirrorInterfaceLiServiceActivated</code>	<ul style="list-style-type: none"> <li><code>packet-data-session-already-established</code></li> </ul>	A mirrored session has been activated.
<code>jnxPacketMirrorSessionLiServiceActivationFailed</code>	—	A mirrored session for a subscriber has failed.
<code>jnxPacketMirrorSessionLiServiceDeactivated</code>	—	A mirrored session for an established subscriber has been deactivated.
<code>jnxPacketMirrorMirroringFailure</code>	—	<p>A mirrored service request failed due to an invalid value in the request.</p> <p>Note: This trap is not related to LAES messages.</p>

## Configuring SNMPv3 Traps for Subscriber Secure Policy Mirroring

This topic provides an overview of the SNMPv3 configuration process as it pertains to subscriber secure policy. The steps are described in detail in Chapter 7, “Configuring SNMPv3” in the *Junos OS Network Management Configuration Guide*.

To configure SNMPv3 trap support for subscriber secure policy and to send the trap information to the mediation device:

1. Configure the MIB view.  
See Configuring MIB Views.
2. Configure the trap notification and trap notification filter. See the following topics:
  - Configuring the SNMPv3 Trap Notification
  - Configuring the Trap Notification Filter

3. Configure the target device. The target device is the mediation device that receives the trap information.

See [Configuring SNMPv3 Traps on a Device Running Junos OS](#).

4. Configure the SNMPv3 user, authentication method and password, and privacy method and password. See the following topics:

- [Creating SNMPv3 Users](#)
- [Configuring the SNMPv3 Authentication Type](#)
- [Configuring the Encryption Type](#)

5. Configure user access privileges to management information.

See [Defining Access Privileges for an SNMP Group](#).

**Related  
Documentation**

- [Subscriber Secure Policy Overview](#) on page 625
- [Example: SNMPv3 Traps Configuration for Subscriber Secure Policy Mirroring](#) on page 655
- For information about SNMPv3, see the [Junos OS Network Management Configuration Guide](#)



# Subscriber Secure Policy Mirroring Examples

- Example: Subscriber Secure Policy Mirroring Using RADIUS on page 649
- Example: Subscriber Secure Policy Mirroring Using DTCP on page 651
- Example: Subscriber Secure Policy Dynamic Profile on page 654
- Example: SNMPv3 Traps Configuration for Subscriber Secure Policy Mirroring on page 655

## Example: Subscriber Secure Policy Mirroring Using RADIUS

---

This example shows a subscriber secure policy mirroring configuration that uses RADIUS. The configuration captures and sends information for a subscriber to a mediation device defined on the RADIUS server.

```
system {
  ports {
    console log-out-on-disconnect;
  }
  services {
    dhcp-local-server {
      pool-match-order {
        external-authority;
        ip-address-first;
        option-82;
      }
      authentication {
        password myPassword;
        username-include {
          user-prefix BSMITH;
        }
      }
      group southwest25 {
        interface ge-1/0/0.100;
      }
    }
  }
}
interfaces {
  ge-1/0/0 {
    flexible-vlan-tagging;
```

```
    unit 100 {
      proxy-arp;
      vlan-id 100;
      family inet {
        unnumbered-address lo0.0 preferred-source-address
          192.168.25.2;
      }
    }
  }
  vt-1/1/10 {
    unit 0 {
      family inet;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 192.168.25.2/32;
      }
    }
  }
}
snmp {
  community oslo {
    authorization read-only;
    clients {
      192.168.35.225/32;
    }
  }
  trap-group oslo {
    version v2;
    targets {
      192.168.35.225;
    }
  }
}
access {
  radius-server {
    192.168.11.178 secret " myRadiusSecret-1";
    192.168.35.225 {
      port 1812;
      secret "myRadiusSecret-2";
    }
  }
  profile myProf1 {
    authentication-order radius;
    radius {
      authentication-server 192.168.35.225;
      accounting-server 192.168.11.178;
    }
  }
  address-assignment {
    pool poolA {
      family inet {
        network 192.168.42.0/8;
        range limited {
```



```

        low 192.168.42.10;
        high 192.168.42.254;
    }
}
}
}
chassis {
    fpc 1 {
        pic 1 {
            tunnel-services {
                bandwidth 1g;
            }
        }
    }
}
services {
    radius-flow-tap {
        traceoptions {
            file myFile-20;
        }
        source-ipv4-address 192.168.200.1;
        interfaces {
            vt-1/1/10.0;
        }
    }
}
}
access-profile myProf1;

```

- Related Documentation**
- [Subscriber Secure Policy Overview on page 625](#)
  - [Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 635](#)

## Example: Subscriber Secure Policy Mirroring Using DTCP

This example shows a subscriber secure policy mirroring configuration that uses DTCP. The configuration captures and sends information for a subscriber and to a mediation device defined on the DTCP server.

```

system {
    ports {
        console log-out-on-disconnect;
    }
    login {
        class ft-class {
            permissions flow-tap-operation;
        }
        user ft-user1 {
            uid 2000;
            class ft-class;
            authentication {
                encrypted-password
                "yourSecret";
            }
        }
    }
}

```

```
    }
  }
  services {
    flow-tap-dtcp {
      ssh;
    }
    dhcp-local-server {
      pool-match-order {
        external-authority;
        ip-address-first;
        option-82;
      }
      authentication {
        password myPassword;
        username-include {
          user-prefix JDOE;
        }
      }
      group northeast42 {
        interface ge-1/0/0.100;
      }
    }
  }
}
chassis {
  fpc 0 {
    pic 1 {
      tunnel-services {
        bandwidth 1g;
      }
    }
  }
}
interfaces {
  ge-1/0/0 {
    flexible-vlan-tagging;
    unit 100 {
      proxy-arp;
      vlan-id 100;
      family inet {
        unnumbered-address lo0.0 preferred-source-address
        192.168.22.2;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 192.168.22.2/32;
      }
    }
  }
}
snmp {
  community madrid {
    authorization read-only;
```

```

clients {
  192.168.30.225/32;
}
}
trap-group madrid {
  version v2;
  targets {
    192.168.30.225;
  }
}
}
access {
  radius-server {
    192.1168.11.178 secret "yourRadiusSecret-1";
    SECRET-DATA
    192.168.30.225 {
      port 1812;
      secret "yourRadiusSecret-2";
    }
  }
  profile myProf2 {
    authentication-order radius;
    radius {
      authentication-server 192.168.30.225;
      accounting-server 192.168.11.178;
    }
  }
  address-assignment {
    pool poolA {
      family inet {
        network 192.168.22.0/8;
        range limited {
          low 192.168.22.10;
          high 192.168.22.254;
        }
      }
    }
  }
}
}
services {
  radius-flow-tap {
    traceoptions {
      file myFile10;
    }
    source-ipv4-address 192.168.100.1;
    interfaces {
      vt-1/1/10.0;
    }
  }
}
}

```

**Related  
Documentation**

- [Subscriber Secure Policy Overview on page 625](#)
- [Configuring DTCP-Initiated Subscriber Secure Policy Mirroring Overview on page 641](#)

## Example: Subscriber Secure Policy Dynamic Profile

In this example, subscriber secure policy mirroring is configured for subscriber access using user-defined variables and Junos OS predefined variables. This example is for the flow-tap service configured on a router without a Tunnel Services PIC.

The user-defined variables equate to RADIUS settings as follows:

User-Defined Variable Name	Junos OS Variable	RADIUS VSA Name	RADIUS Attribute Number	Example RADIUS Setting
ssp-intercept-id	\$ssp-intercept-id	Med-Dev-Handle	26-59	subscriber-bg-2350
ssp-destination-addr	\$ssp-destination-addr	Med-IP-Address	26-60	192.163.100.22
ssp-destination-port	\$ssp-destination-port	Med-Port-Number	26-61	2222

```

variables {
  var ssp-intercept-id;
  var ssp-destination-addr;
  var ssp-destination-port;
}
interfaces {
  <*> {
    unit <*> {
      family inet {
        filter {
          input ssp;
          output ssp;
        }
      }
    }
  }
}
firewall {
  family inet {
    filter ssp {
      term $ssp-id {
        from {
          # optional classifiers.
        }
        then {
          flowtap-destination-address $ssp-destination-addr;
          flowtap-destination-port $ssp-destination-port;
          flowtap;
        }
      }
    }
  }
}

```

## Example: SNMPv3 Traps Configuration for Subscriber Secure Policy Mirroring

This example shows an SNMP configuration that provides SNMPv3 trap support.

Configure the SNMPv3 trap support at the **[edit snmp]** hierarchy level.

```
[edit snmp]
view system {
  oid 1.3.6.1.2.1.1 include;
}
view all {
  oid .1 include;
}
v3 {
  notify n1 {
    type trap;
    tag mediation8;
  }
  notify-filter nf1 {
    oid .1 include;
  }
  target-address london-1 {
    address 172.19.87.240; # Address of the mediation device receiving the traps
    port 162;
    tag-list mediation-8;
    target-parameters tp1 {
      parameters {
        message-processing-model v3;
        security-model usm;
        security-level authentication;
        security-name mediation-device1; # Name of the mediation device
      }
      notify-filter nf1;
    }
  }
}
usm {
  local-engine {
    user mediation-device1 { # Name of the mediation device
      authentication-md5 {
        authentication-key
          "yourAuthenticationKey"
      }
      privacy-des {
        privacy-password "yourPrivacyPassword"
      }
    }
  }
}
vacm {
  access {
    group london-10 {
      default-context-prefix {
        security-model usm {
          security-level privacy {
```

```
        read-view system;
        notify-view all;
    }
}
}
}
}
security-to-group {
    security-model usm {
        security-name mediation-device1 { # Name of the mediation device
            group london-10;
        }
    }
}
}
```

**Related  
Documentation**

- Subscriber Secure Policy Overview on page 625
- Configuring SNMPv3 Traps for Subscriber Secure Policy Mirroring on page 646
- For information about SNMPv3, see the [Junos OS Network Management Configuration Guide](#)

## PART 14

# Class of Service for Subscriber Access

- [Dynamic CoS for Subscriber Access Overview on page 659](#)
- [Configuration Summary of Dynamic CoS for Subscriber Access on page 669](#)
- [Configuring Dynamic Shaping and Scheduling for Subscriber Access on page 677](#)
- [RADIUS and Dynamic CoS Overview on page 689](#)
- [Configuring RADIUS for Dynamic CoS on page 697](#)
- [Interface Solutions for Dynamic CoS Overview on page 703](#)
- [Configuring Interface Solutions for Dynamic CoS on page 707](#)
- [Dynamic CoS for Subscriber Access Examples on page 713](#)
- [Bandwidth Management for Dynamic CoS Overview on page 747](#)
- [Configuring Bandwidth Management Parameters for Dynamic CoS on page 757](#)
- [Bandwidth Management for Dynamic CoS Examples on page 771](#)





# Dynamic CoS for Subscriber Access Overview

- CoS for Subscriber Access Overview on page 659
- Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660

## 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 functionality 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. 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 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.

In a subscriber access network, a subscriber is an authenticated user—a user that has logged in to 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. In this network, subscribers are mapped to VLANs, demux, or PPPoE interfaces.

You can configure the router to provide *hierarchical scheduling* or *per-unit scheduling* for subscribers.

Hierarchical CoS enables you to apply traffic scheduling and queuing 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. Hierarchical CoS enables you to dynamically modify queues when subscribers require services.

Per-unit scheduling enables one set of output queues for each logical interface configured under the physical interface. In per-unit scheduling configurations, each Layer 3 scheduler node is allocated a dedicated set of queues.

**Related  
Documentation**

- Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660
- Configuring Static Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 669
- Configuring Dynamic Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 671
- Configuring Per-Unit Scheduling in a Dynamic Profile for Subscriber Access on page 673

---

## Guidelines for Configuring Dynamic CoS for Subscriber Access

This topic describes the hardware requirements and guidelines for configuring dynamic CoS in a subscriber access environment.

### Hardware Requirements for Dynamic CoS

Table 64 on page 661 lists the hardware requirements based on subscriber interface type for the hierarchical scheduling and per-unit scheduling dynamic CoS configurations.

Table 64: Hardware Required for Dynamic CoS Configurations

Dynamic CoS Configuration	Subscriber Interface Type	EQ DPCs on MX Series Routers	Trio MPC/MIC Modules on MX Series Routers	IQ2 PICs on M120 and M320 Routers	IQ2E PICs on M120 and M320 Routers
Hierarchical CoS	Static and dynamic VLANs	Yes	Yes	No	No
	Static and dynamic VLANs over aggregated Ethernet	Yes	Yes	No	No
	Static or dynamic IP demux interfaces	Yes	Yes	No	No
	Static or dynamic IP demux interfaces over aggregated Ethernet	Yes	Yes	No	No
	Static or dynamic VLAN demux interfaces	No	Yes	No	No
	Static or dynamic VLAN demux interfaces over aggregated Ethernet	No	Yes	No	No
	Static PPPoE interfaces	No	Yes	Yes	Yes
	Dynamic PPPoE interfaces	No	Yes	No	Yes
	Static or dynamic PPPoE interfaces over aggregated Ethernet	No	Yes	No	No
	L2TP LAC tunnel over PPP	No	Yes	No	No

Table 64: Hardware Required for Dynamic CoS Configurations (*continued*)

Dynamic CoS Configuration	Subscriber Interface Type	EQ DPCs on MX Series Routers	Trio MPC/MIC Modules on MX Series Routers	IQ2 PICs on M120 and M320 Routers	IQ2E PICs on M120 and M320 Routers
Per-unit scheduling	Static and dynamic VLANs	Yes	Yes	No	No
	Static and dynamic VLANs over aggregated Ethernet	No	No	No	No
	Static or dynamic IP demux interfaces	Yes	No	No	No
	Static or dynamic IP demux interfaces over aggregated Ethernet	No	No	No	No
	Static or dynamic VLAN demux interfaces	No	No	No	No
	Static or dynamic VLAN demux interfaces over aggregated Ethernet	No	No	No	No
	Static PPPoE interfaces	No	Yes	Yes	Yes
	Dynamic PPPoE interfaces	No	No	Yes	Yes
	Static or dynamic PPPoE interfaces over aggregated Ethernet	No	No	No	No
	L2TP LAC tunnel over PPP	No	No	No	No

## Configuration Guidelines for Dynamic Scheduling and Queuing

When configuring scheduling and queuing for subscriber access, consider the following guidelines:

- You can configure dynamic CoS with one of the following scheduling configurations:
  - For hierarchical scheduling configurations, you must enable hierarchical scheduling in the static CLI for the interface referenced in the dynamic profile. If not, the dynamic profile fails.
  - For per-unit scheduling configurations, you must enable per-unit scheduling in the static CLI for the interface referenced in the dynamic profile. If not, the dynamic profile fails and schedulers are not attached to the interface.
- 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 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.

## Configuration Guidelines for Dynamic Classifiers and Rewrite Rules

When you configure classifiers and rewrite rules for subscriber access, consider the following guidelines:

- To apply classifiers and rewrite rules to a subscriber interface in a dynamic profile, you must configure the rewrite rule and classifier definitions in the static **[edit class-of-service]** hierarchy and reference them in the dynamic profile.
  - If a static classifier or a rewrite rule definition that is referenced by a dynamic subscriber interface does not exist, the configuration is invalid and the subscriber cannot log in.
  - If a network administrator changes the static classifiers and rewrite rules definitions that are referenced in a dynamic profile with an active subscriber interface logged in, the changes are applied to the active subscriber interface immediately.
  - If a network administrator deletes a classifier or a rewrite rule definition that is referenced by an active dynamic subscriber interface, the system removes the classifier or rewrite rule binding from the interface. The classifier is replaced by the

default classifier. If the network administrator adds the removed classifier or rewrite rule to the configuration while the dynamic interface is active, the addition does not take effect until the subscriber logs out and then logs in again.

- IP demux interfaces can only instantiate Layer 3 rules (both rewrite rules and classifiers).
  - An IP demux subscriber interface can implicitly inherit a classifier from the underlying interface. If an IP demux interface is created without a classifier and a Layer 2 classifier is attached to the underlying interface, the IP demux interface also inherits the Layer 2 classifier. The **show class-of-service interface interface-name** command does not display this attachment.

Table 65 on page 664 lists the classification rule configuration for an IP demux subscriber interface with a VLAN underlying interface.

**Table 65: IP Demux Classification Rules**

VLAN Underlying Interface Classifier Configuration	IP Demux Interface Classifier Configuration	Resulting Classifier Configuration
Layer 2	—	VLAN Layer 2
Layer 2	Layer 3	Demux Layer 3
Layer 3	—	Default
Layer 3	Layer 3	Demux Layer 3

- An IP demux subscriber interface explicitly inherits Layer 2 rewrite rules from the underlying interface if a Layer 2 rewrite rule is present. The **show class-of-service interface interface-name** command displays the attachment.

Table 66 on page 664 lists the rewrite rule configuration for an IP demux subscriber interface with a VLAN underlying interface.

**Table 66: IP Demux Rewrite Rules**

VLAN Underlying Interface Rewrite Rule Configuration	IP Demux Interface Rewrite Rule Configuration	Resulting Rewrite Rule Configuration
Layer 2	—	VLAN Layer 2
Layer 2	Layer 3	VLAN Layer 2 and demux Layer 3
Layer 3	—	Default
Layer 3	Layer 3	Demux Layer 3

- An L2TP subscriber interface can implicitly inherit a classifier from the underlying interface.

Table 67 on page 665 lists the classification rule configuration for an L2TP LAC subscriber interface with a VLAN underlying interface.

**Table 67: L2TP Classification Rules**

VLAN Underlying Interface Classifier Configuration	L2TP LAC Classifier Configuration	Resulting Classifier Configuration
Layer 2 or Fixed	Layer 2 or Fixed	VLAN Layer 2 or Fixed
Layer 2 or Fixed	Layer 3	Demux/PPPoE Layer 3
Layer 3	Layer 2 or Fixed	VLAN Layer 2 or Fixed
Layer 3	Layer 3	Demux/PPPoE Layer 3

- An L2TP LAC subscriber interface explicitly inherits Layer 2 rewrite rules from the underlying interface if a Layer 2 rewrite rule is present. Table 68 on page 665 lists the rewrite rule configuration for an L2TP LAC subscriber interface with a VLAN underlying interface.

**Table 68: L2TP LAC Rewrite Rules**

VLAN Underlying Interface Rewrite Rule Configuration	L2TP Interface Rewrite Rule Configuration	Resulting Rewrite Rule Configuration
Layer 2	Layer 2	VLAN Layer 2
Layer 2	Layer 3	VLAN Layer 2 and demux/PPPoE Layer 3
Layer 3	Layer 2	VLAN Layer 2 and demux/PPPoE Layer 3
Layer 3	Layer 3	Demux/PPPoE Layer 3

## Configuration Guidelines for Dynamic Excess Bandwidth Distribution

When you configure excess bandwidth distribution parameters for subscriber access, consider the following guidelines:

For queues, you cannot configure the excess rate or excess priority in these cases:

- When the **transmit-rate exact** statement is configured. In this case, the shaping rate is equal to the transmit rate and the queue does not operate in the excess region.
- When the scheduling priority is configured as **strict-high**. In this case, the queue gets all available bandwidth and never operates in the excess region.
- When logical interface units are configured in peak information rate (PIR) mode. The excess rate distributes excess bandwidth once the scheduling nodes reach their guaranteed rate. In PIR mode, none of the scheduling nodes have guaranteed rates configured, so you do not need to configure the excess rate.

## Configuration Guidelines for Dynamic CoS on Aggregated Ethernet Interfaces

Keep the following guidelines in mind when configuring static or dynamic CoS for a subscriber interface on a 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. For more information, see Table 64 on page 661.
- Configure the aggregated Ethernet logical interface with both underlying links operating in link-protect mode.
- 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.
- For specific configuration guidelines for applying CoS to subscribers in a targeted distribution model, see “Distribution of Demux Subscribers in an Aggregated Ethernet Interface” on page 474.

## Configuration Guidelines for Dynamic CoS on PPPoE Interfaces

For specific configuration guidelines, see “CoS for PPPoE Subscriber Interfaces Overview” on page 704.

## Configuration Guidelines for Dynamic CoS on L2TP Interfaces

For additional configuration guidelines, see “CoS for L2TP Subscriber Interfaces Overview” on page 704.



## Configuration Guidelines for Dynamic CoS on Interface Sets

Keep the following guidelines in mind when configuring dynamic interface sets:

- Dynamic interface sets are not supported for aggregated Ethernet interfaces.
- You can configure the interface set and the traffic scheduling and shaping parameters in the dynamic profile. However, you must apply the traffic-control profile to the interface set in the static **[edit class-of-service]** hierarchy.
- The **\$junos-interface-set-name** predefined variable is available only for RADIUS Accept messages; change of authorization (CoA) requests are not supported.
- An interface can only belong to one interface set. If you try to add the same interface to different interface sets, the commit operation fails.

### Related Documentation

- CoS for Subscriber Access Overview on page 659
- Configuring Static Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 669
- Configuring Dynamic Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 671
- Configuring Per-Unit Scheduling in a Dynamic Profile for Subscriber Access on page 673
- For information about static CoS configurations, see the [Junos OS Class of Service Configuration Guide](#)



# Configuration Summary of Dynamic CoS for Subscriber Access

- Configuring Static Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 669
- Configuring Dynamic Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 671
- Configuring Per-Unit Scheduling in a Dynamic Profile for Subscriber Access on page 673

## Configuring Static Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access

---

You configure static scheduling and queuing in a dynamic profile for subscriber access.

To configure CoS in a dynamic profile for subscriber access using static scheduling and queuing parameters:

1. Configure the static CoS parameters in the **[edit class-of-service]** hierarchy.
  - a. Enable the hierarchical scheduler for the interface.  
See Configuring Hierarchical Schedulers for CoS.
  - b. Configure the scheduler map and schedulers.  
When you configure static scheduling and queuing in a dynamic profile, you reference the scheduler map in the dynamic profile.  
See Configuring Schedulers.
  - c. Configure the drop profiles.  
See Configuring RED Drop Profiles.
  - d. Configure the forwarding classes.  
See Configuring Forwarding Classes
  - e. Configure the rewrite-rules and classifier definitions.  
See Configuring Rewrite Rules and Defining Classifiers.

See the *Junos OS Class of Service Configuration Guide* for information about configuring the remaining CoS parameters.

2. Configure a static or dynamic subscriber interface that can be referenced in the dynamic profile.
  - For static VLAN interfaces, see “Configuring Static Subscriber Interfaces in Dynamic Profiles” on page 439.
  - For dynamic VLAN interfaces, see “Configuring a Static or Dynamic VLAN Subscriber Interface over Aggregated Ethernet” on page 479.
  - For dynamic IP demux interfaces, see “Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles” on page 445 and “Configuring a Static or Dynamic IP Demux Subscriber Interface over Aggregated Ethernet” on page 481.
  - For dynamic VLAN demux interfaces, see “Configuring Dynamic Subscriber Interfaces Using VLAN Demux Interfaces in Dynamic Profiles” on page 446.
  - For dynamic PPPoE interfaces, see “Configuring Dynamic PPPoE Subscriber Interfaces Using Dynamic Profiles” on page 535.
3. Configure CoS parameters in a dynamic profile.
  - a. Configure the dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 391.
  - 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 Static Traffic Shaping and Scheduling Parameters in a Dynamic Profile” on page 677.
  - c. Apply CoS parameters to a subscriber interface by referencing an interface in the dynamic profile.

See “Applying Traffic Shaping and Scheduling to a Subscriber Interface in a Dynamic Profile” on page 685.
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 698.

**Related Documentation**

- For hardware requirements and configuration guidelines, see Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660
- CoS for Subscriber Access Overview on page 659
- Example: Configuring Static Hierarchical Scheduling and Queuing for Subscriber Access on page 713

## Configuring Dynamic Hierarchical 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 using dynamic scheduling and queuing parameters:

1. Configure the static CoS parameters in the **[edit class-of-service]** hierarchy.

- a. Enable the hierarchical scheduler for the interface.

See [Configuring Hierarchical Schedulers for CoS](#).

- b. Configure the drop profiles.

See [Configuring RED Drop Profiles](#).

- c. Configure the forwarding classes.

See [Configuring Forwarding Classes](#).

- d. Configure the rewrite-rules and classifier definitions.

See [Configuring Rewrite Rules and Defining Classifiers](#).

See the [Junos OS Class of Service Configuration Guide](#) for information about configuring the remaining CoS parameters.

2. Configure a static or dynamic subscriber interface that can be referenced in the dynamic profile.

- For static VLAN interfaces, see “Configuring Static Subscriber Interfaces in Dynamic Profiles” on page 439.
- For dynamic VLAN interfaces, see “Configuring a Static or Dynamic VLAN Subscriber Interface over Aggregated Ethernet” on page 479.
- For dynamic IP demux interfaces, see “Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles” on page 445 and “Configuring a Static or Dynamic IP Demux Subscriber Interface over Aggregated Ethernet” on page 481.
- For dynamic VLAN demux interfaces, see “Configuring Dynamic Subscriber Interfaces Using VLAN Demux Interfaces in Dynamic Profiles” on page 446.
- For dynamic PPPoE interfaces, see “Configuring Dynamic PPPoE Subscriber Interfaces Using Dynamic Profiles” on page 535.

3. Configure CoS parameters in a dynamic profile.

a. Configure the dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 391.

b. Configure traffic shaping and scheduling parameters in the dynamic profile using a traffic-control profile.

See “Configuring Traffic Scheduling and Shaping for Subscriber Access” on page 677.

c. Configure the schedulers and scheduler map in the dynamic profile.

You can configure the schedulers using dynamic variables or a combination of both static values and dynamic variables.

See “Configuring Schedulers in a Dynamic Profile for Subscriber Access” on page 679.

d. Apply CoS parameters to a subscriber interface by referencing an interface in the dynamic profile.

- For traffic shaping and scheduling, see “Applying Traffic Shaping and Scheduling to a Subscriber Interface in a Dynamic Profile” on page 685.
- For rewrite-rules, see “Applying a Rewrite Rule Definition to a Subscriber Interface in a Dynamic Profile” on page 686.
- For classifiers, see “Applying a Classifier to a Subscriber Interface in a Dynamic Profile” on page 687.

4. (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.

a. Configure user-defined CoS variables in a dynamic profile.

See “Configuring User-Defined CoS Variables in a Dynamic Service Profile” on page 698

b. (Optional) Enable multiple clients for the same subscriber (logical interface) to aggregate attributes 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 125.

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, and the dynamic profile referenced by DHCP does not have the **replace** keyword configured, the system does not replace the parameters. Instead, it combines the values of the parameters to their maximum scalar value.

- Related Documentation**
- For hardware requirements and configuration guidelines, see [Guidelines for Configuring Dynamic CoS for Subscriber Access](#) on page 660
  - [CoS for Subscriber Access Overview](#) on page 659
  - [Example: Configuring Dynamic Hierarchical Scheduling and Queuing for Subscriber Access](#) on page 715

---

## Configuring Per-Unit Scheduling in a Dynamic Profile for Subscriber Access

Per-unit scheduling enables one set of output queues for each logical interface configured under the physical interface. In per-unit scheduling configurations, each Layer 3 scheduler node is allocated a dedicated set of queues.

If you do not explicitly configure CoS parameters, a default traffic profile with queues is attached to the logical interface.

To configure per-unit scheduling and queuing for subscriber access:

1. Configure the static CoS parameters in the **[edit class-of-service]** hierarchy.

- a. Enable the per-unit scheduler for the physical interface.

```
[edit interfaces interface-name]  
user@host# set per-unit-scheduler
```

- b. Configure the drop profiles.

See [Configuring RED Drop Profiles](#).

- c. Configure the forwarding classes.

See [Configuring Forwarding Classes](#).

- d. Configure the rewrite-rules and classifier definitions.

See [Configuring Rewrite Rules and Defining Classifiers](#).

See the [Junos OS Class of Service Configuration Guide](#) for information about configuring the remaining CoS parameters.

2. Configure a static or dynamic subscriber interface that can be referenced in the dynamic profile.
  - For static VLAN interfaces, see “[Configuring Static Subscriber Interfaces in Dynamic Profiles](#)” on page 439.
  - For dynamic IP demux interfaces, see “[Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles](#)” on page 445.
  - For dynamic PPPoE interfaces, see “[Configuring Dynamic PPPoE Subscriber Interfaces Using Dynamic Profiles](#)” on page 535.

3. Configure CoS parameters in a dynamic profile.

a. Configure the dynamic profile.

See “Configuring a Basic Dynamic Profile” on page 391.

b. Configure traffic shaping and scheduling parameters in the dynamic profile using a traffic-control profile.

See “Configuring Traffic Scheduling and Shaping for Subscriber Access” on page 677.

c. Configure the schedulers and scheduler map in the dynamic profile.

You can configure the schedulers using dynamic variables or a combination of both static values and dynamic variables.

See “Configuring Schedulers in a Dynamic Profile for Subscriber Access” on page 679.

d. Apply CoS parameters to a subscriber interface by referencing an interface in the dynamic profile.

- For traffic shaping and scheduling, see “Applying Traffic Shaping and Scheduling to a Subscriber Interface in a Dynamic Profile” on page 685.
- For rewrite rules, see “Applying a Rewrite Rule Definition to a Subscriber Interface in a Dynamic Profile” on page 686.
- For classifiers, see “Applying a Classifier to a Subscriber Interface in a Dynamic Profile” on page 687.

4. (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, and the dynamic profile referenced by DHCP does not have the **replace** keyword configured, 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 698

b. (Optional) Enable multiple clients for the same subscriber (logical interface) to aggregate attributes 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 125.



- Related Documentation**
- CoS for Subscriber Access Overview on page 659
  - Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660
  - Example: Configuring Per-Unit Scheduling for Subscriber Access



# Configuring Dynamic Shaping and Scheduling for Subscriber Access

- Configuring Traffic Scheduling and Shaping for Subscriber Access on page 677
- Configuring Schedulers in a Dynamic Profile for Subscriber Access on page 679
- Applying CoS Parameters to a Subscriber Interface in a Dynamic Profile on page 685
- Verifying the Scheduling and Shaping Configuration for Subscriber Access on page 688

## Configuring Traffic Scheduling and Shaping for Subscriber Access

---

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.

You can choose to configure static values or dynamic variables for the shaping parameters. The values for the dynamic variables are obtained from RADIUS when a subscriber logs in or when a subscriber changes services.

You cannot configure a traffic-control profile that contains a combination of static and dynamic parameters.

This topic includes the following tasks:

- Configuring Static Traffic Shaping and Scheduling Parameters in a Dynamic Profile on page 677
- Configuring Dynamic Traffic Shaping and Scheduling Parameters in a Dynamic Profile on page 678

## Configuring Static Traffic Shaping and Scheduling Parameters in a Dynamic Profile

To configure static traffic shaping and scheduling parameters in a traffic-control 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 profile-name
```

2. Do one of the following:

- Reference a static 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
  profile-name]
user@host# set scheduler-map map-name
```

- Reference a dynamic scheduler map in the dynamic profile. The scheduler map is dynamically configured in the **[edit dynamic-profiles profile-name class-of-service scheduler-maps]** hierarchy.

```
[edit dynamic-profiles business-profile class-of-service traffic-control-profiles
  profile-name]
user@host# set scheduler-map map-name
```

3. Configure the shaping rate to be used in the dynamic profile.

```
[edit dynamic-profiles business-profile class-of-service traffic-control-profiles
  profile-name]
user@host# set shaping-rate (percent percentage | rate)
```

4. Configure the guaranteed rate to be used in the dynamic profile.

```
[edit dynamic-profiles business-profile class-of-service traffic-control-profiles
  profile-name]
user@host# set guaranteed-rate (percent percentage | rate)
```

5. 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 on the shaping rate if no guaranteed rate is configured.

```
[edit dynamic-profiles business-profile class-of-service traffic-control-profiles
  profile-name]
user@host# set delay-buffer-rate (percent percentage | rate)
```

## Configuring Dynamic Traffic Shaping and Scheduling Parameters in a Dynamic Profile

You can configure variables for the traffic shaping and scheduling parameters. The values for the parameters are dynamically obtained by RADIUS when a subscriber logs in or changes a service.

To configure dynamic traffic-control profiles in a dynamic profile:

1. Create the traffic-control profile.

```
[edit dynamic-profiles business-profile class-of-service]
user@host# edit traffic-control-profiles profile-name
```

2. Configure the scheduler map variable.

```
[edit dynamic-profiles business-profile class-of-service traffic-control-profiles
  profile-name]
user@host# set scheduler-map $juno-cos-scheduler-map
```

3. Configure the shaping rate variable.

```
[edit dynamic-profiles business-profile class-of-service traffic-control-profiles
  profile-name]
user@host# set shaping-rate $junos-cos-shaping-rate
```

4. Configure the guaranteed rate variable.

```
[edit dynamic-profiles business-profile class-of-service traffic-control-profiles
  profile-name]
user@host# set guaranteed-rate $junos-cos-guaranteed-rate
```

5. Configure a variable for 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
  profile-name]
user@host# set delay-buffer-rate $junos-cos-delay-buffer-rate
```

**Related  
Documentation**

- For hardware requirements and configuration guidelines, see Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660
- CoS for Subscriber Access Overview on page 659
- Configuring Static Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 669
- Configuring Dynamic Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 671
- Example: Configuring Static Hierarchical Scheduling and Queuing for Subscriber Access on page 713
- Example: Configuring Dynamic Hierarchical Scheduling and Queuing for Subscriber Access on page 715
- Verifying the Scheduling and Shaping Configuration for Subscriber Access on page 688

---

## Configuring 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.

Within a dynamic profile, you can choose to define schedulers with static values, dynamic variables, or a combination of static values and dynamic variables. The dynamic variables enable RADIUS to provide the value for the scheduler parameter when the subscriber logs in.

- Configuring Static Schedulers in a Dynamic Profile on page 680
- Configuring Dynamic Schedulers with Variables in a Dynamic Profile on page 681
- Configuring a Combination of Static and Dynamic Scheduler Parameters in a Scheduler Definition on page 682

## Configuring Static Schedulers in a Dynamic Profile

This topic describes how to configure schedulers with static values in a dynamic profile for subscriber access.

To configure static 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 profile-name class-of-service]  
user@host# edit schedulers scheduler-name
```

- b. Configure the buffer size.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]  
user@host# set buffer-size remainder
```

- c. Configure the drop-profile map and drop profile.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]  
user@host# set drop-profile-map loss-priority any protocol any drop-profile d3
```

- d. Configure the priority.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]  
user@host# set priority low
```

- e. Configure the transmit rate.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]  
user@host# set transmit-rate percent 40
```

- f. Configure the excess rate.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]  
user@host# set excess-rate percent 90
```

- g. (Optional) Configure the priority value for the excess-rate.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]  
user@host# set excess-priority high
```

2. Associate the scheduler with a scheduler map.

- a. Configure the scheduler map name.

```
[edit dynamic-profiles profile-name class-of-service]  
user@host# set scheduler-maps data-smap
```

- b. Configure the forwarding class.

```
[edit dynamic-profiles profile-name class-of-service scheduler-maps map-name]  
user@host# set forwarding-class be
```

- c. Configure the scheduler.

```
[edit dynamic-profiles profile-name class-of-service scheduler-maps map-name  
forwarding-class forwarding-class-name]
```

```
user@host# set scheduler be_sch
```

## Configuring Dynamic Schedulers with Variables in a Dynamic Profile

You can configure variables for the dynamic scheduler parameters. These values are dynamically obtained by RADIUS when a subscriber logs in or changes a service using a RADIUS change of authorization (CoA) message.

To configure dynamic scheduling and queuing in a dynamic profile:

1. Configure the scheduler and queuing parameters.

- a. Specify the scheduler name using a variable.

```
[edit dynamic-profiles profile-name class-of-service]
user@host# edit schedulers $junos-cos-scheduler
```

- b. Configure the variable for the buffer size.

```
[edit dynamic-profiles profile-name class-of-service schedulers]
user@host# set buffer-size (percent $junos-cos-scheduler-bs | temporal
$junos-cos-scheduler-bs)
```

- c. Configure the variables for the drop-profile maps and the drop profile.

```
[edit dynamic-profiles profile-name class-of-service schedulers]
user@host# set drop-profile-map loss-priority low protocol any drop-profile
$junos-cos-scheduler-low
user@host# set drop-profile-map loss-priority medium-low protocol any
drop-profile $junos-cos-scheduler-medium-low
user@host# set drop-profile-map loss-priority medium-high protocol any
drop-profile $junos-cos-scheduler-medium-high
user@host# set drop-profile-map loss-priority high protocol any drop-profile
$junos-cos-scheduler-high
user@host# set drop-profile-map loss-priority any protocol any drop-profile
$junos-cos-scheduler-any
```

- d. Configure the variable for the priority.

```
[edit dynamic-profiles profile-name class-of-service schedulers]
user@host# set priority $junos-cos-scheduler-pri
```

- e. Configure the variable for the transmit rate.

```
[edit dynamic-profiles profile-name class-of-service schedulers]
user@host# set transmit-rate $junos-cos-scheduler-tx
```

- f. Configure the variable for the excess rate.

```
[edit dynamic-profiles profile-name class-of-service schedulers]
user@host# set excess-rate percent $junos-cos-scheduler-excess-rate
```

- g. Configure the variable for the priority of the excess-rate.

```
[edit dynamic-profiles profile-name class-of-service schedulers]
user@host# set excess-priority $junos-cos-scheduler-excess-priority
```

2. Associate the scheduler with a scheduler map.

- a. Configure the scheduler map name.

```
[edit dynamic-profiles profile-name class-of-service]
user@host# edit scheduler-maps scheduler-map-name
```

- b. Configure the forwarding class.

```
[edit dynamic-profiles profile-name class-of-service scheduler-maps
scheduler-map-name]
user@host# set forwarding-class be
```

- c. Configure the scheduler.

```
[edit dynamic-profiles profile-name class-of-service scheduler-maps
scheduler-map-name]
user@host# set scheduler $junos-cos-scheduler
```

## Configuring a Combination of Static and Dynamic Scheduler Parameters in a Scheduler Definition

Within a dynamic profile, you can choose to configure one dynamic scheduler definition, or combine static and dynamic scheduler parameters in many static scheduler definitions.

Combining static and dynamic scheduler parameters enables you to provide subscribers with unique rate configurations that the RADIUS definitions for predefined variables do not allow.

To configure a scheduler definition that contains static and dynamic scheduling and queuing parameters:

1. Configure the scheduler definition.

- a. Specify the scheduler name.



**NOTE:** To configure a static scheduler that contains both static and dynamic parameters, you must specify a unique scheduler name, not the `$junos-cos-scheduler` variable.

```
[edit dynamic-profiles profile-name class-of-service]
user@host# edit schedulers scheduler-name
```

- b. Configure the buffer size.

Do either of the following:

- Configure a static value.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]
user@host# set buffer-size (percent percentage | remainder | temporal
(microseconds))
```

- Configure a variable.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]
```



```
user@host# set buffer-size (percent $junos-cos-scheduler-bs | temporal
$junos-cos-scheduler-bs)
```

- c. Configure the drop-profile maps, the drop profile, and the priority.

Do either of the following:

- Configure static values.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]
user@host# set drop-profile-map loss-priority any protocol any drop-profile d3
```

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]
user@host# set priority low
```

- Configure variables.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]
user@host# set drop-profile-map loss-priority low protocol any drop-profile
$junos-cos-scheduler-low
```

```
user@host# set drop-profile-map loss-priority medium-low protocol any
drop-profile $junos-cos-scheduler-medium-low
```

```
user@host# set drop-profile-map loss-priority medium-high protocol any
drop-profile $junos-cos-scheduler-medium-high
```

```
user@host# set drop-profile-map loss-priority high protocol any drop-profile
$junos-cos-scheduler-high
```

```
user@host# set drop-profile-map loss-priority any protocol any drop-profile
$junos-cos-scheduler-any
```

- d. Configure the priority.

Do either of the following:

- Configure a static value.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]
user@host# set excess-priority high
```

- Configure a variable.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]
user@host# set excess-priority $junos-cos-scheduler-excess-priority
```

- e. Configure the transmit rate.

Do either of the following:

- Configure a static value.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]
user@host# set transmit-rate
```

- Configure a variable.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]
user@host# set transmit-rate $juno-cos-scheduler-tx
```

- f. Configure the excess rate.

Do either of the following:

- Configure a static value.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]  
user@host# set excess-rate percent 250
```

- Configure a variable.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]  
user@host# set excess-rate percent $juno-cos-scheduler-excess-rate
```

- g. Configure the priority for the excess-rate.

Do either of the following:

- Configure a static value.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]  
user@host# set excess-priority high
```

- Configure a variable.

```
[edit dynamic-profiles profile-name class-of-service schedulers scheduler-name]  
user@host# set excess-priority percent $junos-cos-scheduler-excess-priority
```

2. Associate the scheduler with a scheduler map.

- a. Configure the scheduler map name.

```
[edit dynamic-profiles profile-name class-of-service]  
user@host# edit scheduler-maps scheduler-map-name
```

- b. Configure the forwarding class.

```
[edit dynamic-profiles profile-name class-of-service scheduler-maps  
  scheduler-map-name]  
user@host# set forwarding-class be
```

- c. Configure the scheduler.

```
[edit dynamic-profiles profile-name class-of-service scheduler-maps  
  scheduler-map-name]  
user@host# set scheduler $junos-cos-scheduler
```

**Related  
Documentation**

- For hardware requirements and configuration guidelines, see Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660
- Configuring Dynamic Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 671
- Verifying the Scheduling and Shaping Configuration for Subscriber Access on page 688
- Changing CoS Services Overview on page 693

## Applying CoS Parameters to a Subscriber Interface in a Dynamic Profile

You provide CoS parameters to a subscriber by associating the CoS parameters with an interface in a dynamic profile.

Traffic and scheduling parameters can be configured in the dynamic profile and associated with a subscriber by attaching an output traffic control profile to the interface in the dynamic profile.

You configure rewrite rules and classifiers statically in the **[edit class-of-service]** hierarchy and reference them in the dynamic profile.

- Applying Traffic Shaping and Scheduling to a Subscriber Interface in a Dynamic Profile on page 685
- Applying Minimal Shaping and Scheduling to Remaining Subscriber Traffic on page 685
- Applying a Rewrite Rule Definition to a Subscriber Interface in a Dynamic Profile on page 686
- Applying a Classifier to a Subscriber Interface in a Dynamic Profile on page 687

### Applying Traffic Shaping and Scheduling to a Subscriber Interface in a Dynamic Profile

After you configure the traffic shaping and scheduling 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 profile-name 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 profile-name class-of-service interfaces]
user@host# set interfaces $junos-interface-ifd-name unit
$junos-underlying-interface-unit output-traffic-control-profile profile-name
```

### Applying Minimal Shaping and Scheduling to Remaining Subscriber Traffic

It is beneficial to apply a remaining traffic-control profile to a logical interface to provide minimal CoS scheduling when you have not configured or over-provisioned Layer 3 schedulers. In the event that schedulers are not available, the remaining subscriber traffic receives the essential level of service.

To configure scheduling for remaining subscriber traffic:

1. Enable hierarchical scheduling for the interface.

```
[edit interfaces interface-name]
```

```
user@host# set hierarchical-scheduler
```

2. Apply the remaining traffic control profile to the port on which you enabled hierarchical scheduling.

```
[edit class-of-service interfaces interface-name]
```

```
user@host# set output-traffic-control-profile-remaining profile-name
```

## Applying a Rewrite Rule Definition to a Subscriber Interface in a Dynamic Profile

Rewrite rules define the marking for various CoS values, including DSCP, DSCP IPv6, IP precedence, and IEEE 802.1 CoS values. Rewrite rules have an associated forwarding class and code-point alias or bit set.

For dynamic CoS, you define the rewrite rules mapping for the CoS values statically, then reference the rewrite rule configuration in the dynamic profile for the subscriber interface.

To configure a rewrite rule in a dynamic profile:

1. Define the rewrite-rules mapping for the traffic that passes through all queues on the interface. The available rewrite-rules types for dynamic CoS are **dscp**, **dscp6**, **ieee-802.1** and **inet-precedence**.

See Configuring Rewrite Rules.

2. Apply the rewrite-rules definition to the subscriber interface in the dynamic profile.

```
[edit dynamic-profiles profile-name class-of-service interfaces interface-name unit  
  logical-unit-number]
```

```
user@host# edit rewrite-rules
```

3. Configure the applicable rewrite rule markers in the dynamic profile.

- For DSCP:

```
[edit dynamic-profiles profile-name class-of-service interfaces interface-name unit  
  logical-unit-number rewrite-rules]
```

```
user@host# set dscp (rewrite-name | default)
```

- For DSCPv6:

```
[edit dynamic-profiles profile-name class-of-service interfaces interface-name unit  
  logical-unit-number rewrite-rules]
```

```
user@host# set dscp-ipv6 (rewrite-name | default)
```

- For IEEE 802.1:

```
[edit dynamic-profiles profile-name class-of-service interfaces interface-name unit  
  logical-unit-number rewrite-rules]
```

```
user@host# set ieee-802.1 (rewrite-name | default) vlan-tag (outer | outer-and-inner)
```

- For inet-precedence:

```
[edit dynamic-profiles profile-name class-of-service interfaces interface-name unit  
  logical-unit-number rewrite-rules]
```

```
user@host# set inet-precedence (rewrite-name | default)
```

## Applying a Classifier to a Subscriber Interface in a Dynamic Profile

You can apply the classification map to a subscriber interface in a dynamic profile.

For dynamic CoS, you define the classification map for the CoS values statically, then reference the classifier configuration in the dynamic profile for the subscriber interface.

To apply a classifier to an interface in a dynamic profile:

1. Define the classifier.

The available classifier types for subscriber access are **dscp**, **dscp-ipv6**, **ieee-802.1**, and **inet-precedence**.

See Defining Classifiers.

2. Apply the classifier definition to the subscriber interface in the dynamic profile.

```
[edit dynamic-profiles profile-name class-of-service interfaces interface-name unit
logical-unit-number]
user@host# edit classifiers
```

3. Configure the applicable classifiers in the dynamic profile.

- For DSCP:

```
[edit dynamic-profiles profile-name class-of-service interfaces interface-name unit
logical-unit-number classifiers]
user@host# set dscp (classifier-name | default)
```

- For DSCPv6:

```
[edit dynamic-profiles profile-name class-of-service interfaces interface-name unit
logical-unit-number classifiers]
user@host# set dscp-ipv6 (classifier-name | default)
```

- For IEEE 802.1:

```
[edit dynamic-profiles profile-name class-of-service interfaces interface-name unit
logical-unit-number classifiers]
user@host# set ieee-802.1 (classifier-name | default) vlan-tag (inner | outer)
```

- For inet-precedence:

```
[edit dynamic-profiles profile-name class-of-service interfaces interface-name unit
logical-unit-number classifiers]
user@host# set inet-precedence (classifier-name | default)
```

### Related Documentation

- Configuring Static Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 669
- Configuring Dynamic Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 671
- CoS for Subscriber Access Overview on page 659

## Verifying the Scheduling and Shaping Configuration for Subscriber Access

---

**Purpose** View the class-of-service (CoS) configurations that are referenced in a dynamic profile for subscriber access.

- Action**
- To display the entire CoS configuration, including static and dynamic parameters:  
user@host> **show class-of-service**
  - To display the CoS configuration for a subscriber interface:  
user@host> **show class-of-service interface**
  - To display traffic shaping and scheduling profiles:  
user@host> **show class-of-service traffic-control-profile**
  - To display the mapping of schedulers to forwarding classes and a summary of scheduler parameters for each entry:  
user@host> **show class-of-service scheduler-map**

# RADIUS and Dynamic CoS Overview

- Subscriber Interfaces That Provide Initial CoS Parameters Dynamically Obtained from RADIUS on page 689
- Changing CoS Services Overview on page 693

## Subscriber Interfaces That Provide Initial CoS Parameters Dynamically Obtained from RADIUS

---

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 3D Universal Edge Routers.

To configure a dynamic profile to provide initial CoS Services, make sure you understand the following concepts:

- Dynamic Configuration of Initial CoS in Access Profiles on page 689
- Predefined Variables for Dynamic Configuration of Initial Traffic Shaping on page 690
- Predefined Variables for Dynamic Configuration of Initial Scheduling and Queuing on page 690

### Dynamic Configuration of Initial CoS in Access Profiles

When a router interface receives a join message from a DHCP subscriber, the Junos OS applies the values configured in the dynamic profile associated with that router interface. A dynamic profile that is activated through its association with a subscriber interface is known as an *access dynamic profile*. 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.

The Junos OS supports predefined variables for obtaining a scheduler-map name and traffic-shaping parameters from the RADIUS authentication server and predefined 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 access dynamic profile, the router replaces the predefined variables with interface-specific values obtained from the RADIUS server.



**NOTE:** To associate dynamically configured initial CoS features with a subscriber interface, reference *Junos OS predefined variables*—and not *user-defined variables*—in an access dynamic profile for that interface.

## Predefined Variables for Dynamic Configuration of Initial Traffic Shaping

You can configure an access dynamic profile that provides initial traffic-shaping parameters when a subscriber logs in. The Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the access dynamic profile is attached.

If you define the Juniper Networks authentication and authorization VSA for CoS traffic-shaping parameter values (attribute number 26–108) on the RADIUS authentication server, the RADIUS server includes the values in RADIUS Access-Accept messages it sends to the router when a subscriber successfully authenticates over the interface.

To provide an initial scheduler map name and traffic shaping parameters obtained from the RADIUS authentication server when a subscriber logs in, reference the Junos OS predefined variables for CoS listed in Table 69 on page 690 in an access dynamic profile associated with the subscriber interface.

**Table 69: CoS Predefined Variables for Scheduler Map and Traffic Shaping**

Variable	Description
\$junos-cos-scheduler-map	<p>Scheduler-map name to be dynamically configured in a traffic-control profile in the access dynamic profile when a subscriber logs in.</p> <p><b>NOTE:</b> The scheduler map referenced by the <b>scheduler-map</b> statement can be defined dynamically (at the <b>[edit dynamic-profiles profile-name class-of-service scheduler-maps]</b> hierarchy level) or statically (at the <b>[edit class-of-service scheduler-maps]</b> hierarchy level).</p>
\$junos-cos-shaping-rate	Shaping rate to be dynamically configured in a traffic-control profile in the access dynamic profile when a subscriber logs in. You can configure a RADIUS authentication server to include this information in the Accept-Accept message when a subscriber successfully authenticates over the static or dynamic subscriber interface to which the access dynamic profile is attached.
\$junos-cos-guaranteed-rate	Guaranteed rate to be dynamically configured in a traffic-control profile in the access dynamic profile when a subscriber logs in. You can configure a RADIUS authentication server to include this information in the Accept-Accept message when a subscriber successfully authenticates over the static or dynamic subscriber interface to which the access dynamic profile is attached.
\$junos-cos-delay-buffer-rate	Delay-buffer rate to be dynamically configured in a traffic-control profile in the access dynamic profile when a subscriber logs in. You can configure a RADIUS authentication server to include this information in the Accept-Accept message when a subscriber successfully authenticates over the static or dynamic subscriber interface to which the access dynamic profile is attached.

## Predefined Variables for Dynamic Configuration of Initial Scheduling and Queuing

You can configure an access dynamic profile that provides initial traffic-shaping parameters when a subscriber logs in. The Junos OS obtains this information from the



RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the access dynamic profile is attached.

If you define the Juniper Networks authentication and authorization VSA for CoS scheduling and queuing parameter values (attribute number 26–146) on the RADIUS authentication server, the RADIUS server includes the values in RADIUS Access-Accept messages it sends to the router when a subscriber successfully authenticates over the interface.

To provide an initial scheduler name and scheduler and queuing parameters obtained from the RADIUS authentication server when a subscriber logs in, reference the Junos OS predefined variables listed in Table 70 on page 691 in an access dynamic profile associated with the subscriber interface.

**Table 70: CoS Predefined Variables for Scheduling and Queuing**

Variable	Description
\$junos-cos-scheduler	Name of a scheduler to be dynamically configured in the access dynamic profile. You can configure a RADIUS authentication server to include this information in the Accept-Accept message when a subscriber successfully authenticates over the static or dynamic subscriber interface to which the access dynamic profile is attached.
\$junos-cos-scheduler-transmit-rate	Transmit rate to be dynamically configured for the scheduler in the access dynamic profile. You can configure a RADIUS authentication server to include this information in the Accept-Accept message when a subscriber successfully authenticates over the static or dynamic subscriber interface to which the access dynamic profile is attached.
\$junos-cos-scheduler-bs	Buffer size, as a percentage of total buffer, to be dynamically configured for the scheduler in the access dynamic profile. You can configure a RADIUS authentication server to include this information in the Accept-Accept message when a subscriber successfully authenticates over the static or dynamic subscriber interface to which the access dynamic profile is attached.
\$junos-cos-scheduler-pri	Packet-scheduling priority value to be dynamically configured for the scheduler in the access dynamic profile. You can configure a RADIUS authentication server to include this information in the Accept-Accept message when a subscriber successfully authenticates over the static or dynamic subscriber interface to which the access dynamic profile is attached.
\$junos-cos-scheduler-dropfile-low	<p>Name of the drop profile for RED for loss-priority level <b>low</b> to be dynamically configured for the scheduler in the access dynamic profile. You can configure a RADIUS authentication server to include this information in the Accept-Accept message when a subscriber successfully authenticates over the static or dynamic subscriber interface to which the access dynamic profile is attached.</p> <p><b>NOTE:</b> The drop profile must be configured statically (at the <b>[edit class-of-service schedulers scheduler-name drop-profiles]</b> hierarchy level) for loss-priority <b>low</b>.</p>

Table 70: CoS Predefined Variables for Scheduling and Queuing (*continued*)

Variable	Description
\$junos-cos-scheduler-dropfile-medium-low	<p>Name of the drop profile for RED for loss-priority level <b>medium-low</b> to be dynamically configured for the scheduler in the access dynamic profile. The Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the access dynamic profile is attached.</p> <p><b>NOTE:</b> The drop profile must be configured statically (at the <b>[edit class-of-service schedulers scheduler-name drop-profiles]</b> hierarchy level).</p>
\$junos-cos-scheduler-dropfile-medium-high	<p>Name of the drop profile for RED for loss-priority level <b>medium-high</b> to be dynamically configured for the scheduler in the access dynamic profile. You can configure a RADIUS authentication server to include this information in the Accept-Accept message when a subscriber successfully authenticates over the static or dynamic subscriber interface to which the access dynamic profile is attached.</p> <p><b>NOTE:</b> The drop profile must be configured statically (at the <b>[edit class-of-service schedulers scheduler-name drop-profiles]</b> hierarchy level).</p>
\$junos-cos-scheduler-dropfile-high	<p>Name of the drop profile for RED for loss-priority level <b>high</b> to be dynamically configured for the scheduler in the access dynamic profile. You can configure a RADIUS authentication server to include this information in the Accept-Accept message when a subscriber successfully authenticates over the static or dynamic subscriber interface to which the access dynamic profile is attached.</p> <p><b>NOTE:</b> The drop profile must be configured statically (at the <b>[edit class-of-service schedulers scheduler-name drop-profiles]</b> hierarchy level).</p>
\$junos-cos-scheduler-dropfile-any	<p>Name of the drop profile for RED for loss-priority level <b>any</b> to be dynamically configured for the scheduler in the access dynamic profile. You can configure a RADIUS authentication server to include this information in the Accept-Accept message when a subscriber successfully authenticates over the static or dynamic subscriber interface to which the access dynamic profile is attached.</p> <p><b>NOTE:</b> The drop profile must be configured statically (at the <b>[edit class-of-service schedulers scheduler-name drop-profiles]</b> hierarchy level).</p>

#### Related Documentation

- Subscriber Activation and Service Management in an Access Network on page 8
- Dynamic Profiles Overview on page 369
- Dynamic Variables Overview on page 371
- Junos OS Predefined Variables on page 372
- Configuring Initial CoS Parameters Dynamically Obtained from RADIUS on page 697
- Example: Configuring Initial CoS Parameters Dynamically Obtained from RADIUS on page 721

---

## 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 *subscriber 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 OS predefined 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 *subscriber service profile* that includes user-defined variables.

### Types of CoS Variables Used in a Service Profile

You can configure variables for the following CoS parameters in a 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** statements in the dynamic profile referenced by DHCP. When you specify the **aggregate-clients merge** statement, the scheduler map names specified in the dynamic profile are appended. When you

specify the **aggregate-clients replace** statement, the scheduler map names are replaced. In both cases, 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 71 on page 694 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 71: CoS Services and Variables**

Scenario	Static CoS Configuration (Single Subscriber)	Dynamic CoS Configuration (Single Subscriber)	Dynamic CoS Configuration (Multiple Subscribers Enabled on a Logical Interface with the aggregate-clients merge Statement)	Dynamic CoS Configuration (Multiple Subscribers Enabled on a Logical Interface with the aggregate-clients replace Statement)
Subscriber login	<ul style="list-style-type: none"> <li>Configure RADIUS values or default values for all parameters in access profile</li> <li>Configure scheduler map in <b>edit class-of-service</b> hierarchy and reference in access profile</li> </ul>	<ul style="list-style-type: none"> <li>Configure RADIUS values or default values for all parameters in access profile</li> <li>Configure scheduler map and schedulers in access profile</li> </ul>	<ul style="list-style-type: none"> <li>Configure RADIUS values or default values for all parameters in access profile</li> <li>Configure scheduler map and schedulers in access profile</li> </ul>	<ul style="list-style-type: none"> <li>Configure RADIUS values or default values for all parameters in access profile</li> <li>Configure scheduler map and schedulers in access profile</li> </ul>
RADIUS CoA for service or variable change	Replaces the following parameters: <ul style="list-style-type: none"> <li>Delay buffer rate</li> <li>Guaranteed rate</li> <li>Scheduler map</li> <li>Shaping rate</li> </ul>	Replaces the following parameters: <ul style="list-style-type: none"> <li>Delay buffer rate</li> <li>Guaranteed rate</li> <li>Shaping rate</li> <li>Scheduler map</li> </ul>	Combines the values of the following parameters to their maximum scalar value: <ul style="list-style-type: none"> <li>Delay buffer rate</li> <li>Guaranteed rate</li> <li>Shaping rate</li> </ul> Appends the scheduler map parameter	Replaces the following parameters: <ul style="list-style-type: none"> <li>Delay buffer rate</li> <li>Guaranteed rate</li> <li>Shaping rate</li> <li>Scheduler map</li> </ul>
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  <b>NOTE:</b> 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  <b>NOTE:</b> 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  <b>NOTE:</b> Do not instantiate a CoA request using a service dynamic profile that is already in use on the same logical interface.

**Related  
Documentation**

- [Configuring Static Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 669](#)
- [Configuring Dynamic Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 671](#)
- [Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview on page 104](#)
- [RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 39](#)
- [Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660](#)



# Configuring RADIUS for Dynamic CoS

- Configuring Initial CoS Parameters Dynamically Obtained from RADIUS on page 697
- Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 698

## Configuring 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.

1. Configure external RADIUS server VSAs with values that you expect subscribers to log in with.
  - 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 “Configuring Router or Switch Interaction with RADIUS Servers” on page 20 and “Configuring RADIUS Server Parameters for Subscriber Access” on page 26.
2. Configure a subscriber interface that supports hierarchical CoS.
  - For static VLAN interfaces, see “Configuring Static Subscriber Interfaces in Dynamic Profiles” on page 439.
  - For static VLAN interfaces over aggregated Ethernet, see “Configuring a Static or Dynamic VLAN Subscriber Interface over Aggregated Ethernet” on page 479.
  - For static IP demux interface sets, see “Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles” on page 445.
  - For dynamic IP demux interface sets, see “Configuring a Subscriber Interface Using a Set of Static IP Demux Interfaces” on page 443
3. Associate a traffic control profile with the interface.

See “Applying Traffic Shaping and Scheduling to a Subscriber Interface in a Dynamic Profile” on page 685.

4. Configuring initial traffic-shaping parameters to be obtained from RADIUS.  
See “Configuring Dynamic Traffic Shaping and Scheduling Parameters in a Dynamic Profile” on page 678.
5. Configure forwarding classes and scheduler maps statically.  
See Configuring Forwarding Classes and Configuring Scheduler Maps.
6. Configure a scheduler to specify initial scheduling and queuing parameters to be dynamically obtained from RADIUS when a subscriber logs in.  
See “Configuring Dynamic Schedulers with Variables in a Dynamic Profile” on page 681.

**Related Documentation**

- Subscriber Interfaces That Provide Initial CoS Parameters Dynamically Obtained from RADIUS on page 689
- Example: Configuring Initial CoS Parameters Dynamically Obtained from RADIUS on page 721
- Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660
- Subscriber Activation and Service Management in an Access Network on page 8
- Juniper Networks VSAs Supported by the AAA Service Framework on page 45
- Dynamic Profiles Overview on page 369
- Dynamic Variables Overview on page 371
- Junos OS Predefined Variables on page 372

---

## 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 OS predefined 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 2
```



**NOTE:** You can configure user-defined values for RADIUS tags that are different than the values that are required in access profiles with predefined variables. For example, in a dynamic service profile, you can assign the shaping rate with a tag of 1 rather than 2, which is required for the \$junos-shaping-rate variable. When you configure user-defined values, the VSA that is sent from RADIUS must share the same definition.

- 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 3
```

- 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 4
```

- 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 1
```

- 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 is 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 Documentation**
- Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660
  - Changing CoS Services Overview on page 693



# Interface Solutions for Dynamic CoS Overview

- CoS and Static IP Demux Interface Set Overview on page 703
- CoS for PPPoE Subscriber Interfaces Overview on page 704
- CoS for L2TP Subscriber Interfaces Overview on page 704

## 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 72 on page 703 shows the scheduler mapping for interface sets of IP demux interfaces.

Table 72: 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 Documentation**

- Configuring CoS on a Set of Static IP Demux Interfaces on page 709

## CoS for PPPoE Subscriber Interfaces Overview

---

You can configure CoS functionality for static and dynamic PPPoE subscriber interfaces configured on Gigabit Ethernet Intelligent Queuing 2 (IQ2) and Ethernet Enhanced IQ2 (IQ2E) PICs on the M120 and M320 routers, and on Trio MPC/MIC modules on the MX Series 3D Universal Edge Router.

For all supported hardware platforms, you can attach an output traffic control profile that contains basic shaping and scheduling properties directly to a PPPoE interface. In this type of scenario, you can use each PPPoE interface to represent a household and shape all of the household traffic to an aggregate rate. Each forwarding class is mapped to a queue, and represents one type of services provided to a household customer.

Both the IQ2E PIC and Trio MPC/MIC modules support hierarchical scheduling functionality that is not available on the IQ2 PIC. To shape customer or DSLAM traffic at different levels of the PPPoE interface hierarchy, you can attach traffic control profiles to interface sets that contain PPPoE members.

Trio MPC/MIC modules support subscriber interfaces with PPPoE encapsulation over aggregated Ethernet interfaces. These PPPoE subscriber interfaces are configured over VLAN demux interfaces, which are also configured over Aggregated Ethernet interfaces.



**NOTE:** For static PPPoE underlying logical interfaces, use PPPoE interface sets.

---

### Related Documentation

- Configuring Static Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 669
- Configuring Dynamic Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 671
- Configuring Hierarchical CoS on a Static PPPoE Subscriber Interface on page 708
- For more information about the IQ2 and IQ2 PICs, see the [Junos OS Class of Service Configuration Guide](#)

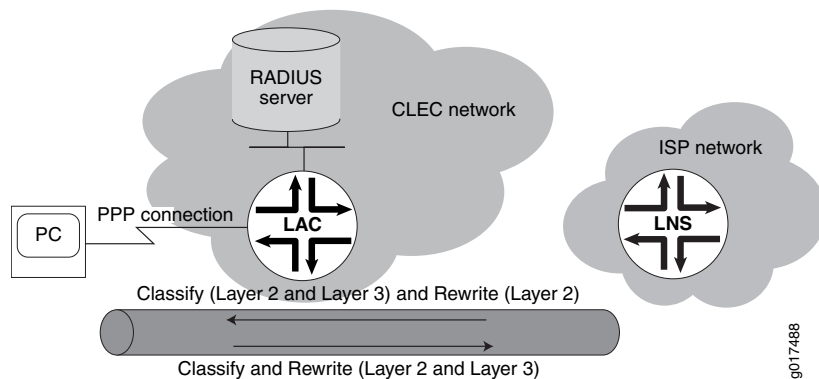
## CoS for L2TP Subscriber Interfaces Overview

---

In Layer 2 Tunnel Protocol (L2TP) configurations, IP and L2TP headers are added to packets arriving at a PPP subscriber interface on the L2TP access concentrator (LAC) before being tunneled to the L2TP network server (LNS). You can manage the IP header by configuring classifiers and rewrite-rules that transfer the ToS (Type of Service) value or the 802.1p value from the *inner* IP header to the *outer* IP header of the L2TP packet.

Figure 14 on page 705 shows the classifier and rewrite rules that you can configure from the LAC to the LNS, and from the LNS to the LAC.

Figure 14: CoS Configuration for Simple L2TP Topology



### Traffic from LAC to LNS

To set the ToS value or the 802.1p value on the inner IP header, you can configure both fixed and behavior aggregate (BA) classifiers for subscribers at Layer 2 or Layer 3 of the network.

Table 73 on page 705 lists the configuration options for applying classifiers to a subscriber interface on an ingress LAC tunnel.

Table 73: Ingress LAC Tunnel Classifier Options

Classifier	Subscriber Interface
Fixed	Either of the following: <ul style="list-style-type: none"> <li>• PPP interface</li> <li>• Underlying VLAN interface</li> </ul>
Layer 2	Either of the following: <ul style="list-style-type: none"> <li>• PPP interface</li> <li>• Underlying VLAN interface</li> </ul>
Layer 3	Family of PPP interfaces

You cannot configure a Layer 2 and fixed classifier together.

The behavior of the Layer 2 and Layer 3 classifiers depends on the configuration. For example, a Layer 3 classifier for a family of PPP interfaces overrides a Layer 2 classifier configured at the PPP interface, except for the unknown packets and control packets.

If you do not configure a classifier for Layer 2, the system applies the default Layer 3 classifier so that tunneled and terminated subscribers have the same behavior. To prevent unknown packets and control packets from being discarded, the system assigns them to the best-effort forwarding class.

## Traffic from LNS to LAC

For egress tunnels, you configure rewrite rules at the PPP interface to set the ToS or 802.1p value of the outer IP header. Rewrite rules are applied accordingly to the forwarding class, packet loss priority (PLP), and code point.

Mapping the inner IP header to the outer IP header of the L2TP packet depends on the classifier and rewrite-rule configurations. For example, Table 74 on page 706 lists the values for the classifier and rewrite rules for a VLAN interface. For assured forwarding, the inner 802.1p value (ob001) is classified with the assured-forwarding class and low loss priority at the ingress interface. Based on the assured-forwarding class and low loss priority in the rewrite rule, the ToS value in the outer IP header is set to ob001.

**Table 74: Sample Result**

Inner .1p Value	Forwarding Class	Loss Priority	Code Point	Outer ToS Value
ob000	best-effort	low	000	ob000
ob001	assured-forwarding	low	001	ob001
ob101	expedited-forwarding	low	101	ob101
ob111	network-control	low	11	ob111

**Related Documentation** • [Managing the IP Header Values for an L2TP LAC Tunnel with Dynamic CoS on page 711](#)



## Configuring Interface Solutions for Dynamic CoS

- Configuring Hierarchical CoS for a Subscriber Interface of Aggregated Ethernet Links on page 707
- Configuring Hierarchical CoS on a Static PPPoE Subscriber Interface on page 708
- Configuring CoS on a Set of Static IP Demux Interfaces on page 709
- Managing the IP Header Values for an L2TP LAC Tunnel with Dynamic CoS on page 711
- Configuring an Interface Set of Subscribers in a Dynamic Profile on page 712

### Configuring Hierarchical CoS for a Subscriber Interface of Aggregated Ethernet Links

You can enable hierarchical CoS on a subscriber interface with an underlying aggregated Ethernet interface.

Before you begin, configure the subscriber interface with aggregated Ethernet:

- For static and dynamic VLAN interfaces, see “Configuring a Static or Dynamic VLAN Subscriber Interface over Aggregated Ethernet” on page 479.
- Configure the demux subscriber interface with aggregated Ethernet.

For static and dynamic IP demux interfaces, see “Configuring a Static or Dynamic IP Demux Subscriber Interface over Aggregated Ethernet” on page 481.

For static and dynamic VLAN demux interfaces, see “Configuring a Static or Dynamic VLAN Demux Subscriber Interface over Aggregated Ethernet” on page 482.

To configure hierarchical CoS on the link aggregation (LAG) bundle:

1. Specify that you want to access the LAG bundle.

```
user@host# edit interfaces aex
```

2. Configure the link aggregation (LAG) bundle with hierarchical scheduler mode.

```
[edit interfaces aex]  
user@host# set hierarchical-scheduler
```



**BEST PRACTICE:** For VLAN subscriber interfaces, you must enable link protection on the aggregated Ethernet interface for hierarchical CoS to operate on these interfaces. See [Configuring Link Protection for Aggregated Ethernet Interfaces](#).

Link protection is not required for IP or demux subscriber interfaces. We recommend that you enable targeted distribution on the demux interface to provide accurate hierarchical scheduling for these links. See “[Providing Accurate Scheduling for a Demux Subscriber Interface of Aggregated Ethernet Links](#)” on page 761.

You can then attach static or dynamic traffic shaping and scheduling parameters at the aggregated Ethernet logical interface or its underlying physical interface. See:

- [Configuring Traffic Scheduling and Shaping for Subscriber Access](#) on page 677
- [Configuring Schedulers in a Dynamic Profile for Subscriber Access](#) on page 679
- [Applying Traffic Shaping and Scheduling to a Subscriber Interface in a Dynamic Profile](#) on page 685

**Related  
Documentation**

- [Guidelines for Configuring Dynamic CoS for Subscriber Access](#) on page 660
- [Verifying the Scheduling and Shaping Configuration for Subscriber Access](#) on page 688
- [CoS for Subscriber Access Overview](#) on page 659

---

## Configuring Hierarchical CoS on a Static PPPoE Subscriber Interface

You can configure hierarchical CoS on a static PPPoE subscriber interface.

Before you begin:

- [Configure the static PPPoE subscriber interface.](#)

See [Configuring PPPoE](#).

To configure hierarchical CoS on a static PPPoE subscriber interface:

1. Specify the PPPoE interface that you want to configure.

```
user@host# edit interfaces pppoe-interface-name
```

2. Configure the hierarchical scheduler for the interface.

```
[edit interfaces interface-name]  
user@host# set hierarchical-scheduler
```

3. (Optional) Group the PPPoE interfaces in an interface set.

```
[edit]  
user@host# edit interfaces interface-set interface-set-name
```

You can now configure static traffic and scheduling parameters for each traffic-control profile, and attach each traffic-control profile to the PPPoE interface or the PPPoE interface set. For more information, see the [Junos OS Class of Service Configuration Guide](#).

- Related Documentation**
- For hardware requirements and configuration guidelines, see Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660
  - CoS for PPPoE Subscriber Interfaces Overview on page 704
  - Example: Configuring Hierarchical Scheduling and Queuing for a Static PPPoE Subscriber Interface on page 727
  - Example: Configuring Hierarchical Scheduling and Queuing for an Underlying Static PPPoE Subscriber Interface on page 729
  - Example: Configuring Hierarchical Scheduling and Queuing for an Interface Set of Static PPPoE Subscriber Interfaces on page 731
  - Verifying the Scheduling and Shaping Configuration for Subscriber Access on page 688

## 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 a Subscriber Interface Using a Set of Static IP Demux Interfaces” on page 443.

To configure CoS on a set of static IP demux interfaces:

1. Define the CoS parameters for the interface set.

```
[edit]
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.

```
[edit]  
class-of-service {  
    interfaces {  
        interface-set demux-set1 {  
            output-traffic-control-profile t2;  
        }  
        interface-set 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 Documentation**
- For more information about interface sets and hierarchical scheduling for VLANs, see the *Junos OS Class of Service Configuration Guide*

## Managing the IP Header Values for an L2TP LAC Tunnel with Dynamic CoS

In L2TP configurations, IP and L2TP headers are added to packets arriving at a PPP subscriber interface on the LAC before being tunneled to the L2TP network server (LNS).

Classifiers and rewrite rules enable you to properly transfer the ToS (Type of Service) value or the 802.1p value from the inner IP header to the outer IP header of the L2TP packet.

To manage the IP header values for a LAC tunnel:

- Configure the classifier for the inner tunnel.
  - Define the fixed or behavior aggregate (BA) classifier.
    - To configure a fixed classifier:
 

```
[edit class-of-service interfaces interface-name unit logical-unit-number]
user@host# set forwarding-class class-name
```
    - To configure a BA classifier:
 

```
[edit class-of-service]
user@host# set classifiers (ieee-802.1 | inet-precedence) classifier-name
forwarding-class class-name loss-priority level code-points [ aliases ] [
bit-patterns]
```
  - Apply the classifier to the Layer 2 interface or Layer 3 interface. For Layer 2, you can apply the classifier at the PPP interface or an underlying VLAN interface. For Layer 3, you can apply classifiers to a family of PPP interfaces.
    - To apply the classifier for the IEEE 802.1p value:
 

```
[edit dynamic-profiles profile-name class-of-service interfaces interface-name
unit logical-unit-number classifiers]
user@host# set ieee-802.1 (classifier-name | default) vlan-tag (inner | outer)
```
    - To apply the classifier for the ToS value:
 

```
[edit dynamic-profiles profile-name class-of-service interfaces interface-name
unit logical-unit-number classifiers]
user@host# set inet-precedence (classifier-name | default)
```
- Configure the rewrite rule for the egress tunnel.
  - Configure the rewrite rule with the forwarding class and the loss priority value.
 

```
[edit class-of-service]
user@host# set rewrite-rules (ieee-802.1 | inet-precedence) rewrite-name
forwarding-class class-name loss-priority level code-point (alias | bits)
```
  - Apply the rewrite rule to the PPP interface for which the L2TP tunnel is configured.
    - To apply the rewrite-rule for the IEEE 802.1p value:

```
[edit dynamic-profiles profile-name class-of-service interfaces interface-name
  unit logical-unit-number rewrite-rules]
user@host# set ieee-802.1 (rewrite-name | default) vlan-tag (outer |
  outer-and-inner)
```

- To apply the rewrite rule for the ToS value:

```
[edit dynamic-profiles profile-name class-of-service interfaces interface-name
  unit logical-unit-number rewrite-rules]
user@host# set inet-precedence (rewrite-name | default)
```

**Related Documentation**

- Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660
- CoS for L2TP Subscriber Interfaces Overview on page 704
- Configuring an L2TP LAC on page 241

---

## Configuring an Interface Set of Subscribers in a Dynamic Profile

---

Interface sets enable you to provide hierarchical scheduling to a group of subscriber interfaces.

To configure an interface set of subscriber interfaces:

1. Configure the interface-set in the dynamic profile.

The interface-set is created dynamically when the subscriber logs in.

```
[edit dynamic-profiles profile-name interfaces]
user@host# edit interface-set $junos-interface-set-name
```

2. Include the interfaces within the dynamic interface-set.

```
[edit dynamic-profiles profile-name interfaces interface-set $junos-interface-set-name]
user@host# set interface interface-name unit logical-unit-number
```

3. Apply traffic shaping and queuing parameters to the interface set.



**TIP:** You must configure the interface set in the static [edit class-of-service] hierarchy, not in the [edit dynamic-profiles] hierarchy.

```
[edit class-of-service interfaces]
user@host# edit interface-set interface-set-name
[edit class-of-service interfaces interface-set interface-set-name]
user@host# set output-traffic-control-profile profile-name
```

**Related Documentation**

- Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660
- Example: Configuring a Dynamic Interface Set of VLAN Subscribers on page 734

# Dynamic CoS for Subscriber Access Examples

- Example: Configuring Static Hierarchical Scheduling and Queuing for Subscriber Access on page 713
- Example: Configuring Dynamic Hierarchical Scheduling and Queuing for Subscriber Access on page 715
- Example: Configuring Initial CoS Parameters Dynamically Obtained from RADIUS on page 721
- Example: Providing Unique Rate Configurations for Schedulers in a Dynamic Profile on page 724
- Example: Configuring Aggregate Scheduling of Queues for Residential Subscribers on Static IP Demux Interfaces on page 725
- Example: Configuring Hierarchical Scheduling and Queuing for a Static PPPoE Subscriber Interface on page 727
- Example: Configuring Hierarchical Scheduling and Queuing for an Underlying Static PPPoE Subscriber Interface on page 729
- Example: Configuring Hierarchical Scheduling and Queuing for an Interface Set of Static PPPoE Subscriber Interfaces on page 731
- Example: Configuring a Dynamic Interface Set of VLAN Subscribers on page 734

## Example: Configuring Static Hierarchical 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 Dynamic Hierarchical 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 RADIUS administrator supplies the initial values on the RADIUS server, and the service activation is performed at subscriber 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 VLAN interface for the access profile.

```

[edit]
dynamic-profiles access-profile {
  interfaces {
    $junos-interface-ifd-name {
      unit $junos-underlying-interface-unit {
        family inet;
      }
    }
  }
}

```

- b. Configure the class of service parameters in the access profile. In this example, you configure Junos OS predefined variables that provide the initial scheduler name and scheduler parameters obtained from the RADIUS authentication server when the subscriber logs in.

Include the configurations for the interfaces, schedulers, and the scheduler maps.

```

[edit]
dynamic-profiles access-profile {
  class-of-service {
    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;
      }
    }
  }
  interfaces {

```

```

$junos-interface-ifd-name {
  unit "$junos-underlying-interface-unit" {
    classifiers {
      ieee-802.1 l2_classifier;
    }
    rewrite-rules {
      ieee-802.1 l2_rewrite;
    }
    output-traffic-control-profile tcp1;
  }
}
schedulers {
  $junos-cos-scheduler {
    buffer-size percent $junos-cos-scheduler-bs;
    priority $junos-cos-scheduler-pri;
    transmit-rate percent $junos-cos-scheduler-tx;
    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;
  }
}
scheduler-maps {
  data_voice_smap {
    forwarding-class be scheduler be_sch;
    forwarding-class ef scheduler ef_sch;
  }
}
}

```

Table 75 on page 716 lists the initial values defined by the RADIUS administrator for the scheduler map and shaping rates.

**Table 75: Initial Scheduler Map and Shaping Values at Subscriber Login**

Predefined Variable	RADIUS Tag	Value
\$junos-cos-scheduler-map	T01	data_voice_smap
\$junos-cos-shaping-rate	T02	6m
\$junos-cos-guaranteed-rate	T03	4m
\$junos-cos-delay-buffer-rate	T04	4m

Table 76 on page 717 lists the initial values defined by the RADIUS administrator for the voice (expedited forwarding) scheduler.

**Table 76: Initial CoS Values for the Voice Scheduler at Subscriber Login**

Predefined Variable	Tag	Value
\$junos-cos-scheduler	—	ef_sch
\$junos-cos-scheduler-tx	T01	10
\$junos-cos-scheduler-bs	T02	10
\$junos-cos-scheduler-pri	T03	medium-high
\$junos-cos-scheduler-dropfile-low	T04	d3
\$junos-cos-scheduler-dropfile-medium-low	T05	d2
\$junos-cos-scheduler-dropfile-medium-high	T06	d1
\$junos-cos-scheduler-dropfile-high	T07	d0

Table 77 on page 717 lists the initial values defined by the RADIUS administrator for the data (best effort) scheduler.

**Table 77: Initial CoS Values for the Data Scheduler at Subscriber Login**

Predefined Variable	Tag	Value
\$junos-cos-scheduler	—	be_sch
\$junos-cos-scheduler-tx	T01	10
\$junos-cos-scheduler-bs	T02	10
\$junos-cos-scheduler-pri	T03	low
\$junos-cos-scheduler-dropfile-low	T04	d0
\$junos-cos-scheduler-dropfile-medium-low	T05	d1
\$junos-cos-scheduler-dropfile-medium-high	T06	d2
\$junos-cos-scheduler-dropfile-high	T07	d3

2. Configure the classifiers, drop profiles, forwarding classes, and rewrite rules in the static **[edit class-of-service]** hierarchy.

```
[edit]
class-of-service {
  classifiers {
    dscp dscp_classifier {
      forwarding-class be {
```

```
        loss-priority low code-points 000000;
    }
    forwarding-class af {
        loss-priority medium-low code-points 000001;
    }
}
ieee-802.1 l2_classifier {
    forwarding-class be {
        loss-priority medium-low code-points 000;
    }
    forwarding-class ef {
        loss-priority medium-low code-points 100;
    }
    forwarding-class af {
        loss-priority medium-low code-points 010;
    }
}
}
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;
    }
}
rewrite-rules {
    ieee-802.1 l2_rewrite {
        forwarding-class be {
            loss-priority medium-low code-point 000;
        }
        forwarding-class ef {
            loss-priority medium-low code-point 001;
        }
        forwarding-class af {
```

```

        loss-priority medium-low code-point 100;
    }
    dscp l2_rewrite {
        forwarding-class be {
            loss-priority medium-low code-points 000;
        }
        forwarding-class ef {
            loss-priority medium-low code-points 001;
        }
        forwarding-class af {
            loss-priority medium-low code-points 001;
        }
    }
}

```

3. Configure the service profile enable RADIUS to activate the video service after login. The video service corresponds to assured forwarding PHB.

In this example, you configure Junos OS predefined variables that provide the initial scheduler name and scheduler parameters obtained from the RADIUS authentication server when the subscriber logs in.

```

[edit]
dynamic-profiles service-af {
    variables {
        af_fc default-value video;
        af_sch default-value af_sch;
        sch-drop-any default-value all;
        sch-pri-2 default-value strict-high;
        sch-bs-2 default-value 40;
        sch-tx-2 default-value 3m;
        smap default-value any
    }
    class-of-service {
        scheduler-maps {
            "$smap" {
                forwarding-class "$af_fc" scheduler "$af_sch";
            }
        }
        schedulers {
            "$af_sch" {
                transmit-rate percent "$sch-tx-2";
                buffer-size percent "$sch-bs-2";
                priority "$sch-pri-2";
                drop-profile-map loss-priority any protocol any drop-profile "$sch-drop-any";
            }
        }
    }
}

```

After the three services are activated, subscribers receive upgraded values for the 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 78 on page 720 lists the upgraded values defined by the RADIUS administrator.

**Table 78: Upgraded CoS Values for the Video Service**

Variable	RADIUS Tag	Value
junos-cos-scheduler-map	T01	data_voice_smap
junos-cos-shaping-rate	T02	14m
junos-cos-guaranteed-rate	T03	13m
junos-cos-delay-buffer-rate	T04	12m

Table 79 on page 720 lists the values defined by the RADIUS administrator for the video (assured forwarding) scheduler.

**Table 79: Upgraded CoS Values for the Video Scheduler**

Predefined Variable	Tag	Value
\$junos-cos-scheduler	—	af_sch
\$junos-cos-scheduler-tx	T01	10
\$junos-cos-scheduler-bs	T02	10
\$junos-cos-scheduler-pri	T03	medium
\$junos-cos-scheduler-dropfile-low	T04	d3
\$junos-cos-scheduler-dropfile-medium-low	T05	d2
\$junos-cos-scheduler-dropfile-medium-high	T06	d1
\$junos-cos-scheduler-dropfile-high	T07	d0

Table 80 on page 720 lists the values defined by the RADIUS administrator for the expedited forwarding scheduler in the CoA message. The values are the same as the initial service.

**Table 80: Initial CoS Values for the Expedited Forwarding Scheduler at Subscriber Login**

Predefined Variable	Tag	Value
\$junos-cos-scheduler	—	ef_sch
\$junos-cos-scheduler-tx	T01	10
\$junos-cos-scheduler-bs	T02	10
\$junos-cos-scheduler-pri	T03	medium-high

**Table 80: Initial CoS Values for the Expedited Forwarding Scheduler at Subscriber Login (*continued*)**

Predefined Variable	Tag	Value
\$junos-cos-scheduler-dropfile-low	T04	d3
\$junos-cos-scheduler-dropfile-medium-low	T05	d2
\$junos-cos-scheduler-dropfile-medium-high	T06	d1
\$junos-cos-scheduler-dropfile-high	T07	d0

Table 81 on page 721 lists the values defined by the RADIUS administrator for the best effort scheduler in the CoA message. The values are the same as the initial service.

**Table 81: Initial CoS Values for the Best Effort Scheduler at Subscriber Login**

Predefined Variable	Tag	Value
\$junos-cos-scheduler	—	be_sch
\$junos-cos-scheduler-tx	T01	10
\$junos-cos-scheduler-bs	T02	10
\$junos-cos-scheduler-pri	T03	low
\$junos-cos-scheduler-dropfile-low	T04	d0
\$junos-cos-scheduler-dropfile-medium-low	T05	d1
\$junos-cos-scheduler-dropfile-medium-high	T06	d2
\$junos-cos-scheduler-dropfile-high	T07	d3

**Related  
Documentation**

- [Changing CoS Services Overview on page 693](#)
- [Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 698](#)

## Example: Configuring Initial CoS Parameters Dynamically Obtained from RADIUS

The following configuration is an example of a client dynamic profile in which initial CoS parameters are dynamically obtained from the RADIUS server when a subscriber authenticates over the interface to which the dynamic profile is applied.

For this example, assume that the RADIUS authentication server has been configured with traffic-shaping parameters (at Juniper Networks VSA 26-108) and CoS scheduling and queuing parameters (at Juniper Networks VSA 26-146).

The subscriber interface is a single-unit static gigabit Ethernet VLAN interface on an EQ DPC port:

```
[edit]
interfaces {
  ge-9/0/3 {
    hierarchical-scheduler;
    vlan-tagging;
    unit 100 {
      vlan-id 100;
      family inet {
        address 192.168.32.2/24;
      }
    }
  }
}
```

The client dynamic profile **residential\_silver** attaches the traffic-control profile **tcp\_1** to the subscriber interface that is defined in the dynamic profile using the **\$junos-interface-ifd-name** predefined variable.

```
[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 tcp_1;
          }
        }
      }
    }
  }
}
```

The traffic-control profile **tcp\_1**, references Junos OS predefined variables to obtain a scheduler-map name and traffic-shaping parameter values from RADIUS when a subscriber logs in. For this example, assume that the RADIUS server replaces the Junos OS predefined variable **\$junos-cos-scheduler-map** scheduler-map name **business\_smap\_1**. The scheduler map **business\_smap\_1** is configured in the client dynamic profile:

```
[edit]
dynamic-profiles {
  residential_silver {
    class-of-service {
      traffic-control-profiles {
        tcp_1 {
          scheduler-map "$junos-cos-scheduler-map"; # 'business_smap_1'
          shaping-rate "$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 best-effort scheduler be_sched;
        forwarding-class ef scheduler home_sched
    }
}
}
}
}

```

A scheduler definition references Junos OS predefined variables to obtain scheduler configurations from RADIUS when a subscriber logs in. For this example, assume that the RADIUS server provides scheduler configurations for schedulers named **be\_sched** and **home\_sched**, which are included in the scheduler map **business\_smap\_1**:

```

[edit]
dynamic-profiles {
    residential_silver {
        class-of-service {
            schedulers {
                "$junos-cos-scheduler" { # 'be_sched' and 'home_sched'
                    transmit-rate "$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";
                }
            }
        }
    }
}

```

Static configurations for CoS consist of configurations for the forwarding classes used in the scheduler map **business\_smap\_1** and configurations for drop-profile names provided by RADIUS for as part of the scheduler configurations provided (for **be\_sched** and **home\_sched**) when a subscriber logs in:

```

[edit]
class-of-service {
    forwarding-classes {
        queue 0 best-effort;
        queue 1 ef;
    }
    drop-profiles {
        ... configurations_for_drop_profile_names_provided_by_RADIUS ...
    }
}

```

```
}
```

**Related Documentation**

- Subscriber Activation and Service Management in an Access Network on page 8
- Dynamic Profiles Overview on page 369
- Dynamic Variables Overview on page 371
- Junos OS Predefined Variables on page 372
- Subscriber Interfaces That Provide Initial CoS Parameters Dynamically Obtained from RADIUS on page 689
- Configuring Initial CoS Parameters Dynamically Obtained from RADIUS on page 697

---

## Example: Providing Unique Rate Configurations for Schedulers in a Dynamic Profile

---

Combining static and dynamic schedulers in a dynamic profile enables you to provide subscribers with services that have unique scheduler definitions.

In this example, the network administrator configures the data service with a **transmit-rate** that is rate controlled using the **\$junos-cos-scheduler-tx** predefined variable. RADIUS dynamically supplies the percentage value for the transmission rate that is specified in the RADIUS VSA to the data scheduler when the subscriber logs in.

For the best-effort service, the network administrator assigns the remaining transmission rate that is available.

```
schedulers {
  data-scheduler {
    transmit-rate percent rate-limit $junos-cos-scheduler-tx;
    buffer-size percent $junos-cos-scheduler-bs;
    priority $junos-cos-scheduler-pri;
    drop-profile-map loss-priority low protocol any drop-profile d0;
    drop-profile-map loss-priority medium-low protocol any drop-profile d1;
    drop-profile-map loss-priority medium-high protocol any drop-profile d2;
    drop-profile-map loss-priority high protocol any drop-profile d3;
    drop-profile-map loss-priority any protocol any drop-profile all;
  }
  best-effort-scheduler {
    transmit-rate remainder;
    buffer-size percent $junos-cos-scheduler-bs;
    priority medium-high;
    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 d1;
    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 d3;
    drop-profile-map loss-priority any protocol any drop-profile
      $junos-cos-scheduler-dropfile-any;
  }
}
```

## 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 multiplex 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.

```
[edit]
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 {
        address 1.1.1.1/24;
        demux-source {
          1.1.1.0/24;
        }
      }
    }
    unit 1 {
      demux-options {
        underlying-interface ge-2/0/1.1;
      }
      family inet {
        address 1.1.2.1/24;
        demux-source {
          1.1.2.0/24;
        }
      }
    }
  }
}
class-of-service {
```

```
traffic-control-profiles {
  T1 {
    scheduler-map m1;
    shaping-rate 5m;
  }
  T2 {
    shaping-rate 60m;
  }
}
interfaces {
  interface-set 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 Hierarchical Scheduling and Queuing for a Static PPPoE Subscriber Interface

In this example, the network administrator defines hierarchical queuing and scheduler parameters by configuring traffic control profile and binding it directly to a PPPoE subscriber interface.

This configuration is supported on the IQ2E PIC.

To use this configuration in a broadband access network, each forwarding class can represent one type of services provided to a household customer and is mapped to a queue. Each PPPoE interface represents a household and provides shaping of all household traffic to an aggregate rate. All of the PPPoE interfaces on the physical interfaces are shaped to the underlying physical interface rate.

Table 82 on page 727 lists the scheduler and queue mapping for this configuration.

**Table 82: Scheduler Per Logical Interface Mapping**

Level	Type	Mapping
4	Queue	PPPoE interface
3	Scheduler	PPPoE interface
2	Scheduler	—
1	Scheduler	Underlying physical interface

```

interfaces {
  ge-3/0/3 {
    hierarchical-scheduler;
    vlan-tagging;
    unit 0 {
      encapsulation ppp-over-ether;
      vlan-id 100;
    }
  }
  pp0 {
    unit 0 {
      pppoe-options {
        underlying-interface ge-3/0/3.0;
        server;
      }
      family inet {
        address 120.20.20.20/32 {
          destination 120.20.20.21;
        }
      }
    }
    unit 1 {
      pppoe-options {

```

```
        underlying-interface ge-3/0/3.0;
        server;
    }
    family inet {
        address 130.30.30.30/32 {
            destination 130.30.30.31;
        }
    }
}
unit 2 {
    pppoe-options {
        underlying-interface ge-3/0/3.0;
        server;
    }
    family inet {
        address 140.40.40.40/32 {
            destination 140.40.40.41;
        }
    }
}
}
}
class-of-service {
    traffic-control-profiles {
        tcp {
            scheduler-map data_smap;
            shaping-rate 50k;
            guaranteed-rate 10k;
        }
    }
}
interfaces {
    pp0 {
        unit 0 {
            output-traffic-control-profile tcp;
        }
        unit 1 {
            output-traffic-control-profile tcp;
        }
        unit 2 {
            output-traffic-control-profile tcp;
        }
    }
    forwarding-classes {
        queue 0 be;
        queue 1 ef;
        queue 3 nc;
        queue 2 af;
    }
    scheduler-maps {
        data_smap {
            forwarding-class be scheduler be_sch;
        }
        voice_data_smap {
            forwarding-class be scheduler be_sch;
        }
        vid_data_smap {
```

```

        forwarding-class ef scheduler ef_sch;
    }
}
schedulers {
    be_sch {
        transmit-rate percent 10;
        buffer-size remainder;
        priority low;
    }
    ef_sch {
        transmit-rate percent 10;
        buffer-size remainder;
        priority low;
    }
    af_sch {
        transmit-rate percent 10;
        buffer-size remainder;
        priority low;
    }
    nc_sch {
        transmit-rate percent 10;
        buffer-size remainder;
        priority low;
    }
}

```

- Related Documentation**
- CoS for PPPoE Subscriber Interfaces Overview on page 704
  - Configuring Hierarchical CoS on a Static PPPoE Subscriber Interface on page 708

## Example: Configuring Hierarchical Scheduling and Queuing for an Underlying Static PPPoE Subscriber Interface

In this example, the network administrator defines hierarchical queues and scheduler parameters by configuring a traffic control profile and binding it directly to a PPPoE subscriber interface. The network administrator then configures the traffic control profile on the underlying interface where a group of PPPoE interfaces reside.

This configuration is supported on the IQ2E PIC.

To use this configuration in a broadband access network, each forwarding class represents one type of services provided to a household customer and is mapped to a queue. Each PPPoE interface represents a household and provides shaping of all household traffic to an aggregate rate. The underlying logical interface where a group of PPPoE interfaces resides represents a DSLAM and provides shaping to the DSLAM rate.

Table 83 on page 729 lists the scheduler and queue mapping for this configuration.

**Table 83: Scheduler per Underlying Interface Mapping**

Level	Type	Mapping
4	Queue	PPPoE interface

Table 83: Scheduler per Underlying Interface Mapping (*continued*)

Level	Type	Mapping
3	Scheduler	PPPoE interface
2	Scheduler	Underlying logical interface
1	Scheduler	Underlying interface

```

interfaces {
  ge-3/0/3 {
    hierarchical-scheduler;
    vlan-tagging;
    unit 0 {
      encapsulation ppp-over-ether;
      vlan-id 100;
    }
    unit 1 {
      vlan-id 101;
    }
  }
  pp0 {
    hierarchical-scheduler;
    unit 0 {
      pppoe-options {
        underlying-interface ge-3/0/3.0;
        server;
      }
      family inet {
        address 120.20.20.20/32 {
          destination 120.20.20.21;
        }
      }
    }
    unit 1 {
      pppoe-options {
        underlying-interface ge-3/0/3.0;
        server;
      }
      family inet {
        address 130.30.30.30/32 {
          destination 130.30.30.31;
        }
      }
    }
    unit 2 {
      pppoe-options {
        underlying-interface ge-3/0/3.0;
        server;
      }
      family inet {
        address 140.40.40.40/32 {
          destination 140.40.40.41;
        }
      }
    }
  }
}

```



```

    }
  }
}
class-of-service {
  traffic-control-profiles {
    tcp1 {
      scheduler-map data_smap;
      shaping-rate 50k;
      guaranteed-rate 10k;
    }
    tcp2 {
      scheduler-map data_smap;
      shaping-rate 50m;
      guaranteed-rate 10m;
    }
  }
}
interfaces {
  pp0 {
    unit 0 {
      output-traffic-control-profile tcp1;
    }
    unit 1 {
      output-traffic-control-profile tcp1;
    }
    unit 2 {
      output-traffic-control-profile tcp1;
    }
    ge-3/0/3 {
      unit 0 {
        output-traffic-control-profile tcp2;
      }
    }
  }
  ...
}

```

- Related Documentation**
- [CoS for PPPoE Subscriber Interfaces Overview on page 704](#)
  - [Configuring Hierarchical CoS on a Static PPPoE Subscriber Interface on page 708](#)

## Example: Configuring Hierarchical Scheduling and Queuing for an Interface Set of Static PPPoE Subscriber Interfaces

In this example, the network administrator defines hierarchical queues and scheduler parameters by configuring traffic-control profile and binding it directly to a PPPoE subscriber interface. The network administrator then configures the traffic-control profile on a set of PPPoE interfaces.

This configuration is supported on the IQ2E PIC.

To use this configuration in a broadband access network, each forwarding class represents one type of services provided to a household customer and is mapped to a queue. Each

PPPoE interface represents a household and provides shaping of all household traffic to an aggregate rate. In addition, the PPPoE interface-set configuration provides shaping of traffic for a group of PPPoE interface on a DSLAM to a DSLAM aggregate rate.

Table 84 on page 732 lists the scheduler and queue mapping for this configuration.

**Table 84: Scheduler per Logical Interface with Interface Set Mapping**

Level	Type	Mapping
4	Queue	PPPoE interface
3	Scheduler	PPPoE interface
2	Scheduler	Set of PPPoE interfaces
1	Scheduler	Underlying physical interface

```

interfaces {
  interface-set iflset1 {
    interface pp0 {
      unit 0;
      unit 1;
      unit 2;
    }
  }
  pp0 {
    unit 0 {
      pppoe-options {
        underlying-interface ge-3/0/3.0;
        server;
      }
      family inet {
        address 120.20.20.20/32 {
          destination 120.20.20.21;
        }
      }
    }
    unit 1 {
      pppoe-options {
        underlying-interface ge-3/0/3.0;
        server;
      }
      family inet {
        address 130.30.30.30/32 {
          destination 130.30.30.31;
        }
      }
    }
    unit 2 {
      pppoe-options {
        underlying-interface ge-3/0/3.0;
        server;
      }
    }
  }
}

```

```

        family inet {
            address 140.40.40.40/32 {
                destination 140.40.40.41;
            }
        }
    }
}
ge-3/0/3 {
    hierarchical-scheduler;
    vlan-tagging;
    unit 0 {
        encapsulation ppp-over-ether;
        vlan-id 100;
    }
    unit 1 {
        vlan-id 101;
    }
    unit 2 {
        vlan-id 102;
    }
}
}
class-of-service {
    traffic-control-profiles {
        tcp1 {
            scheduler-map data_smap;
            shaping-rate 50k;
            guaranteed-rate 10k;
        }
        tcp2 {
            scheduler-map data_smap;
            shaping-rate 50m;
            guaranteed-rate 10m;
        }
    }
}
interfaces {
    pp0 {
        unit 0 {
            output-traffic-control-profile tcp1;
        }
        unit 1 {
            output-traffic-control-profile tcp1;
        }
        unit 2 {
            output-traffic-control-profile tcp1;
        }
        interface-set iflset1 {
            output-traffic-control-profile tcp2;
        }
        ...
    }
}

```

- Related Documentation**
- CoS for PPPoE Subscriber Interfaces Overview on page 704
  - Configuring Hierarchical CoS on a Static PPPoE Subscriber Interface on page 708

## Example: Configuring a Dynamic Interface Set of VLAN Subscribers

---

- Requirements on page 734
- Overview on page 734
- Configuring the Dynamic VLANs on page 734
- Configuring Dynamic Traffic Scheduling and Shaping on page 736
- Configuring the Interface Set in the Dynamic Profile on page 739
- Configuring DHCP Access on page 740
- Configuring RADIUS Authentication on page 741
- Verification on page 746

### Requirements

This example uses the following software and hardware components:

- Junos OS Release 10.4
- MX Series Router with Trio MPC/MIC interfaces

### Overview

In this example, the network administrator groups dynamic VLAN interfaces in an interface set. The interface set is configured in a dynamic profile, and enables hierarchical scheduling for the VLAN interfaces for a multiplay service.

DHCP is used as the access method, and RADIUS is used as the authentication method for the interfaces associated with the interface set.

### Configuring the Dynamic VLANs

**CLI Quick Configuration** To quickly configure the dynamic VLANs, copy the following commands and paste them into the router terminal window:

```
[edit]
edit dynamic-profiles vlan-prof
edit interfaces $junos-interface-ifd-name unit $junos-interface-unit
set vlan-id $junos-vlan-id
set demux-source inet
set family inet unnumbered-address lo0.0 preferred-source-address 100.20.32.2
top
edit interfaces ge-1/0/0
set hierarchical-scheduler
set vlan-tagging
edit auto-configure vlan-ranges dynamic-profile vlan-prof
set ranges any
set accept inet
top
set interfaces lo0 unit 0 family inet address 100.20.32.2/32
```

### Configuring the Dynamic Profile for the Autoconfigured VLANs

**Step-by-Step Procedure** In this section, you create a dynamic profile for the VLAN IDs to be automatically assigned when subscribers log in.

To configure the dynamic profile for the VLANs:

1. Configure the dynamic profile.  

```
[edit]
user@host#edit dynamic-profile vlan-prof
```
2. Configure the interfaces.  

```
[edit dynamic-profiles vlan-prof]
user@host#edit interfaces $junos-interface-ifd-name unit $junos-interface-unit
```
3. Add the VLAN ID variable.  

```
[edit dynamic-profiles vlan-prof interfaces $junos-interface-ifd-name unit
$junos-interface-unit]
user@host#set vlan-id $junos-vlan-id
```
4. Configure the demux source as IPv4.  

```
[edit dynamic-profiles vlan-prof interfaces $junos-interface-ifd-name unit
$junos-interface-unit]
user@host#set demux-source inet
```
5. Configure the family.  

```
[edit dynamic-profiles vlan-prof interfaces $junos-interface-ifd-name unit
$junos-interface-unit]
user@host#set family inet unnumbered-address lo0.0 preferred-source-address
100.20.32.2
```

### Configuring the VLAN Interfaces

**Step-by-Step Procedure** To configure the VLAN interfaces:

1. Create the VLAN interface.  

```
[edit]
user@host# edit interfaces ge-1/0/0
```
2. Enable hierarchical scheduling.  

```
[edit interfaces ge-1/0/0]
user@host# set hierarchical-scheduler
```
3. Configure VLAN tagging.  

```
[edit interfaces ge-1/0/0]
user@host# set vlan-tagging
```
4. Configure auto-configuration for the dynamic profile.  

```
[edit interfaces ge-1/0/0]
user@host# edit auto-configure vlan-ranges dynamic-profile vlan-prof
```
5. Configure any VLAN ID range.

```
[edit interfaces ge-1/0/0 auto-configure vlan-ranges dynamic-profile vlan-prof]
user@host# set ranges any
```

6. Specify IPv4 traffic for the VLAN.

```
[edit interfaces ge-1/0/0 auto-configure vlan-ranges dynamic-profile vlan-prof]
user@host# set accept inet
```

---

### Configuring the Loopback Interface

#### Step-by-Step Procedure

To configure the loopback interface:

1. Create the loopback interface.

```
[edit]
user@host# edit interfaces lo0
```

2. Configure the unit and the family.

```
[edit interfaces lo0]
user@host# set unit 0 family inet address 100.20.32.2/32
```

### Configuring Dynamic Traffic Scheduling and Shaping

#### CLI Quick Configuration

To quickly configure the traffic scheduling and shaping parameters, copy the following commands and paste them into the router terminal window:

```
[edit]
edit dynamic-profiles multiplay class-of-service schedulers be_sch
set transmit-rate percent 12
set buffer-size percent 12
set priority low
up
edit ef_sch
set transmit-rate percent 12
set buffer-size percent 12
set priority low
up
edit af_sch
set transmit-rate percent 12
set buffer-size percent 12
set priority low
up
edit nc_sch
set transmit-rate percent 12
set buffer-size percent 12
set priority low
up
edit voice_sch
set transmit-rate percent 12
set buffer-size percent 12
set priority low
up
edit video_sch
set transmit-rate percent 12
set buffer-size percent 12
set priority low
```

```

up
edit game_sch
set transmit-rate percent 12
set buffer-size percent 12
set priority low
up
edit data_sch
set transmit-rate percent 12
set buffer-size percent 12
set priority low
up 2
edit scheduler-maps all_smap
set forwarding-class be scheduler be_sch
set forwarding-class ef scheduler ef_sch
set forwarding-class af scheduler af_sch
set forwarding-class nc scheduler nc_sch
set forwarding-class voice scheduler voice_sch
set forwarding-class video scheduler video_sch
set forwarding-class game scheduler game_sch
set forwarding-class data scheduler data_sch
up 2
edit traffic-control-profiles multiplay
set scheduler-map all_smap
set shaping-rate 100m
set guaranteed-rate 20m

```

### Configuring the Schedulers in the Dynamic Profile

**Step-by-Step Procedure** In this section, you create a dynamic profile for the multiplay service and configure scheduling and shaping.

To configure the schedulers:

1. Create the **multiplay** dynamic profile.  

```

[edit]
user@host# edit dynamic-profiles multiplay class-of-service schedulers

```
2. Configure the best effort scheduler.  

```

[edit dynamic-profiles multiplay class-of-service schedulers]
user@host# edit be_sch
user@host# set transmit-rate percent 12
user@host# set buffer-size percent 12
user@host# set priority low

```
3. Configure the expedited forwarding scheduler.  

```

[edit dynamic-profiles multiplay class-of-service schedulers]
user@host# edit ef_sch
user@host# set transmit-rate percent 12
user@host# set buffer-size percent 12
user@host# set priority low

```
4. Configure the assured forwarding scheduler.  

```

[edit dynamic-profiles multiplay class-of-service schedulers]
user@host# edit af_sch

```

```
user@host# set transmit-rate percent 12
user@host# set buffer-size percent 12
user@host# set priority low
```

5. Configure the network control scheduler.

```
[edit dynamic-profiles multiplay class-of-service schedulers]
user@host# edit nc_sch
user@host# set transmit-rate percent 12
user@host# set buffer-size percent 12
user@host# set priority low
```

6. Configure the voice scheduler.

```
[edit dynamic-profiles multiplay class-of-service schedulers]
user@host# edit voice_sch
user@host# set transmit-rate percent 12
user@host# set buffer-size percent 12
user@host# set priority low
```

7. Configure the video scheduler.

```
[edit dynamic-profiles multiplay class-of-service schedulers]
user@host# edit video_sch
user@host# set transmit-rate percent 12
user@host# set buffer-size percent 12
user@host# set priority low
```

8. Configure the gaming scheduler.

```
[edit dynamic-profiles multiplay class-of-service schedulers]
user@host# edit game_sch
user@host# set transmit-rate percent 12
user@host# set buffer-size percent 12
user@host# set priority low
```

9. Configure the data scheduler.

```
[edit dynamic-profiles multiplay class-of-service schedulers]
user@host# edit data_sch
user@host# set transmit-rate percent 12
user@host# set buffer-size percent 12
user@host# set priority low
```

---

### Configuring the Scheduler Map in the Dynamic Profile

---

#### Step-by-Step Procedure

To configure the scheduler map:

1. Configure the scheduler map for all of the services.

```
[edit dynamic-profiles multiplay class-of-service]
user@host# edit scheduler-maps all_smap
```

2. Configure the forwarding classes for each service in the scheduler map.

```
[edit dynamic-profiles multiplay class-of-service scheduler-maps all_smap]
user@host# set forwarding-class be scheduler be_sch
user@host# set forwarding-class ef scheduler ef_sch
user@host# set forwarding-class af scheduler af_sch
user@host# set forwarding-class nc scheduler nc_sch
```



```

user@host# set forwarding-class voice scheduler voice_sch
user@host# set forwarding-class video scheduler video_sch
user@host# set forwarding-class game scheduler game_sch
user@host# set forwarding-class data scheduler data_sch

```

### Configuring the Traffic-Control Profile in the Dynamic Profile

#### Step-by-Step Procedure

To configure the traffic-control profile the interface set:

1. Configure the traffic-control profile.  

```

[edit dynamic-profiles multiplay class-of-service]
user@host# edit traffic control-profiles multiplay

```
2. Configure the scheduler map.  

```

[edit dynamic-profiles multiplay class-of-service traffic control-profiles multiplay]
user@host# set scheduler-map all_smap

```
3. Configure the shaping rate.  

```

[edit dynamic-profiles multiplay class-of-service traffic control-profiles multiplay]
user@host# set shaping-rate 100m

```
4. Configure the guaranteed rate.  

```

[edit dynamic-profiles multiplay class-of-service traffic control-profiles multiplay]
user@host# set guaranteed-rate 20m

```

### Configuring the Interface Set in the Dynamic Profile

#### CLI Quick Configuration

To quickly configure the interface set, copy the following commands and paste them into the router terminal window:

```

[edit]
edit dynamic-profiles multiplay
edit interfaces interface-set $junos-interface-set-name
set interface $junos-interface-ifd-name unit $junos-underlying-interface-unit
top
edit class-of-service interfaces interface-set
set output-traffic-control-profile multiplay

```

### Configuring the Interfaces for the Interface Set

#### Step-by-Step Procedure

To configure the interface variable for the interface set:

1. Configure the dynamic profile for the interface set.  

```

[edit]
user@host#edit dynamic-profiles multiplay

```
2. Configure the interface using the Junos OS predefined variable.  

```

[edit dynamic-profiles multiplay]
user@host#edit interfaces $junos-interface-ifd-name unit
$junos-underlying-interface-unit

```
3. Configure the family.

```
[edit dynamic-profiles multiplay interfaces $junos-interface-set-name unit
$junos-underlying-interface-unit]
user@host#set family inet unnumbered-address lo0.0 preferred-source-address
100.20.32.2
```

---

### Configuring the Interface Set

#### Step-by-Step Procedure

To configure the interface set:

1. Configure the interface set using the Junos OS predefined variable.

```
[edit dynamic-profiles multiplay]
user@host#edit interfaces interface-set $junos-interface-set-name
```

2. Add the dynamic VLAN interfaces to the interface set.

```
[edit dynamic-profiles multiplay interfaces $junos-interface-set-name]
user@host#set interface $junos-interface-ifd-name unit
$junos-underlying-interface-unit
```

---

### Applying the Traffic Control Profile to the Interface Set

#### Step-by-Step Procedure

You apply the traffic control profile outside of the dynamic profile in the **[edit class-of-service]** hierarchy.

To apply the traffic-control profile:

1. Specify the interface set to which you want to apply the traffic control profile.

```
[edit class-of-service]
user@host#edit interfaces interface-set dynamic-set
```

2. Attach the output-traffic control profile defined in the dynamic profile to the interface set.

```
[edit class-of-service interfaces]
user@host#set output-traffic-control-profile multiplay
```

## Configuring DHCP Access

#### CLI Quick Configuration

To quickly configure DHCP access, copy the following commands and paste them into the router terminal window:

```
[edit]
edit system services dhcp-local-server authentication
set password multiplay
set username-include user-prefix multiplay
up 1
set dynamic-profile dhcp-vlan-prof aggregate-clients replace
set group vlans interface ge-1/0/0
top
edit access address-assignment pool v4 family inet
set network 100.20.0.0/16
set range limited low 100.20.0.10
set range limited high 100.20.128.250
set dhcp-attributes maximum-lease-time 84600
```

### Configuring the DHCP Local Server

#### Step-by-Step Procedure

To configure DHCP access:

1. Configure the DHCP local server.  

```
[edit system]
user@host# edit services dhcp-local-server authentication
```
2. Set the password.  

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

```
[edit system services dhcp-local-server authentication]
user@host# set username-include user-prefix multiplay
```
4. Attach the dynamic profile with the interface set.  

```
[edit system services dhcp-local-server]
user@host# set dynamic-profile dhcp-vlan-prof aggregate-clients replace
```
5. Configure a group for the VLAN interface.  

```
[edit system services dhcp-local-server]
user@host# set group vlans interface ge-1/0/0
```

### Configuring Address Assignment Pools

#### Step-by-Step Procedure

To configure address assignment pools:

1. Configure the pool of IPv4 addresses.  

```
[edit access]
user@host#edit address-assignment pool v4 family inet
```
2. Configure the family of interfaces in the pool.  

```
[edit access address-assignment pool v4]
user@host#set network 100.20.0.0/16
```
3. Configure the upper and lower bounds of the address range.  

```
[edit access address-assignment pool v4]
user@host#set range limited low 100.20.0.10
user@host#set range limited high 100.20.128.250
```
4. Configure the maximum length of time in seconds for which a subscriber can request and hold a lease.  

```
[edit access address-assignment pool v4]
user@host#set dhcp-attributes maximum-lease-time 84600
```

### Configuring RADIUS Authentication

#### CLI Quick Configuration

To quickly configure RADIUS authentication, copy the following commands and paste them into the router terminal window:

```
[edit]
```

```
edit access radius-server 172.28.30.108
set secret $9$1u5ErvW87bwgSr4Zji5T
set timeout 5
set retry 5
up 2
edit profile acc-prof
set authentication-order radius
set radius authentication-server 172.28.30.108
```

---

### Configuring RADIUS Access

#### Step-by-Step Procedure

To configure RADIUS access:

1. Configure the RADIUS server.  

```
[edit access]
user@host#edit radius-server 172.28.30.108
```
2. Configure the required secret (password) that the local router or switch passes to the RADIUS client.  

```
[edit access radius-server 172.28.30.108]
user@host# set secret $9$1u5ErvW87bwgSr4Zji5T
```
3. Configure the length of time that the local router or switch waits to receive a response from a RADIUS server.  

```
[edit access radius-server 172.28.30.108]
user@host# set timeout 5
```
4. Configure the number of times that the router or switch attempts to contact a RADIUS accounting server.  

```
[edit access radius-server 172.28.30.108]
user@host# set retry 5
```
5. Configure the access profile.  

```
[edit access]
user@host#edit profile acc-prof
```
6. Configure the authentication order.  

```
[edit access profile acc-prof ]
user@host# set authentication-order radius
```
7. Configure the authentication server.  

```
[edit access profile acc-prof]
user@host#set radius authentication-server 172.28.30.108
```

**Results**

```
dynamic-profiles {
  vlan-prof {
    interfaces {
      "$junos-interface-ifd-name" {
        unit "$junos-interface-unit" {
          vlan-id "$junos-vlan-id";
          demux-source inet;
          family inet {
            unnumbered-address lo0.0 preferred-source-address 100.20.32.2;
```

```

    }
  }
}
}
multiplay {
  class-of-service {
    traffic-control-profiles {
      multiplay {
        scheduler-map all_smap;
        shaping-rate 100m;
        guaranteed-rate 20m;
      }
    }
  }
  interfaces {
    interface-set "$junos-interface-set-name" {
      interface "$junos-interface-ifd-name" {
        unit "$junos-underlying-interface-unit";
      }
    }
    "$junos-interface-ifd-name" {
      unit "$junos-interface-unit" {
        output-traffic-control-profile multiplay;
      }
    }
  }
}
scheduler-maps {
  all_smap {
    forwarding-class be scheduler be_sch;
    forwarding-class ef scheduler ef_sch;
    forwarding-class af scheduler af_sch;
    forwarding-class nc scheduler nc_sch;
    forwarding-class voice scheduler voice_sch;
    forwarding-class video scheduler video_sch;
    forwarding-class game scheduler game_sch;
    forwarding-class data scheduler data_sch;
  }
}
schedulers {
  be_sch {
    transmit-rate percent 12;
    buffer-size percent 12;
    priority low;
  }
  ef_sch {
    transmit-rate percent 12;
    buffer-size percent 12;
    priority low;
  }
  af_sch {
    transmit-rate percent 12;
    buffer-size percent 12;
    priority low;
  }
  nc_sch {
    transmit-rate percent 12;

```

```
        buffer-size percent 12;
        priority low;
    }
    voice_sch {
        transmit-rate percent 12;
        buffer-size percent 12;
        priority low;
    }
    video_sch {
        transmit-rate percent 12;
        buffer-size percent 12;
        priority low;
    }
    game_sch {
        transmit-rate percent 12;
        buffer-size percent 12;
        priority low;
    }
    data_sch {
        transmit-rate percent 12;
        buffer-size percent 12;
        priority low;
    }
}
}
}
access {
    radius-server {
        172.28.30.108 {
            secret "$9$1u5ErvW87bwgSr4Zji5T"; ## SECRET-DATA
            timeout 5;
            retry 5;
        }
    }
    profile acc-prof {
        authentication-order radius;
        radius {
            authentication-server 172.28.30.108;
        }
    }
    address-assignment {
        pool v4 {
            family inet {
                network 100.20.0.0/16;
                range limited {
                    low 100.20.0.10;
                    high 100.20.128.250;
                }
                dhcp-attributes {
                    maximum-lease-time 84600;
                }
            }
        }
    }
}
class-of-service {
```

```

    interfaces {
        interface-set dynamic-set {
            output-traffic-control-profile multiplay;
        }
    }
}
interfaces {
    interface-set "$junos-interface-set-name" {
        interface "$junos-interface-ifd-name" {
            unit "$junos-underlying-interface-unit";
        }
    }
    "$junos-interface-ifd-name" {
        unit "$junos-underlying-interface-unit" {
            family inet {
                unnumbered-address lo0.0 preferred-source-address 100.20.32.2;
            }
        }
    }
}
}
}
}
interfaces {
    ge-1/0/0 {
        hierarchical-scheduler;
        vlan-tagging;
        auto-configure {
            vlan-ranges {
                dynamic-profile vlan-prof {
                    accept inet;
                    ranges {
                        any;
                    }
                }
            }
        }
    }
}
lo0 {
    unit 0 {
        family inet {
            address 100.20.32.2/32;
        }
    }
}
}
system {
    services {
        dhcp-local-server {
            authentication {
                password multiplay;
                username-include {
                    user-prefix multiplay;
                }
            }
        }
        dynamic-profile multiplay aggregate-clients replace;
        group vlans {

```

```
        interface ge-1/0/0.0;
      }
    }
  }
```

## Verification

To confirm that the configuration is correct, perform these tasks:

- Verifying the Interfaces that are Included in the Interface Set on page 746
- Verifying the Traffic Scheduling and Shaping Parameters for the Interface Set on page 746

### Verifying the Interfaces that are Included in the Interface Set

**Purpose** Verify the interfaces included in the interface set.

**Action** user@host> show interfaces interface-set dynamic-set terse

### Verifying the Traffic Scheduling and Shaping Parameters for the Interface Set

**Purpose** Verify that the traffic scheduling and shaping parameters are applied properly to an interface included in the interface set.

**Action** user@host> show class-of-service interface

**Related Documentation**

- Configuring an Interface Set of Subscribers in a Dynamic Profile on page 712



# Bandwidth Management for Dynamic CoS Overview

- Bandwidth Management for Downstream Traffic in Edge Networks Overview on page 747
- Dedicated Queue Scaling for CoS Configurations on Trio MPC/MIC Interfaces Overview on page 749
- Hierarchical CoS Shaping-Rate Adjustments Overview on page 752
- CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview on page 753
- Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 754

## Bandwidth Management for Downstream Traffic in Edge Networks Overview

In a subscriber access network, traffic with different encapsulations can be passed downstream to other customer premise equipment (CPE) through the MX Series router. Managing the bandwidth of downstream ATM traffic to Ethernet interfaces can be especially difficult because of the different Layer 2 encapsulations.

The *overhead accounting* feature enables you to shape traffic based on either frames or cells and assign a byte adjustment value to account for different encapsulations.

This feature is available on Trio MPC/MIC interfaces on MX Series routers.

### Guidelines for Configuring the Shaping Mode

*Frame shaping mode* is useful for adjusting downstream traffic with different encapsulations. In frame shaping mode, shaping is based on the number of bytes in the frame, without regard to cell encapsulation or padding overhead. Frame is the default shaping mode on the router.



**NOTE:** On the new PD-5-10XGE-SFPP - 10-port 10-Gigabit Ethernet Type-4 PIC with Oversubscription, the default frame shaping overhead (IPG and preamble included) is 20 bytes. To exclude IPG and preamble, change the value to -20.

*Cell shaping mode* is useful for adjusting downstream cell-based traffic. In cell shaping mode, shaping is based on the number of bytes in cells, and accounts for the cell encapsulation and padding overhead.

When you specify cell mode, the resulting traffic stream conforms to the policing rates configured in downstream ATM switches, reducing the number of packet drops in the Ethernet network.

To account for ATM segmentation, the MX Series router adjusts all of the rates by 48/53 to account for ATM AAL5 encapsulation. In addition, the router accounts for cell padding, and internally adjusts each frame by 8 bytes to account for the ATM trailer.

## Guidelines for Configuring Byte Adjustments

When the downstream traffic has different byte sizes per encapsulation, it is useful to configure a *byte adjustment* value to adjust the frame sizes. For example, you can configure the frame shaping mode and a byte adjustment value to account for differences in Layer 2 protocols for downstream Ethernet traffic.

We recommend that you specify a byte adjustment value that represents the difference between the CPE protocol overhead and B-RAS protocol overhead.

The system rounds up the byte adjustment value to the nearest multiple of 4. For example, a value of 6 is rounded to 8, and a value of -10 is rounded to -8.

You do not need to configure a byte adjustment value to account for the downstream ATM network. However, you can specify the byte value to account for additional encapsulations or decapsulations in the downstream network.

## Relationship with Other CoS Features

Enabling the overhead accounting feature affects the resulting shaping rates, guaranteed rate, and excess rate parameters, if they are configured.

The overhead accounting feature also affects the egress shaping overhead feature that you can configure at the chassis level. We recommend that you use the egress shaping-overhead feature to account for the Layer 2 overhead of the outgoing interface, and use the overhead-accounting feature to account for downstream traffic with different encapsulations and cell-based networks.

When both features are configured together, the total byte adjustment value is equal to the adjusted value of the overhead-accounting feature plus the value of the egress-shaping-overhead feature. For example, if the configured byte adjustment value is 40, and the router internally adjusts the size of each frame by 8, the adjusted overhead accounting value is 48. That value is added to the egress shaping overhead of 30 for a total byte adjustment value of 78.

### Related Documentation

- To configure overhead accounting for static Ethernet interfaces, see *Configuring Static Shaping Parameters to Account for Overhead in Downstream Traffic Rates*
- To configure overhead accounting for dynamic subscriber access, see *Configuring Dynamic Shaping Parameters to Account for Overhead in Downstream Traffic Rates* on page 758

## Dedicated Queue Scaling for CoS Configurations on Trio MPC/MIC Interfaces Overview

The 30-Gigabit Ethernet Queuing and 60-Gigabit Ethernet Queuing and Enhanced Queuing Ethernet Modular Port Concentrator (MPC) modules provide a set of dedicated queues for subscriber interfaces configured with hierarchical scheduling or per-unit scheduling.

The dedicated queues offered on these modules enable service providers to reduce costs through different scaling configurations. For example, the 60-Gigabit Ethernet Enhanced Queuing MPC module enables service providers to reduce the cost per subscriber by allowing many subscriber interfaces to be created with four or eight queues. Alternatively, the 30-Gigabit Ethernet and 60-Gigabit Ethernet Queuing MPC modules enable service providers to reduce hardware costs, but allow fewer subscriber interfaces to be created with four or eight queues.

This topic describes the overall queue, scheduler node, and logical interface scaling for subscriber interfaces created on these Trio MPC/MIC module combinations.

### Queue Scaling for Trio MPC/MIC Module Combinations

Table 85 on page 749 lists the number of dedicated queues and number of subscribers supported per Trio MPC module.

**Table 85: Dedicated Queues for Trio MPC/MIC Interfaces**

MPC	Dedicated Egress Queues	Supported Subscriber Interfaces	Logical Interfaces with 4 Queues	Logical Interfaces with 8 Queues
30-Gigabit Ethernet Queuing MPC	64,000	16,000	16,000 (8000 per PIC)	8000 (4000 per PIC)
60-Gigabit Ethernet Queuing MPC	128,000	32,000	32,000 (8000 per PIC)	16,000 (4000 per PIC)
60-Gigabit Ethernet Enhanced Queuing MPC	512,000	64,000	64,000 (16,000 per PIC)	64,000 (16,000 per PIC)

Each interface-set uses eight queues from total available egress queues.

### Determining Maximum Egress Queues per Port

The maximum number of egress queues available on a single port (out of the total egress queues available on the VLAN-queuing module) depends on the number of Packet Forwarding Engine per MPC. 30-Gigabit Ethernet MPC modules have one Packet Forwarding Engine; 60-Gigabit Ethernet MPC modules have two Packet Forwarding Engines. Each Packet Forwarding Engine has two schedulers that share the management of the queues.

A scheduler maps to one-half of a MIC; in CLI configuration statements, that one-half of a MIC corresponds to PIC 0, 1, 2, or 3. MIC ports are partitioned equally across the PICs. A two-port MIC has one port per PIC. A four-port MIC has two ports per PIC.

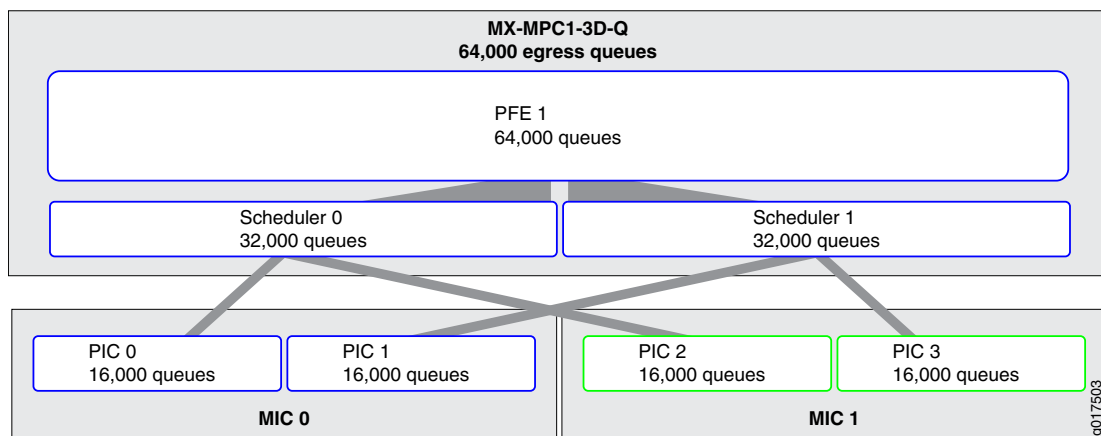
Each interface-set uses 8 queues from total available egress queues.

### Distribution of Queues on 30-Gigabit Ethernet Queuing MPC Modules

On 30-Gigabit Ethernet Queuing MPC modules, each scheduler maps to two PICs on different MICs. For example, scheduler 0 maps to PIC 0 on one MIC and to PIC 2 on the second MIC. Scheduler 1 maps to PIC 1 on the first MIC and to PIC 3 on the second MIC.

Figure 15 on page 750 shows the queue distribution on an 30-Gigabit Ethernet Queuing MPC module. Of the 64,000 egress queues on the module, all are available to the single Packet Forwarding Engine. On the Packet Forwarding Engine, half of these queues (32,000) are managed by each scheduler. One-half of the scheduler complement (16,000) is available to a given PIC. If you have two MICs, then scheduler 0 contributes 16,000 queues to PIC 0 and 16,000 queues to PIC 2. Scheduler 1 contributes 16,000 queues to PIC 1 and 16,000 queues to PIC 3. The distribution is the same when you have only a single MIC, depending on which slot has the MIC: half of the MIC's queues come from each scheduler.

**Figure 15: Distribution of Queues on the 30-Gigabit Ethernet Queuing MPC Module**



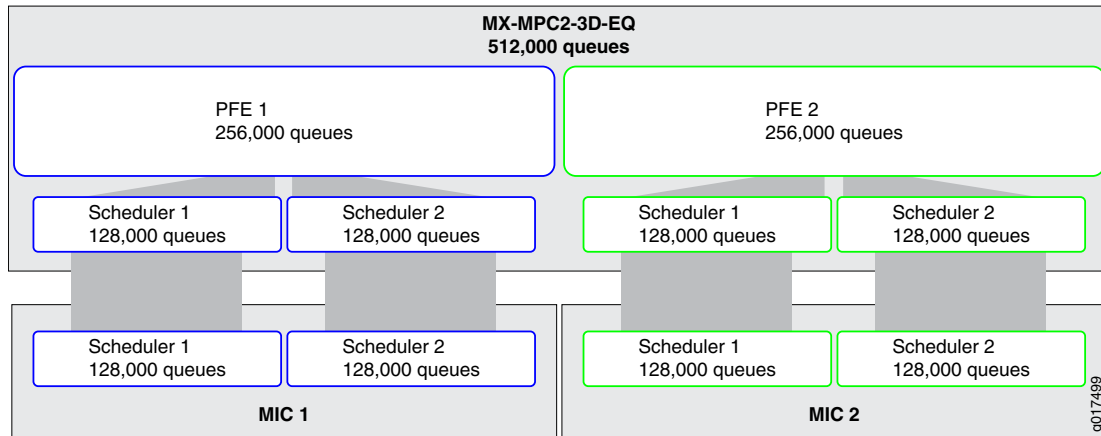
In either case, if you allocate all the queues in a PIC to a single port, then the maximum number of queues per port is 16,000. If you dedicate 4 queues per subscriber, you can accommodate a maximum of 4000 subscribers on a single 30-Gigabit Ethernet Queuing MPC port. If you dedicate 8 queues per subscriber, you can accommodate a maximum of 2000 subscribers on a single port.

### Distribution of Queues on 60-Gigabit Ethernet MPC Modules

On 60-Gigabit Ethernet Queuing and Enhanced Queuing Ethernet MPC modules, each scheduler maps to only one-half of a single MIC: PIC 0 or PIC 1 for the MIC in slot 0 and PIC 2 or PIC 3 for the MIC in slot 1.

Figure 16 on page 751 shows how queues are distributed on an 60-Gigabit Ethernet Enhanced Queuing MPC module. Of the 512,000 egress queues possible on the module, half (256,000) are available for each of the two Packet Forwarding Engines. On each Packet Forwarding Engine, half of these queues (128,000) are managed by each scheduler. The complete scheduler complement (128,000) is available to one PIC in a MIC.

**Figure 16: Distribution of Queues on the 60-Gigabit Ethernet Enhanced Queuing MPC**



If you allocate all the queues from a scheduler to a single port, then the maximum number of queues per port is 128,000. If you dedicate 4 queues per subscriber, you can accommodate a maximum of 32,000 subscribers on a single MPC port. If you dedicate 8 queues per subscriber, you can accommodate a maximum of 16,000 subscribers on a single MPC port.

The number of MICs installed in an MPC and the number of ports per MIC does not affect the maximum number of queues available on a given port. These factors affect only how you are able to allocate queues (and, therefore, subscribers) for your network.

For example, suppose you have an 60-Gigabit Ethernet Enhanced Queuing MPC module. This module supports a maximum of 64,000 subscribers regardless of whether you allocate 4 or 8 queues per PIC. The MPC supports a maximum of 128,000 queues per port. If you have two 2-port MICs installed, each PIC has one port and you can have 128,000 queues on each port. You can have fewer, of course, but you cannot allocate more to any port. If you have a two 4-port MICs installed, you can have 128,000 queues in each PIC, but only on one port in each PIC. Or you can split the queues available for the PIC across the two ports in each PIC.

## Managing Remaining Queues

When the number of available dedicated queues on the module drops below 10 percent, an SNMP trap is generated to notify you .

When the maximum number of dedicated queues on the Trio MPC modules is reached, a system log message, **COSD\_OUT\_OF\_DEDICATED\_QUEUES**, is generated. The system does not provide subsequent subscriber interfaces with a dedicated set of queues. For

per-unit scheduling configurations, there are no configurable queues remaining on the module.

For hierarchical scheduling configurations, remaining queues are available when the maximum number of dedicated queues is reached on the module. Traffic from these logical interfaces are considered unclassified and attached to a common set of queues that are shared by all subsequent logical interfaces. These common queues are the default port queues that are created for every port. You can configure a traffic control profile and attach that to the interface to provide CoS parameters for the remaining queues.

For example, when the 30-Gigabit Ethernet Queuing MPC is configured with 32,000 subscriber interfaces with four queues per subscriber, the module can support 16,000 subscribers with a dedicated set of queues. You can provide CoS shaping and scheduling parameters to the remaining queues for those subscriber interfaces by attaching a special traffic-control profile to the interface.

These subscriber interfaces remain with this traffic control profile, even if dedicated queues become available.

**Related  
Documentation**

- For information about managing dedicated queues in a static CoS configuration, see [Managing Dedicated and Remaining Queues for Static CoS Configurations on Trio MPC/MIC Interfaces](#)
- For information about managing dedicated queues in a dynamic subscriber access configuration, see [Managing Dedicated and Remaining Queues for Dynamic CoS Configurations on Trio MPC/MIC Interfaces](#) on page 759
- [Scheduler Node Scaling on Trio MPC/MIC Interfaces Overview](#)
- [COSD System Log Messages](#)

---

## Hierarchical CoS Shaping-Rate Adjustments Overview

This overview describes how MX Series 3D Universal Edge Routers 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 and the Trio MPC/MIC family of products.

Hierarchical, per-subscriber CoS is supported only for subscriber interfaces on EQ DPC or Trio MPC/MIC interfaces operating in hierarchical scheduler mode. These types of subscriber interfaces can be static VLAN interfaces or static interface sets. 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 Documentation**

- CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview on page 753
- Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 754
- Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 762
- Disabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 767
- Disabling Hierarchical Bandwidth Adjustment for Subscriber Interfaces with Reverse-OIF Mapping on page 768
- Example: Configuring Hierarchical CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 774

## CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview

This overview describes how an MX Series 3D Universal Edge 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. ANCP acquires subscriber line rate information from DSLAMs and then communicates this data transmission rate for use with CoS.

For more information about the ANCP protocol, see the “ANCP Topology Discovery and Traffic Monitoring Overview” on page 781.

**Related  
Documentation**

- Hierarchical CoS Shaping-Rate Adjustments Overview on page 752
- Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 754
- Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 762
- Disabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 767
- Example: Configuring Hierarchical CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 774

## Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops

These guidelines apply to configuring an MX Series 3D Universal Edge 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 ANCP.

When you enhance hierarchical CoS policy by configuring ANCP-driven shaping-rate adjustments, consider the following guidelines:

- Shaping-rate adjustments are supported on EQ DPCs and Trio MPC/MIC interfaces on MX Series routers.
- 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 are 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 781.

**Related  
Documentation**

- Hierarchical CoS Shaping-Rate Adjustments Overview on page 752
- CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview on page 753
- Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 762
- Disabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 767
- Example: Configuring Hierarchical CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 774



## CHAPTER 70

# Configuring Bandwidth Management Parameters for Dynamic CoS

- Managing Excess Bandwidth Distribution for Dynamic CoS on page 757
- Configuring Dynamic Shaping Parameters to Account for Overhead in Downstream Traffic Rates on page 758
- Managing Dedicated and Remaining Queues for Dynamic CoS Configurations on Trio MPC/MIC Interfaces on page 759
- Verifying the Number of Dedicated Queues Configured on Trio MPC/MIC Interfaces on page 761
- Providing Accurate Scheduling for a Demux Subscriber Interface of Aggregated Ethernet Links on page 761
- Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 762
- Disabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 767
- Disabling Hierarchical Bandwidth Adjustment for Subscriber Interfaces with Reverse-OIF Mapping on page 768
- Verifying the Configuration of Shaping-Rate Adjustments for Subscriber Local Loops on page 768
- Verifying the Configuration of ANCP for Shaping-Rate Adjustments on page 769

## Managing Excess Bandwidth Distribution for Dynamic CoS

---

Service providers often used tiered services that must utilize excess bandwidth as traffic patterns vary. By default, excess bandwidth between a configured guaranteed rate and shaping rate is shared equally among all queues with the same excess priority value, which might not be optimal for all subscribers to a service.

This feature is supported for Trio MPC/MIC interfaces on MX Series routers.

To configure parameters to manage excess bandwidth for subscriber interfaces:

1. Configure the parameters for the interface.
  - a. Configure the shaping rate.

```
[edit dynamic-profiles profile-name class-of-service traffic-control-profiles  
  profile-name]
```

```
user@host# set shaping-rate (rate | $junos-cos-shaping-rate)
```

- b. Configure the excess rate.

```
[edit dynamic-profiles profile-name class-of-service traffic-control-profiles  
profile-name]
```

```
user@host# set excess-rate (percent percentage | proportion value | percent  
$junos-cos-excess-rate)
```

2. (Optional) Configure parameters for the queue.

- a. Configure the shaping rate.

```
[edit dynamic-profiles profile-name class-of-service scheduler scheduler-name]
```

```
user@host# set shaping-rate (rate | $junos-cos-scheduler-shaping-rate)
```

- b. Configure the excess rate.

```
[edit dynamic-profiles profile-name class-of-service scheduler scheduler-name]
```

```
user@host# set excess-rate (percent percentage | percent  
$junos-cos-scheduler-excess-rate)
```

- c. Configure the excess priority for a queue.

```
[edit dynamic-profiles profile-name class-of-service scheduler scheduler-name]
```

```
user@host# set excess-priority (low | high | $junos-cos-scheduler-excess-priority)
```

- Related Documentation**
- For hardware requirements and configuration guidelines, see Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660

---

## Configuring Dynamic Shaping Parameters to Account for Overhead in Downstream Traffic Rates

---

You can configure the overhead accounting feature to shape downstream traffic based on either frames or cells.

You can also account for the different byte sizes per encapsulation by configuring a byte adjustment value for the shaping mode.

This feature is supported on Trio MPC/MIC interfaces on MX Series routers.

To configure the overhead accounting feature in a dynamic profile:

1. Do one of the following to configure the shaping mode:

- Specify the shaping mode.

Frame shaping mode is enabled by default.

```
[edit dynamic-profiles profile-name class-of-service traffic-control-profiles  
profile-name]
```

```
user@host# set overhead-accounting (frame-mode | cell-mode)
```

- Configure a variable for the shaping mode.

```
[edit dynamic-profiles profile-name class-of-service traffic-control-profiles  
profile-name]
```

```
user@host#set overhead-accounting $junos-cos-shaping-mode
```

2. (Optional) Do one of the following to configure the byte adjustment value:

- Specify a byte adjustment value.

```
[edit dynamic-profiles profile-name class-of-service traffic-control-profiles
profile-name
user@host#set overhead-accounting bytes byte-value
```

- Configure a variable for the byte adjustment.

```
[edit dynamic-profiles profile-name class-of-service traffic-control-profiles
profile-name
user@host#set overhead-accounting bytes $junos-cos-byte-adjust
```



**BEST PRACTICE:** We recommend that you specify a byte adjustment value that represents the difference between the customer premise equipment (CPE) protocol overhead and B-RAS protocol overhead.

The available range is –120 through 124 bytes. The system rounds up the byte adjustment value to the nearest multiple of 4. For example, a value of 6 is rounded to 8, and a value of –10 is rounded to –8.

#### Related Documentation

- Bandwidth Management for Downstream Traffic in Edge Networks Overview on page 747
- Example: Configuring Dynamic Shaping Parameters to Account for Overhead in Downstream Traffic Rates on page 771
- Verifying the Scheduling and Shaping Configuration for Subscriber Access on page 688

## Managing Dedicated and Remaining Queues for Dynamic CoS Configurations on Trio MPC/MIC Interfaces

This topic describes how to manage dedicated and remaining queues for static and dynamic subscriber interfaces configured in dynamic profiles.

You manage queues at the chassis and physical port level in the static configuration hierarchies, then configure dynamic scheduling and shaping parameters for the subscriber interfaces in the dynamic profile.

- Configuring the Maximum Number of Queues for Trio MPC/MIC Interfaces on page 759
- Configuring Remaining Common Queues on Trio MPC/MIC Interfaces on page 760

### Configuring the Maximum Number of Queues for Trio MPC/MIC Interfaces

30-Gigabit Ethernet Queuing Trio MPC modules and 60-Gigabit Ethernet Queuing and Enhanced Queuing Trio MPC modules support a dedicated number of queues when configured for hierarchical scheduling and per-unit scheduling configurations.

To scale the number of subscriber interfaces per queue, you can modify the number of queues supported on the Trio MIC.

To configure the number of queues:

1. Specify that you want to configure the MIC.

```
user@host# edit chassis fpc slot-number pic pic-number
```

2. Configure the number of queues.

```
[edit chassis fpc slot-number pic pic-number]  
user@host# set max-queues-per-interface (8 | 4)
```

## Configuring Remaining Common Queues on Trio MPC/MIC Interfaces

30-Gigabit Ethernet Queuing Trio MPC modules and 60-Gigabit Ethernet Queuing and Enhanced Queuing Trio MPC modules support a dedicated set of queues when configured with hierarchical scheduling.

When the number of dedicated queues is reached on the module, there can be queues remaining. Traffic from these logical interfaces are considered unclassified and attached to a common set of queues that are shared by all subsequent logical interfaces.

You can configure traffic shaping and scheduling resources for the remaining queues by attaching a special traffic-control profile to the interface. This feature enables you to provide the same shaping and scheduling to remaining queues as the dedicated queues.

To configure the remaining queues on a Trio MPC/MIC interface:

1. Configure CoS parameters in a traffic-control profile.

```
[edit class-of-service]  
user@host# edit traffic-control-profiles profile-name
```

2. Enable hierarchical scheduling for the interface.

```
[edit interfaces interface-name]  
user@host# set hierarchical-scheduler
```

3. Attach the traffic control profiles for the dedicated and remaining queues to the port on which you enabled hierarchical scheduling.

To provide the same shaping and scheduling parameters to dedicated and remaining queues, reference the same traffic-control profile.

- a. Attach the traffic-control profile for the dedicated queues on the interface.

```
[edit class-of-service interfaces interface-name]  
user@host# set output-traffic-control-profile profile-name
```

- b. Attach the traffic-control profile for the remaining queues on the interface.

```
[edit class-of-service interfaces interface-name]  
user@host# set output-traffic-control-profile-remaining profile-name
```

### Related Documentation

- Verifying the Number of Dedicated Queues Configured on Trio MPC/MIC Interfaces on page 761
- Dedicated Queue Scaling for CoS Configurations on Trio MPC/MIC Interfaces Overview on page 749

- Configuring Static Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 669
- Configuring Dynamic Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 671

## Verifying the Number of Dedicated Queues Configured on Trio MPC/MIC Interfaces

**Purpose** Display the number of dedicated queue resources that are configured for the logical interfaces on a port.

**Action** `user@host#show class-of-service interface ge-1/1/0`  
 Physical interface: ge-1/1/0, Index: 166  
 Queues supported: 4, Queues in use: 4  
 Total non-default queues created: 4  
 Scheduler map: <default>, Index: 2  
 Chassis scheduler map: <default-chassis>, Index: 4

Logical interface: ge-1/1/0.100, Index: 72, Dedicated Queues: no  
 Shaping rate: 32000

Object	Name	Type	Index
Scheduler-map	<remaining>		0
Classifier	ipprec-compatibility	ip	13

Logical interface: ge-1/1/0.101, Index: 73, Dedicated Queues: no  
 Shaping rate: 32000

Object	Name	Type	Index
Scheduler-map	<remaining>		0
Classifier	ipprec-compatibility	ip	13

Logical interface: ge-1/1/0.102, Index: 74, Dedicated Queues: yes  
 Shaping rate: 32000

Object	Name	Type	Index
Traffic-control-profile	<control_tc_prof>	Output	45866

- Related Documentation**
- Managing Dedicated and Remaining Queues for Static CoS Configurations on Trio MPC/MIC Interfaces
  - Managing Dedicated and Remaining Queues for Dynamic CoS Configurations on Trio MPC/MIC Interfaces on page 759

## Providing Accurate Scheduling for a Demux Subscriber Interface of Aggregated Ethernet Links

Unlike VLAN subscriber interfaces, enabling link protection is not required for configuring hierarchical CoS on demux interfaces. Instead, we recommend that you enable targeted distribution on the demux interface to provide accurate scheduling for the aggregated Ethernet links.

Before you begin, configure the subscriber interface with aggregated Ethernet:

- For static and dynamic IP demux interfaces, see “Configuring a Static or Dynamic IP Demux Subscriber Interface over Aggregated Ethernet” on page 481.

- For static and dynamic VLAN demux interfaces, see “Configuring a Static or Dynamic VLAN Demux Subscriber Interface over Aggregated Ethernet” on page 482.

To provide accurate scheduling for a demux subscriber interface of aggregated Ethernet links:

1. Enable targeted distribution for the demux interface.

See “Configuring the Distribution Type for Demux Subscribers on Aggregated Ethernet Interfaces” on page 484.

2. Enable hierarchical scheduling on the link aggregation bundle.

See “Configuring Hierarchical CoS for a Subscriber Interface of Aggregated Ethernet Links” on page 707.

3. (Optional) Enable module redundancy to ensure that CoS resources are provisioned for the aggregated Ethernet links if a module or a link fails. By default, link redundancy is supported.

See “Configuring Link and Module Redundancy for Demux Subscribers in an Aggregated Ethernet Interface” on page 484.

4. (Optional) Configure rebalancing periodically or manually for the subscribers. See “Configuring Rebalancing of Demux Subscribers in an Aggregated Ethernet Interface” on page 485.

5. Attach static or dynamic traffic shaping and scheduling parameters at the aggregated Ethernet logical interface or its underlying physical interface. See:

- Configuring Traffic Scheduling and Shaping for Subscriber Access on page 677
- Configuring Schedulers in a Dynamic Profile for Subscriber Access on page 679
- Applying Traffic Shaping and Scheduling to a Subscriber Interface in a Dynamic Profile on page 685
- Applying Minimal Shaping and Scheduling to Remaining Subscriber Traffic on page 685

**Related  
Documentation**

- Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660
- Verifying the Distribution of Demux Subscribers in an Aggregated Ethernet Interface on page 486

---

## Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops

You can enhance a CoS implementation by enabling an MX Series 3D Universal Edge 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:

- Configuring Static Logical Interface Sets to Serve as CoS Hierarchical Scheduler Nodes for Subscriber Loops on page 763
- Configuring the Logical Interfaces That Compose the Static Logical Interface Sets on page 764
- Configuring Hierarchical CoS on the Static Logical Interface Sets That Serve as Hierarchical Scheduler Nodes for Subscriber Local Loops on page 764
- Configuring ANCP Functionality That Supports and Drives Shaping-Rate Adjustments for Subscriber Local Loops on page 766

## 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 OS 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 OS 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:

```

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 OS 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 ANCP to monitor subscriber local loop rates at the DSLAMs and communicate this information to CoS.
- 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.

ANCP uses this information to build a mapping of subscribers to subscriber interfaces. When ANCP 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
        }
      }
      ...
    }
    ...
  }
  ...
}
```

**Related  
Documentation**

- For hardware requirements and configuration guidelines, see [Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 754](#)
- [CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview on page 753](#)
- [Verifying the Configuration of ANCP for Shaping-Rate Adjustments on page 769](#)
- [Verifying the Configuration of Shaping-Rate Adjustments for Subscriber Local Loops on page 768](#)
- [Disabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 767](#)
- [Example: Configuring Hierarchical CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 774](#)

## 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]
user@host# delete qos-adjust
```

Traffic-shaping parameters for all subscriber local loops revert to their current configured values.

**Related  
Documentation**

- For hardware requirements and configuration guidelines, see [Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 754](#)
- [CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview on page 753](#)

- Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 762
- Example: Configuring Hierarchical CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 774

## Disabling Hierarchical Bandwidth Adjustment for Subscriber Interfaces with Reverse-OIF Mapping

---

You can disable hierarchical bandwidth adjustment for all subscriber interfaces with reverse OIF mapping enabled on a specified multicast interface. Reverse OIF mapping is used to determine the subscriber VLAN interface and the multicast traffic bandwidth on the interface.

To disable hierarchical bandwidth adjustment:

1. Specify that you want to access the subscriber interfaces with reverse-OIF mapping enabled.

```
[edit routing-instances routing-instance routing-options multicast interface  
  interface-name]  
user@host# edit reverse-oif-mapping
```

2. Disable hierarchical bandwidth adjustment for all subscriber interfaces on the interface.

```
user@host# set no-qos-adjust
```

### Related Documentation

- For hardware requirements and configuration guidelines, see Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 754
- Hierarchical CoS Shaping-Rate Adjustments Overview on page 752
- Example: Configuring Multicast with Subscriber VLANs

## Verifying the Configuration of Shaping-Rate Adjustments for Subscriber Local Loops

---

**Purpose** Display the configured shaping rate and the adjusted shaping rate for each logical interface set configured for hierarchical CoS.



**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.

**Action** Issue the `show class-of-service interface-set` operational command.

- Related Documentation**
- Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 762

---

## Verifying the Configuration of ANCP for Shaping-Rate Adjustments

---

**Purpose** Use to display or clear information about the ANCP configuration for shaping-rate adjustments.

- Action**
- 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 ANCP is not yet enabled, the process starts when you commit a configuration that contains the **protocols ancp** stanza.

- Related Documentation**
- ANCP Topology Discovery and Traffic Monitoring Overview on page 781
  - Configuring ANCP on page 786





# Bandwidth Management for Dynamic CoS Examples

- Example: Configuring Dynamic Shaping Parameters to Account for Overhead in Downstream Traffic Rates on page 771
- Example: Configuring Hierarchical CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 774

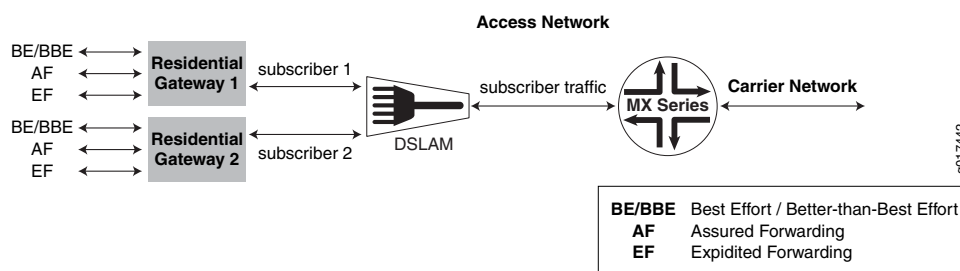
## Example: Configuring Dynamic Shaping Parameters to Account for Overhead in Downstream Traffic Rates

This topic describes two scenarios for which you can configure dynamic shaping parameters to account for packet overhead in a downstream network.

The RADIUS administrator supplies the initial values on the RADIUS server, and the service activation is performed at subscriber login.

Figure 17 on page 771 shows the sample network that the examples reference.

**Figure 17: Sample Network Topology for Downstream Traffic**



## Managing Traffic with Different Encapsulations

In this example, the MX Series router shown in Figure 17 on page 771 sends stacked VLAN frames to the DSLAM, and the DSLAM sends single-tagged VLAN frames to the residential gateway.

To accurately shape traffic at the residential gateway, the MX Series router must account for the different frame sizes. The difference between the stacked VLAN (S-VLAN) frames sent by the router and the single-tagged VLAN frames received at the residential gateway is a 4-byte VLAN tag. The residential gateway receives frames that are 4 bytes less.

To account for the different frame sizes, you configure the frame shaping mode with -4 byte adjustment:

1. Configure the traffic shaping parameters in the dynamic profile and attach them to the interface.

Enabling the overhead accounting feature affects the resulting shaping rate, guaranteed rate, and excess rate parameters, if they are configured.

```
[edit]
dynamic-profiles {
  ethernet-downstream-network {
    interfaces {
      $junos-interface-ifd-name {
        unit $junos-underlying-interface-unit {
          family inet;
        }
      }
    }
  }
  class-of-service {
    traffic-control-profiles {
      tcp-example-overhead-accounting-frame-mode {
        excess-rate percent $junos-cos-excess-rate
        guaranteed-rate $junos-cos-guaranteed-rate
        overhead-accounting $junos-cos-shaping-mode bytes $junos-cos-byte-adjust
        shaping-rate $junos-cos-shaping-rate;
      }
    }
    interfaces {
      $junos-interface-ifd-name {
        unit "$junos-underlying-interface-unit" {
          output-traffic-control-profile tcp1;
        }
      }
    }
  }
}
```

Table 86 on page 772 lists the initial values defined by the RADIUS administrator for the shaping rates.

**Table 86: Initial Shaping Values at Subscriber Login**

Predefined Variable	RADIUS Tag	Value
\$junos-cos-shaping-rate	T02	10m
\$junos-cos-guaranteed-rate	T03	2m
\$junos-cos-excess-rate	T05	50
\$junos-cos-shaping-mode	T07	frame-mode
\$junos-cos-byte-adjust	T08	-4

2. Verify the adjusted rates.

```

user@host#show class-of-service traffic-control-profile

Traffic control profile: tcp-example-overhead-accounting-frame-mode, Index:
61785
Excess rate 50
Shaping rate: 10000000
Guaranteed rate: 2000000
Overhead accounting mode: Frame Mode
Overhead bytes: -4

```

## Managing Downstream Cell-Based Traffic

In this example, the DSLAM and residential gateway shown in Figure 17 on page 771 are connected through an ATM cell-based network. The MX Series router sends Ethernet frames to the DSLAM, and the DSLAM sends ATM cells to the residential gateway.

To accurately shape traffic at the residential gateway, the MX Series router must account for the different physical network characteristics.

The administrator does not need to configure a byte adjustment value to account for the downstream ATM network, but has the option of configuring a byte adjustment value to account for different encapsulations or decapsulations.

To account for the different frame sizes, configure cell shaping mode:

1. Configure the traffic shaping parameters in the dynamic profile and attach them to the interface.

Enabling the overhead accounting feature affects the resulting shaping rate, guaranteed rate, and excess rate parameters, if they are configured.

```

[edit]
dynamic-profiles {
  atm-downstream-network {
    interfaces {
      $junos-interface-ifd-name {
        unit $junos-underlying-interface-unit {
          family inet;
        }
      }
    }
  }
  class-of-service {
    traffic-control-profiles {
      tcp-example-overhead-accounting-cell-mode {
        excess-rate percent $junos-cos-excess-rate
        guaranteed-rate $junos-cos-guaranteed-rate
        overhead-accounting $junos-cos-shaping-mode
        shaping-rate $junos-cos-shaping-rate
      }
    }
  }
  interfaces {
    $junos-interface-ifd-name {
      unit "$junos-underlying-interface-unit" {
        output-traffic-control-profile tcp1;
      }
    }
  }
}

```

```

    }
  }
}
}
}

```

Table 87 on page 774 lists the initial values defined by the RADIUS administrator for the shaping rates.

**Table 87: Initial Shaping Values at Subscriber Login**

Predefined Variable	RADIUS Tag	Value
\$junos-cos-shaping-rate	T02	10m
\$junos-cos-guaranteed-rate	T03	2m
\$junos-cos-excess-rate	T05	50
\$junos-cos-shaping-mode	T07	cell-mode

2. Verify the adjusted rates.

```
user@host#show class-of-service traffic-control-profile
```

```

Traffic control profile: tcp-example-overhead-accounting-cell-mode, Index:
61785
Shaping rate: 10000000
Excess rate 50
Guaranteed rate: 2000000
Overhead accounting Cell Mode
Overhead bytes: 0

```

To account for ATM segmentation, the MX Series router adjusts all of the rates by 48/53 to account for ATM AAL5 encapsulation. In addition, the router accounts for cell padding, and internally adjusts each frame by 8 bytes to account for the ATM trailer.

- Related Documentation**
- [Configuring Dynamic Shaping Parameters to Account for Overhead in Downstream Traffic Rates on page 758](#)

## 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;
    }
  }
}
```

5. 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
      ...
    }
  }
}
```

6. 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 ANCP is not yet enabled, the process starts when you commit a configuration that contains the `protocols ancp` stanza.

7. 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 Documentation

- Hierarchical CoS Shaping-Rate Adjustments Overview on page 752
- CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview on page 753
- Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 754
- Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 762





## PART 15

# Protocols for Subscriber Access

- [ANCP Overview on page 781](#)
- [Configuring ANCP on page 785](#)
- [Dynamic IGMP Configuration Overview on page 797](#)
- [Dynamic MLD Configuration Overview on page 799](#)
- [Dynamic Router Advertisement Overview on page 801](#)



## CHAPTER 72

# ANCP Overview

- ANCP Topology Discovery and Traffic Monitoring Overview on page 781

### 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. A subscriber might receive only a single service

over a single VLAN configured on a logical interface. A group of VLANs carrying services to a subscriber is an *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 the logical interface or 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 logical interface or interface set corresponds to the subscriber.

You can configure a logical interface by specifying the interface name at the **[edit protocols ancp interfaces]** hierarchy level. Include the **access-identifier** statement when you do so to associate the access identifier with the interface. You can configure an interface set 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. Because the access identifier must be unique for a given neighbor, you must also include the **neighbor** statement with the **access-identifier** statement in both cases.

Some access nodes might not be running the current IETF implementation of ANCP. Instead, they run an earlier version. You can enable ANCP to operate in backwards-compatible mode with all neighbors by including the **pre-ietf-mode** statement at the **[edit protocols ancp]** hierarchy level.

You can control how many discovery table entries are accepted from any neighbor by including the **maximum-discovery-table-entries** statement at the **[edit protocols ancp]** hierarchy level.

When you include the **qos-adjust** statement at the **[edit protocols ancp]** hierarchy level, ANCP updates CoS based on monitoring the subscriber traffic. CoS can adjust the traffic shaping rate that it applies to a particular VLAN or set of VLANs to avoid traffic drops in the access node. ANCP can affect only the shaping rate. When ANCP removes a shaping rate that it previously applied, then the traffic shaping rate reverts to that configured in the CLI. If ANCP remains running but loses a connection to a particular neighbor whose subscriber traffic is adjusted as a result of ANCP, the adjusted rate remains in effect. The rate changes only if ANCP restores the connection and sends fresh updates to CoS, or if you remove the **qos-adjust** statement.

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 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 adjacency

messages from all neighbors 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.

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.

You can also configure parameters for a specific neighbor to override global or default configurations by including any of the following statements at the **[edit protocols ancp neighbor ip-address]** hierarchy level:

- **adjacency-timer**—Adjust the interval between adjacency messages exchanged with this neighbor.
- **ietf-mode**—Prevent ANCP from operating in a backwards-compatible mode for this neighbor; for neighbors that use the current IETF implementation of ANCP.
- **maximum-discovery-table-entries**—Specify how many discovery table entries are accepted from this neighbor.
- **pre-ietf-mode**—Enable ANCP to operate in a backwards-compatible mode for this neighbor; for neighbors that use the original IETF implementation of ANCP rather than the current implementation.

You can monitor ANCP events and operations by including the **traceoptions** statement at the **[edit protocols ancp]** hierarchy level.

**Related  
Documentation**

- Configuring ANCP on page 786
- [edit protocols ancp] Hierarchy Level on page 825



## CHAPTER 73

# Configuring ANCP

- Configuring ANCP on page 786
- Configuring ANCP Neighbors on page 786
- Associating an Access Node with Subscribers for ANCP Operations on page 787
- Specifying the Interval Between ANCP Adjacency Messages on page 788
- Specifying the Maximum Number of Discovery Table Entries on page 788
- Configuring ANCP for Backward Compatibility on page 789
- Specifying How Long Processes Wait for ANCP Restart to Complete on page 789
- Configuring ANCP to Adjust CoS Traffic Shaping on page 790
- Verifying and Monitoring ANCP Neighbors on page 790
- Verifying and Monitoring ANCP Subscribers on page 791
- Verifying and Monitoring CoS for ANCP Subscribers on page 791
- Tracing ANCP Operations for Subscriber Access on page 792
- Configuring the ANCP Trace Log Filename on page 792
- Configuring the Number and Size of ANCP Log Files on page 793
- Configuring Access to the ANCP Log File on page 793
- Configuring a Regular Expression for ANCP Lines to Be Logged on page 794
- Configuring the ANCP Tracing Flags on page 794

## 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. Specify each ANCP neighboring access node to be monitored and optionally configure neighbor parameters.  
See “Configuring ANCP Neighbors” on page 786.
2. Specify the subscribers reached by a VLAN or a set of VLANs through a particular access node.  
See “Associating an Access Node with Subscribers for ANCP Operations” on page 787.
3. Configure the adjacency timer.  
See “Specifying the Interval Between ANCP Adjacency Messages” on page 788.
4. (Optional) Specify the maximum number of discovery table entries that are accepted.  
See “Specifying the Maximum Number of Discovery Table Entries” on page 788
5. Configure ANCP to work with an early IETF draft.  
See “Configuring ANCP for Backward Compatibility” on page 789.
6. Configure the graceful restart timer.  
See “Specifying How Long Processes Wait for ANCP Restart to Complete” on page 789.
7. Configure ANCP to adjust QoS subscriber traffic shaping.  
See “Configuring ANCP to Adjust CoS Traffic Shaping” on page 790.
8. Configure trace options for troubleshooting the configuration.  
See “Tracing ANCP Operations for Subscriber Access” on page 792.

## Configuring ANCP Neighbors

---

You must configure each neighboring access node that you want ANCP to monitor and potentially shape traffic for. Some neighbor settings override globally configured values.

To configure an ANCP neighbor:

1. Specify the IP address of the neighbor.  

```
[edit protocols ancp]  
user@host# set neighbor 10.2.3.4
```
2. (Optional) Configure pre-ietf mode when the neighbor does not support the current IETF standard and pre-ietf mode is not configured globally.



```
[edit protocols ancp neighbor 10.2.3.4]
user@host# set pre-ietf-mode
```

3. (Optional) Configure ietf mode when the neighbor supports the current IETF standard and pre-ietf-mode is configured globally.

```
[edit protocols ancp neighbor 10.2.3.4]
user@host# set ietf-mode
```

4. (Optional) Configure the interval in seconds between ANCP adjacency messages exchanged with this neighbor.

```
[edit protocols ancp neighbor 10.2.3.4]
user@host# set adjacency-timer 20
```

5. (Optional) Specify the maximum number of discovery table entries that are accepted from this neighbor.

```
[edit protocols ancp neighbor 10.2.3.4]
user@host# set maximum-discovery-table-entries 10000
```

#### Related Documentation

- Configuring ANCP on page 786
- Configuring ANCP for Backward Compatibility on page 789
- Specifying the Interval Between ANCP Adjacency Messages on page 788
- Specifying the Maximum Number of Discovery Table Entries on page 788

## Associating an Access Node with Subscribers for ANCP Operations

Subscribers are identified by a unique access loop identifier that is associated with a logical interface for a single VLAN or with a named set of VLANs through which traffic is sent to the subscribers. The access identifier must be unique either across the network or for individual ANCP neighbors. When the identifier is unique for a neighbor, you must specify the neighbor's IP address.

To associate the access identifier with subscribers, do one of the following:

- Specify the name for the set of VLANs 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"
```

- Specify the logical interface for a single VLAN and the unique access-loop identifier for the access node.

```
[edit protocols ancp interfaces]
user@host# set ge-1/0/4.12 vlan1 access-identifier "dslam port-2-10" neighbor 10.12.3.4
```

#### Related Documentation

- Configuring ANCP on page 786
- interfaces (ANCP) on page 1025

## Specifying the Interval Between ANCP Adjacency Messages

---

You can specify the interval between adjacency messages that are sent to all ANCP adjacency peers (neighbors) or to a specific neighbor.

To configure the interval between ANCP adjacency messages for all neighbors:

- Specify the time in seconds.  

```
[edit protocols ancp]  
user@host# set adjacency-timer 20
```

To configure the interval between ANCP adjacency messages for a specific neighbor:

- Specify the time in seconds.  

```
[edit protocols ancp neighbor 10.2.3.4]  
user@host# set adjacency-timer 20
```

- Related Documentation**
- [Configuring ANCP on page 786](#)
  - [Configuring ANCP Neighbors on page 786](#)

## Specifying the Maximum Number of Discovery Table Entries

---

You can specify the maximum number of discovery table entries accepted from all neighbors or from a particular neighbor.

To configure the maximum number of entries for all neighbors:

- Specify the number of entries.  

```
[edit protocols ancp]  
user@host# set maximum-discovery-table-entries 5000
```

To configure the maximum number of entries for a specific neighbor:

- Specify the number of entries.  

```
[edit protocols ancp neighbor 10.2.3.4]  
user@host# set maximum-discovery-table-entries 5000
```

- Related Documentation**
- [Configuring ANCP on page 786](#)
  - [Configuring ANCP Neighbors on page 786](#)

## Configuring ANCP for Backward 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 Internet draft draft-wadhwa-gsmp-l2control-configuration-00.txt, *GSMP extensions for layer2 control (L2C)*. Setting this backward-compatible mode enables interoperability with devices that are not compatible with the current Internet draft for ANCP, draft-ietf-ancp-protocol-02.txt, *Protocol for Access Node Control Mechanism in Broadband Networks*.

To configure ANCP to operate in a backward-compatible mode for all neighbors:

- Specify the pre-ietf mode.

```
[edit protocols ancp]
user@host# set pre-ietf-mode
```

To configure ANCP to operate in a backward-compatible mode for a specific neighbor:

- Specify the pre-ietf mode.

```
[edit protocols ancp neighbor 10.2.3.4]
user@host# set pre-ietf-mode
```

### Related Documentation

- Configuring ANCP on page 786
- Configuring ANCP Neighbors on page 786

## Specifying How Long Processes Wait for ANCP Restart to Complete

You can specify how long other processes wait for ANCP to restart. ANCP sends a keepalive message to CoS at intervals equal to one-third the value of the maximum helper restart time. For example, when you configure the maximum restart time to 120 seconds, ANCP sends a keepalive message every 40 seconds.

If CoS does not receive a keepalive message within the maximum helper restart time, it considers ANCP to be down and immediately reverts any traffic shaping updates that were implemented as a result of ANCP monitoring to the configured values. Consequently, traffic to the subscribers is not effectively shaped, potentially resulting in traffic drops in the DSLAMs. The configured values are maintained until ANCP comes back up and sends fresh traffic shaping updates to CoS.

To configure how long other processes wait for ANCP to restart:

- Specify the time in seconds.

```
[edit protocols ancp]
user@host# set maximum-helper-restart-time 150
```

### Related Documentation

- Configuring ANCP on page 786
- Configuring ANCP to Adjust CoS Traffic Shaping on page 790

- **qos-adjust on page 1135**

---

## Configuring ANCP to Adjust CoS Traffic Shaping

You can specify that CoS policy for 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.

If CoS does not receive a keepalive message within the maximum helper restart time, it considers ANCP to be down and immediately reverts any traffic shaping updates that were implemented as a result of ANCP monitoring to the configured values. The configured values are maintained until ANCP comes back up and sends fresh traffic shaping updates to CoS.

Adjusted traffic shaping values remain in effect for subscribers in the event that ANCP remains running, but loses the connection to a neighbor. In this case, CoS does not revert to the configured values. The ANCP-adjusted values can change only if you remove the **qos-adjust** statement or if ANCP restores the connection to that neighbor and sends fresh shaping updates.

To configure CoS adjustment for subscriber traffic based on ANCP messages:

- Specify CoS adjustment.  

```
[edit protocols ancp]  
user@host# set qos-adjust
```

### Related Documentation

- **Configuring ANCP on page 786**
- **CoS Shaping-Rate Adjustments for Subscriber Local Loops Overview on page 753**
- **Guidelines for Configuring CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 754**
- **Enabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 762**
- **Disabling CoS Shaping-Rate Adjustments for Subscriber Local Loops on page 767**
- **Specifying How Long Processes Wait for ANCP Restart to Complete on page 789**
- **maximum-helper-restart-time on page 1054**

---

## Verifying and Monitoring ANCP Neighbors

**Purpose** View ANCP neighbor information:

**Action** • To display summary information about all ANCP neighbors:

```
user@host> show ancp neighbor
```

- To display information about a specific ANCP neighbor, add the IP address or MAC address to the command:

```
user@host> show ancp neighbor 10.25.64.21
```

- To display detailed information, add **detail** to the command:  

```
user@host> show ancp neighbor detail
```

```
user@host> show ancp neighbor ba:ad:be:ef:10:10 detail
```

**Related  
Documentation**

- [Junos OS Routing Protocols and Policies Command Reference](#)

## Verifying and Monitoring ANCP Subscribers

**Purpose** View ANCP subscriber (local access loop) information:

**Action**

- To display summary information about all ANCP subscribers:  

```
user@host> show ancp subscriber
```
- To display information about all ANCP subscribers connected through a particular ANCP neighbor:  

```
user@host> show ancp subscriber neighbor 10.25.64.21
```
- To display information about an ANCP subscriber specified by the access identifier:  

```
user@host> show ancp subscriber "port-2-11"
```
- To display detailed information, add **detail** to the command:  

```
user@host> show ancp subscriber detail
```

```
user@host> show ancp subscriber neighbor 10.25.64.21 detail
```

**Related  
Documentation**

- [Junos OS Routing Protocols and Policies Command Reference](#)

## Verifying and Monitoring CoS for ANCP Subscribers

**Purpose** View ANCP CoS state information:

**Action**

- To display summary information about the CoS state for all ANCP subscribers:  

```
user@host> show ancp cos
```
- To display information about the CoS state for an ANCP subscriber specified by the access identifier:  

```
user@host> show ancp cos "port-2-11"
```
- To display the most recently updated CoS information:  

```
user@host> show ancp cos last-update
```
- To display the CoS information that is pending (will be used to update the fields):  

```
user@host> show ancp cos pending-update
```

**Related  
Documentation**

- [Junos OS Routing Protocols and Policies Command Reference](#)

## Tracing ANCP Operations for Subscriber Access

---

The Junos OS trace feature tracks ANCP operations and records events 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 finally **ancpd.2**, until there are three trace files. Then the oldest trace file (**ancpd.2**) is overwritten.

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

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To configure ANCP tracing operations:

1. (Optional) Configure a trace log filename.  
See “Configuring the ANCP Trace Log Filename” on page 792.
2. (Optional) Configure the number and size of trace logs.  
See “Configuring the Number and Size of ANCP Log Files” on page 793.
3. (Optional) Configure user access to trace logs.  
See “Configuring Access to the ANCP Log File” on page 793.
4. (Optional) Configure a regular expression to filter the information to be included in the trace log.  
See “Configuring a Regular Expression for ANCP Lines to Be Logged” on page 794.
5. (Optional) Configure flags to specify which events are logged.  
See “Configuring the ANCP Tracing Flags” on page 794.

### Related Documentation

## 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
```

#### Related Documentation

- Tracing ANCP Operations for Subscriber Access on page 792
- Configuring ANCP on page 786
- **traceoptions on page 1215**

## 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 finally **filename.2**, until there are three trace files. Then the oldest trace file (**filename.2**) is overwritten.

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

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.

```
[edit protocols ancp traceoptions]
user@host# set file ancp_1 _logfile_1 files 20 size 2097152
```

#### Related Documentation

- Tracing ANCP Operations for Subscriber Access on page 792
- Configuring ANCP on page 786
- **traceoptions on page 1215**

## Configuring Access to the ANCP Log File

By default, only the user who configures the tracing operation can access the log files. 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, only the user who configured tracing can read the log file:

- Configure the log file to be no-world-readable.

```
[edit protocols ancp traceoptions]
user@host# set file ancp_1_logfile_1 no-world-readable
```

#### Related Documentation

- Tracing ANCP Operations for Subscriber Access on page 792
- Configuring ANCP on page 786
- **traceoptions (ANCP) on page 1215**

## 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 to 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
```

#### Related Documentation

- Tracing ANCP Operations for Subscriber Access on page 792
- Configuring ANCP on page 786
- **traceoptions on page 1215**

## 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
<b>all</b>	Trace all operations
<b>config</b>	Trace configuration events
<b>cos</b>	Trace class-of-service events
<b>general</b>	Trace general flow.
<b>packet</b>	Trace ANCP packet transmit and receive events



Flag	Description
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 ancpancp traceoptions]  
user@host# set flag restart

- Related Documentation

  - [Tracing ANCP Operations for Subscriber Access on page 792](#)
  - [Configuring ANCP on page 786](#)
  - [traceoptions on page 1215](#)



# Dynamic IGMP Configuration Overview

- [Dynamic IGMP Configuration Overview on page 797](#)

## 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 Documentation

- [Dynamic Profiles Overview on page 369](#)
- [Configuring a Dynamic Profile for Client Access on page 395](#)
- For general information about configuring IGMP, see the [Junos OS Multicast Protocols Configuration Guide](#)



# Dynamic MLD Configuration Overview

- Dynamic MLD Configuration Overview on page 799

## Dynamic MLD Configuration Overview

---

The Multicast Listener Discovery (MLD) Protocol manages the membership of hosts and routers in multicast groups. IP version 6 (IPv6) multicast routers use MLD to learn, for each of their attached physical networks, which groups have interested listeners. Each router maintains a list of host multicast addresses that have listeners for each subnet, as well as a timer for each address. However, the router does not need to know the address of the listeners—just the address of the hosts. The router provides addresses to the multicast routing protocol it uses; this ensures that multicast packets are delivered to all subnets where there are interested listeners. In this way, MLD is used as the transport for the Protocol Independent Multicast (PIM) protocol.

Subscriber access supports the configuration of MLD within the **dynamic profiles** hierarchy for dynamically created interfaces. By specifying MLD statements within a dynamic profile, you can dynamically apply MLD configuration when a subscriber connects to an interface using a particular access technology (DHCP), enabling the subscriber to access a carrier (multicast) network.

### Related Documentation

- Dynamic Profiles Overview on page 369
- Configuring a Dynamic Profile for Client Access on page 395
- For general information about configuring MLD, see the [Junos OS Multicast Protocols Configuration Guide](#)



# Dynamic Router Advertisement Overview

- Dynamic Router Advertisement Configuration Overview on page 801

## Dynamic Router Advertisement Configuration Overview

---

In a network deployment where router interfaces are configured statically, you might need to configure the Router Advertisement Protocol on only a small number of interfaces on which it might run. However, in a subscriber access network, static configuration of the Router Advertisement Protocol becomes impractical because the number of interfaces that potentially need the Router Advertisement Protocol increases substantially. In addition, deploying services in a dynamic environment requires dynamic modifications to interfaces as they are created.

Subscriber access supports the configuration of the Router Advertisement Protocol at the **[edit dynamic-profiles *profile-name* protocols]** hierarchy level. By specifying Router Advertisement Protocol statements within a dynamic profile, you can dynamically apply a Router Advertisement configuration when a subscriber connects to an interface using a particular access technology (for example, DHCP), enabling the subscriber to access a carrier (multicast) network.

To minimally configure the Router Advertisement Protocol requires that you include the **router-advertisement** statement at the **[edit dynamic-profiles *profile-name* protocols]** hierarchy level and the **interface** statement along with the ***\$junos-interface-name*** dynamic variable. All other statements are optional.



**NOTE:** Statements used for Router Advertisement Protocol configuration at the **[edit dynamic-profiles *profile-name* protocols]** hierarchy level are identical in function to those same statements used for static Router Advertisement Protocol configuration, with the exception of the **interface** and **prefix** statements, which use dynamic variables.

### Related Documentation

- Dynamic Profiles Overview on page 369
- Configuring a Dynamic Profile for Client Access on page 395
- RADIUS Support for Dynamic Router Advertisement
- Configuring an Address-Assignment Pool for Router Advertisement

- For general information about configuring the Router Advertisement Protocol, see the *Junos OS Routing Protocols Configuration Guide*.



## PART 16

# Subscriber Access Examples

- Service Profile Examples on page 805



## Service Profile Examples

- Example: Configuring a Tiered Service Profile for Subscriber Access on page 805

### 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 2 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 Documentation**
- For more information about configuring CoS for subscriber access, see CoS for Subscriber Access Overview on page 659

## PART 17

# Complete Configuration Statement Hierarchy and Summary of Statements for Subscriber Access

- Subscriber Access Statement Hierarchy on page 811
- Subscriber Access Configuration Statements on page 835





# Subscriber Access Statement Hierarchy

- [edit access address-assignment] Hierarchy Level on page 811
- [edit access domain] Hierarchy Level on page 812
- [edit access gx-plus] Hierarchy Level on page 813
- [edit access profile] Hierarchy Level on page 813
- [edit access tunnel-profile] Hierarchy Level on page 815
- [edit chassis] Hierarchy Level on page 816
- [edit diameter] Hierarchy Level on page 816
- [edit dynamic-profiles] Hierarchy Level on page 817
- [edit forwarding-options dhcp-relay] Hierarchy Level on page 822
- [edit jsr] Hierarchy Level on page 824
- [edit protocols ancp] Hierarchy Level on page 825
- [edit services captive-portal-content-delivery] Hierarchy Level on page 825
- [edit services l2tp] Hierarchy Level on page 826
- [edit services mobile-ip] Hierarchy Level on page 827
- [edit services radius-flow-tap] Hierarchy Level on page 828
- [edit system services dhcp-local-server] Hierarchy Level on page 828
- [edit system services packet-triggered-subscribers] Hierarchy Level on page 831
- [edit system services static-subscribers] Hierarchy Level on page 832
- [edit system services subscriber-management] Hierarchy Level on page 833

## [edit access address-assignment] Hierarchy Level

---

```
access {
  address-assignment {
    abatedUtilization percentage;
    abatedUtilization-v6 percentage;
    highUtilization percentage;
    highUtilization-v6 percentage;
    neighbor-discovery-router-advertisement ndra-pool-name;
    pool pool-name {
      family family {
        dhcp-attributes {
```

```
        [protocol-specific attributes]
    }
    host hostname {
        hardware-address mac-address;
        ip-address ip-address;
    }
    network ip-prefix / <prefix-length>;
    prefix ipv6-prefix;
    range range-name {
        high upper-limit;
        low lower-limit;
        prefix-length prefix-length;
    }
}
}
link pool-name;
}
```

- Related Documentation**
- [Address-Assignment Pools Overview on page 67](#)
  - [Configuring Address-Assignment Pools on page 68](#)

---

## [edit access domain] Hierarchy Level

```
access {
  domain {
    delimiter [delimiter-character];
    map domain-map-name {
      aaa-logical-system logical-system-name {
        aaa-routing-instance routing-instance-name;
      }
      aaa-routing-instance routing-instance-name;
      access-profile profile-name;
      address-pool pool-name;
      dynamic-profile profile-name;
      padn destination-address {
        mask destination-mask;
        metric route-metric;
      }
      strip-domain;
      target-logical-system logical-system-name {
        target-routing-instance routing-instance-name;
      }
      target-routing-instance routing-instance-name;
      tunnel-profile profile-name;
    }
    parse-direction (left-to-right | right-to-left);
  }
}
```

- Related Documentation**
- [Domain Mapping Overview on page 80](#)
  - [Configuring Domain Maps on page 81](#)

## [edit access gx-plus] Hierarchy Level

```
access {
  gx-plus {
    global {
      max-outstanding-requests number;
    }
    partition partition-name {
      diameter-instance instance-name;
      destination-host hostname;
      destination-realm realm;
    }
  }
}
```

- Related Documentation**
- Gx-Plus for Provisioning Subscribers Overview on page 329
  - Configuring Gx-Plus on page 339

## [edit access profile] Hierarchy Level

```
access {
  profile profile-name {
    accounting {
      accounting-stop-on-access-deny;
      accounting-stop-on-failure;
      coa-immediate-update
      immediate-update
      order [ accounting-method ];
      statistics (time | volume-time);
      update-interval minutes;
    }
    authentication-order [ authentication-methods ];
    authorization-order jsrc;
    client client-name {
      ...
    }
    provisioning-order (gx-plus | jsrc);
    radius {
      authentication-server [ ip-address ];
      accounting-server [ ip-address ];
      options {
        accounting-session-id-format (decimal | description);
        client-accounting-algorithm (detail | round-robin);
        client-authentication-algorithm(detail | round-robin);
        ethernet-port-type-virtual;
        interface-description-format {
          exclude-adapter;
          exclude-sub-interface;
        }
      }
      nas-identifier identifier-value;
      nas-port-extended-format {
        adapter-width width;
      }
    }
  }
}
```

```
    port-width width;  
    slot-width width;  
    stacked-vlan-width width;  
    vlan-width width;  
  }  
  revert-interval interval;  
  vlan-nas-port-stacked-format;  
}  
attributes {  
  exclude  
    accounting-authentic [ accounting-on | accounting-off ];  
    accounting-delay-time [ accounting-on | accounting-off ];  
    accounting-session-id [ access-request | accounting-on | accounting-off |  
      accounting-stop ];  
    accounting-terminate-cause [ accounting-off ];  
    called-station-id [ access-request | accounting-start | accounting-stop ];  
    calling-station-id [ access-request | accounting-start | accounting-stop ];  
    class [ accounting-start | accounting-stop ];  
    dhcp-gi-address [ access-request | accounting-start | accounting-stop ];  
    dhcp-mac-address [ access-request | accounting-start | accounting-stop ];  
    event-timestamp [ accounting-on | accounting-off | accounting-start |  
      accounting-stop ];  
    framed-ip-address [ accounting-start | accounting-stop ];  
    framed-ip-netmask [ accounting-start | accounting-stop ];  
    input-filter [ accounting-start | accounting-stop ];  
    input-gigapackets [ accounting-stop ];  
    input-gigawords [ accounting-stop ];  
    interface-description [ access-request | accounting-start | accounting-stop ];  
    nas-identifier [ access-request | accounting-on | accounting-off | accounting-start  
      | accounting-stop ];  
    nas-port [ access-request | accounting-start | accounting-stop ];  
    nas-port-id [ access-request | accounting-start | accounting-stop ];  
    nas-port-type [ access-request | accounting-start | accounting-stop ];  
    output-filter [ accounting-start | accounting-stop ];  
    output-gigapackets [ accounting-stop ];  
    output-gigawords [ accounting-stop ];  
  }  
  ignore {  
    framed-ip-netmask;  
    input-filter;  
    logical-system--routing-instance;  
    output-filter;  
  }  
}  
options {  
  accounting-session-id-format (decimal | description);  
  client-accounting-algorithm (detail | round-robin);  
  client-authentication-algorithm(detail | round-robin);  
  ethernet-port-type-virtual;  
  interface-description-format {  
    exclude-adapter;  
    exclude-sub-interface;  
  }  
  nas-identifier identifier-value;  
  nas-port-extended-format {  
    adapter-width width;
```

```

        port-width width;
        slot-width width;
        stacked-vlan-width width;
        vlan-width width;
    }
    revert-interval interval;
    vlan-nas-port-stacked-format;
}
}
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;
}
session-options {
    client-idle-timeout minutes;
    client-session-timeout minutes;
}
}
}

```

**Related Documentation** • AAA Service Framework Overview on page 18

## [\[edit access tunnel-profile\] Hierarchy Level](#)

```

access {
    tunnel-profile profile-name {
        tunnel tunnel-id {
            identification name;
            logical-system logical-system-name;
            max-sessions number;
            medium type;
            preference number;
            remote-gateway {
                address server-ip-address;
                gateway-name server-name;
            }
            routing-instance routing-instance-name;
            secret password;
            source-gateway {
                address client-ip-address;
                gateway-name client-name;
            }
            type tunnel-type;
        }
    }
}
}

```

**Related Documentation** • Configuring a Tunnel Profile for Subscriber Access on page 242

## [edit chassis] Hierarchy Level

---

```
chassis {  
  ...  
  ppp-subscriber-services (disable | enable);  
  ...  
}
```

**Related Documentation**

- [Configuring PPP Subscriber Services for MLPPP Bundles on page 226](#)

## [edit diameter] Hierarchy Level

---

```
diameter {  
  network-element element-name {  
    forwarding {  
      route dne-route-name {  
        destination realm realm-name <host hostname>;  
        function function-name <partition partition-name>;  
        metric route-metric;  
      }  
    }  
    function function-name;  
    peer peer-name {  
      priority priority-number;  
    }  
  }  
  origin {  
    host hostname;  
    realm realm-name;  
  }  
  peer peer-name {  
    address ip-address;  
    connect-actively {  
      port port-number;  
      transport transport-name;  
    }  
    logical-system logical-system-name <routing-instance routing-instance-name>;  
    routing-instance routing-instance-name;  
  }  
  transport transport-name {  
    address;  
    logical-system logical-system-name <routing-instance routing-instance-name>;  
    routing-instance routing-instance-name;  
  }  
}
```

**Related Documentation**

- [Diameter Base Protocol Overview on page 255](#)
- [Configuring Diameter on page 259](#)

## [edit dynamic-profiles] Hierarchy Level

```

dynamic-profiles {
  profile-name {
    class-of-service {
      interfaces {
        interface-name {
          unit logical-unit-number {
            classifiers {
              type (classifier-name | default);
            }
            output-traffic-control-profile profile-name;
            rewrite-rules {
              dscp (rewrite-name | default);
              dscp-ipv6 (rewrite-name | default);
              ieee-802.1 (rewrite-name | default) vlan-tag (outer | outer-and-inner);
              inet-precedence (rewrite-name | default);
            }
          }
        }
      }
    }
  }
  scheduler-maps {
    map-name {
      forwarding-class class-name scheduler scheduler-name;
    }
  }
  schedulers {
    (scheduler-name) {
      buffer-size (percent percentage | remainder | temporal microseconds |
        $junos-cos-scheduler-bs);
      drop-profile-map loss-priority (any | low | medium-low | medium-high | high)
        protocol (any | non-tcp | tcp) drop-profile (profile-name | predefined-variable);
      excess-priority (low | high | $junos-cos-scheduler-excess-priority);
      excess-rate (percent percentage | percent $junos-cos-scheduler-excess-rate);
      overhead-accounting (shaping-mode) <bytes (byte-value>;
      priority (priority-level | $junos-cos-scheduler-priority);
      shaping-rate (rate | predefined-variable);
      transmit-rate (rate | percent percentage | remainder | percent percentage
        $junos-cos-scheduler-tx) <exact | rate-limit>;
    }
  }
  traffic-control-profiles profile-name {
    delay-buffer-rate (percent percentage | rate);
    excess-rate (percent percentage | proportion value | percent
      $junos-cos-excess-rate);
    guaranteed-rate (percent percentage | rate);
    overhead-accounting (shaping-mode) <bytes (byte-value>;
    scheduler-map map-name;
    shaping-rate (percent percentage | rate | predefined-variable);
  }
}
firewall {
  family family {

```

```

fast-update-filter filter-name {
  interface-specific;
  match-order [match-order];
  term term-name {
    from {
      match-conditions;
    }
    then {
      action;
      action-modifiers;
    }
    only-at-create;
  }
}
}
}
interfaces {
  interface-name {
    unit logical-unit-number {
      family family {
        access-concentrator name;
        address address;
        duplicate-protection;
        dynamic-profile profile-name;
        filter {
          adf {
            counter;
            input-precedence precedence;
            output-precedence precedence;
            rule rule-value;
          }
          input filter-name {
            precedence precedence;
          }
          output filter-name {
            precedence precedence;
          }
        }
      }
      max-sessions number;
      service {
        input {
          service-set service-set-name {
            service-filter filter-name;
          }
          post-service-filter filter-name;
        }
        output {
          service-set service-set-name {
            service-filter filter-name;
          }
        }
      }
    }
    service-name-table table-name
    unnumbered-address interface-name <preferred-source-address address>;
  }
}
ppp-options {

```



```

        chap;
        pap;
    }
    vlan-id number;
}
vlan-tagging;
}
interface-set interface-set-name {
    interface interface-name {
        unit logical-unit-number;
    }
}
demux0 {
    unit logical-unit-number {
        demux-options {
            underlying-interface interface-name
        }
        demux-source {
            source-prefix;
        }
        family family {
            access-concentrator name;
            address address;
            duplicate-protection;
            dynamic-profile profile-name;
            filter {
                input filter-name;
                output filter-name;
            }
            mac-validate (loose | strict):
            max-sessions number;
            service-name-table table-name
            unnumbered-address interface-name <preferred-source-address address>;
        }
    }
}
pp0 {
    unit logical-unit-number {
        keepalives interval seconds;
        no-keepalives;
        pppoe-options {
            underlying-interface interface-name;
            server;
        }
        ppp-options {
            chap;
            pap;
        }
        family inet {
            unnumbered-address interface-name destination address;
            address address;
            service {
                input {
                    service-set service-set-name {
                        service-filter filter-name;
                    }
                }
            }
        }
    }
}

```

Copyright © 2011, Juniper Networks, Inc.

**Related Documentation**

- Dynamic Profiles Overview on page 369
- CoS for Subscriber Access Overview on page 659

- Configuring a Basic Dynamic Profile on page 391
- Configuring Static Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 669

---

## [edit forwarding-options dhcp-relay] Hierarchy Level

```
forwarding-options {
  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;
      }
    }
    duplicate-clients-on-interface;
    dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
      primary-profile-name>;
    forward-snooped-clients (all-interfaces | configured-interfaces |
      non-configured-interfaces);
    interface-traceoptions {
      file filename <files number> <match regular-expression > <size maximum-file-size>
        <world-readable | no-world-readable>;
      flag flag;
      no-remote-trace;
    }
    overrides {
      allow-snooped-clients;
      always-write-giaddr;
      always-write-option-82;
      client-discover-match <option60-and-option82>;
      disable-relay;
      interface-client-limit number;
      layer2-unicast-replies;
      no-allow-snooped-clients;
      no-arp;
      no-bind-on-request;
      proxy-mode;
      replace-ip-source-with;
      send-release-on-delete;
      trust-option-82;
    }
    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 prefix;
        use-interface-description (logical | device);
    }
}
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 {
                allow-snooped-clients;
                always-write-giaddr;
                always-write-option-82;
                client-discover-match <option60-and-option82>;
                disable-relay;
                interface-client-limit number;
                layer2-unicast-replies;
                no-allow-snooped-clients;
                no-arp;
                no-bind-on-request;
                proxy-mode;
                replace-ip-source-with;
                send-release-on-delete;
                trust-option-82;
            }
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
}
dynamic-profile profile-name (aggregate-clients (merge | replace) | 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 prefix;
    use-interface-description (logical | device);
  }
}
interface interface-name {
  exclude;
  overrides {
    allow-snooped-clients;
    always-write-giaddr;
    always-write-option-82;
    client-discover-match <option60-and-option82>;
    disable-relay;
    interface-client-limit number;
    layer2-unicast-replies;
    no-allow-snooped-clients;
    no-arp;
    proxy-mode;
    replace-ip-source-with;
    send-release-on-delete;
    trust-option-82;
  }
  trace;
  upto upto-interface-name;
}
}
traceoptions {
  file filename <files number> <size maximum-file-size> <world-readable |
  no-world-readable> <match regular-expression>;
  flag flag;
}
}
```

**Related Documentation**

- Extended DHCP Relay Agent Overview on page 154

---

## [\[edit jsrc\] Hierarchy Level](#)

```
jsrc {
  partition partition-name {
    diameter-instance instance-name;
    destination-host hostname;
    destination-realm realm-name;
  }
}
```

```

    }
  }

```

**Related  
Documentation**

- Juniper Networks Session and Resource Control (SRC) and JSRC Overview on page 271
- Configuring JSRC on page 279

## [\[edit protocols ancp\] Hierarchy Level](#)

```

protocols {
  ancp {
    adjacency-timer seconds;
    interfaces {
      interface-set interface-set-name {
        access-identifier identifier-string <neighbor ip-address>;
      }
      interface-name {
        access-identifier identifier-string <neighbor ip-address>;
      }
    }
    maximum-discovery-table-entries entry-number;
    maximum-helper-restart-time;
    neighbor ip-address {
      adjacency-timer;
      ietf-mode;
      maximum-discovery-table-entries entry-number;
      pre-ietf-mode;
    }
    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;
    }
  }
}

```

**Related  
Documentation**

- ANCP Topology Discovery and Traffic Monitoring Overview on page 781
- Configuring ANCP on page 786

## [\[edit services captive-portal-content-delivery\] Hierarchy Level](#)

```

services {
  captive-portal-content-delivery {
    rule rule-name {
      match-direction (input | output | input-output);
      term term-name {
        from {
          application [ application-name ];
          destination-address address <except>;

```

```

        destination-prefix-list list-name <except>;
    }
    then {
        action;
        action-modifiers;
    }
}
}
rule-set rule-set-name{
    [ rule rule-names];
}
}
}

```

- Related Documentation**
- Notational Conventions Used in Junos OS Configuration Hierarchies
  - [edit services] Hierarchy Level

## [edit services l2tp] Hierarchy Level



**NOTE:** The tunnel-group *group-name* is not supported for LAC on MX Series routers. It applies only to LNS on M Series routers. Similarly, some of the options for the traceoptions statement apply only to LNS on M Series routers; for more information, see traceoptions.

```

services {
  l2tp {
    disable-calling-number-avp;
    disable-failover-protocol;
    fail-over-within-preference;
    tunnel-group group-name {
      hello-interval seconds;
      hide-avps;
      l2tp-access-profile profile-name;
      local-gateway address address;
      maximum-send-window packets;
      ppp-access-profile profile-name;
      receive-window packets;
      retransmit-interval seconds;
      service-interface interface-name;
    }
    syslog {
      host hostname {
        facility-override facility-name;
        log-prefix prefix-number;
        services severity-level;
      }
    }
    tunnel-timeout seconds;
  }
  traceoptions {
    debug-level level;
  }
}

```



```

file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
filter {
    protocol name;
    user-name username;
}
flag flag;
interfaces interface-name {
    debug-level severity;
    flag flag;
}
level (all | error | info | notice | verbose | warning);
no-remote-trace;
}
weighted-load-balancing;
}

```

- Related Documentation**
- L2TP for Subscriber Access Overview on page 231
  - Configuring an L2TP LAC on page 241

## [edit services mobile-ip] Hierarchy Level

```

services {
  mobile-ip {
    access-type {
      (generic | wimax);
    }
    authenticate {
      order (aaa | local);
    }
    dynamic-home-assignment {
      home-agent {
        nai (name@domain | @domain) {
          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 name@domain) {
      spi hexadecimal-value {
        algorithm (hmac-md5 | md5);
        entity-type (host | mobility-agent);
        key (hex | ascii) string;
      }
    }
  }
}

```

```
        replay-method (none | timestamp seconds);
    }
}
traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
    flag flag;
    level <all | error | info | notice | verbose | warning>;
    no-remote-trace;
}
}
```

- Related Documentation**
- Mobile IP Home Agent Elements and Behavior on page 345
  - Configuring Mobile IP on page 357

---

### [edit services radius-flow-tap] Hierarchy Level

```
services {
    radius-flow-tap {
        forwarding-class class-name;
        interfaces interface-name;
        source-ipv4-address ipv4-address;
    }
}
```

- Related Documentation**
- Subscriber Secure Policy Overview on page 625
  - Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 635

---

### [edit system services dhcp-local-server] Hierarchy Level

```
system {
    services {
        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;
                }
            }
        }
        dhcpv6 {
            authentication {
                password password-string;
            }
        }
    }
}
```

```

    username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name-string;
        logical-system-name;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix-string;
    }
}
group group-name {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
}
interface interface-name {
    exclude;
    overrides {
        interface-client-limit number;
    }
    trace;
    upto upto-interface-name;
}
overrides {
    interface-client-limit number;
}
}
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
        radius-disconnect;
    }
}
}
overrides {
    interface-client-limit number;
}
}
reconfigure {

```

```
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
        radius-disconnect;
    }
}
}
duplicate-clients-on-interface;
dynamic-profile profile-name (aggregate-clients (merge | replace) | use-primary
    primary-profile-name);
forward-snooped-clients (all-interfaces | configured-interfaces |
    non-configured-interfaces);
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 (merge | replace) | use-primary
        primary-profile-name>;
    interface interface-name {
        exclude;
        overrides {
            client-discover-match <option60-and-option82>;
            interface-client-limit number;
            no-arp;
        }
        trace;
        upto upto-interface-name;
    }
    overrides {
        client-discover-match <option60-and-option82>;
        interface-client-limit number;
        no-arp;
    }
    reconfigure {
        attempts attempt-count;
        clear-on-abort;
        timeout timeout-value;
        token token-value;
        trigger {
            radius-disconnect;
        }
    }
}
```

```

    }
  }
  interface-traceoptions {
    file filename <files number> <match regular-expression> <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
  }
  overrides {
    client-discover-match <option60-and-option82>;
    interface-client-limit number;
    no-arp;
  }
  pool-match-order {
    external-authority;
    ip-address-first;
    option-82;
  }
  reconfigure {
    attempts attempt-count;
    clear-on-abort;
    timeout timeout-value;
    token token-value;
    trigger {
      radius-disconnect;
    }
  }
  traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
      no-world-readable> <match regular-expression>;
    flag flag;
    no-remote-trace;
  }
}
}
}

```

Related Documentation • Extended DHCP Local Server Overview on page 98

## [\[edit system services packet-triggered-subscribers\] Hierarchy Level](#)

```

system {
  services {
    packet-triggered-subscribers {
      partition partition-name {
        destination-host hostname;
        destination-realm realm;
        diameter-instance instance-name;
      }
      traceoptions {
        file filename <files number> <match regular-expression> <size maximum-file-size>
          <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
      }
    }
  }
}

```

```
    }  
  }  
}
```

**Related Documentation**

- [Configuring the PTSP Application on page 311](#)

## [\[edit system services static-subscribers\]](#) Hierarchy Level

---

```
system {  
  services {  
    static-subscribers {  
      access-profile profile-name;  
      authentication {  
        password password-string;  
        username-include {  
          domain-name domain-name;  
          interface;  
          logical-system-name;  
          routing-instance-name;  
          user-prefix user-prefix-string;  
        }  
      }  
    }  
    dynamic-profile profile-name {  
      aggregate-clients (merge | replace);  
    }  
    group group-name {  
      access-profile profile-name;  
      authentication {  
        password password-string;  
        username-include {  
          domain-name domain-name;  
          interface;  
          logical-system-name;  
          routing-instance-name;  
          user-prefix user-prefix-string;  
        }  
      }  
    }  
    dynamic-profile profile-name {  
      aggregate-clients (merge | replace);  
    }  
    interface interface-name <exclude> <upto upto-interface-name>;  
  }  
  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;  
  }  
}
```

- Related Documentation**
- [Subscribers on Static Interfaces Overview on page 283](#)
  - [Configuring Subscribers over Static Interfaces on page 288](#)

### [\[edit system services subscriber-management\]](#) Hierarchy Level

---

```
system {
  services {
    subscriber-management {
      maintain-subscriber {
        interface-delete;
      }
      traceoptions {
        file <filename> <files number> <match regular-expression > <size
          maximum-file-size> <world-readable | no-world-readable>;
        flag flag;
      }
    }
  }
}
```

- Related Documentation**
- [Subscriber Binding Retention During Interface Delete Events on page 123](#)





# Subscriber Access Configuration Statements

## aaa-logical-system (Domain Maps)

---

<b>Syntax</b>	<code>aaa-logical-system <i>logical-system-name</i> {     aaa-routing-instance <i>routing-instance-name</i>; }</code>
<b>Hierarchy Level</b>	[edit access domain map <i>domain-map-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Configure a non-default logical system in which the <b>authd</b> daemon sends AAA requests for the domain map.
<b>Default</b>	Default logical system for the subscriber.
<b>Options</b>	<i>logical-system-name</i> —Name of the logical system.  The remaining statement is explained separately.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Specifying an AAA Logical System/Routing Instance in a Domain Map on page 84</li></ul>

## aaa-routing-instance (Domain Maps)

---

<b>Syntax</b>	<code>aaa-routing-instance <i>routing-instance-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access domain map <i>domain-map-name</i>],</code> <code>[edit access domain map <i>domain-map-name</i> aaa-logical-system <i>logical-system-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Configure a non-default routing instance in which the <b>authd</b> daemon sends AAA requests for the domain map.
<b>Default</b>	Default routing instance for the subscriber.
<b>Options</b>	<i>routing-instance-name</i> —Name of the routing instance.
<b>Required Privilege Level</b>	<b>admin</b> —To view this statement in the configuration. <b>admin-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Specifying an AAA Logical System/Routing Instance in a Domain Map on page 84</li></ul>

## abatedUtilization (Address-Assignment Pools)

---

<b>Syntax</b>	<code>abatedUtilization <i>percentage</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access address-assignment]</code> <code>[edit routing-instances <i>routing-instance-name</i> address-assignment]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Generate SNMP traps for DHCP address pools or linked set of address pools. No SNMP traps are generated unless a value is configured.
<b>Default</b>	Abated utilization is not set. Delete the <code>abatedUtilization</code> value to unset.
<b>Options</b>	<i>percentage</i> —Threshold below which an SNMP trap clear is generated. <b>Range:</b> 1 through 98
<b>Required Privilege Level</b>	<b>admin</b> —To view this statement in the configuration. <b>admin-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Address-Assignment Pools Overview on page 67</li><li>• Configuring Address-Assignment Pool Usage Threshold Traps on page 71</li></ul>

## abatedUtilization-v6 (Address-Assignment Pools)

<b>Syntax</b>	<code>abatedUtilization-v6 <i>percentage</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access address-assignment]</code> <code>[edit routing-instances <i>routing-instance-name</i> address-assignment]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Generate SNMP traps for DHCPv6 address pools or linked set of address pools. No SNMP traps are generated unless a value is configured.
<b>Default</b>	Abated utilization is not set. Delete the <code>abatedUtilization</code> value to unset.
<b>Options</b>	<b><i>percentage</i></b> —Threshold below which an SNMP trap clear is generated. <b>Range:</b> 1 through 98
<b>Required Privilege Level</b>	<code>admin</code> —To view this statement in the configuration. <code>admin-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Address-Assignment Pools Overview on page 67</li> <li>Configuring Address-Assignment Pool Usage Threshold Traps on page 71</li> </ul>

## access

<b>Syntax</b>	<pre>access {   route <i>prefix</i> {     next-hop <i>next-hop</i>;     metric <i>route-cost</i>;     preference <i>route-distance</i>;     tag <i>route-tag</i>;   } }</pre>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles routing-options]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Dynamically configure access routes.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	<code>routing</code> —To view this statement in the configuration. <code>routing-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Dynamic Access Routes for Subscriber Management on page 206</li> </ul>

## access-concentrator

---

<b>Syntax</b>	<code>access-concentrator <i>name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family pppoe],</code> <code>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family pppoe],</code> <code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family pppoe],</code> <code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> pppoe-options],</code> <code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> pppoe-underlying-options],</code> <code>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family pppoe],</code> <code>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> pppoe-options],</code> <code>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> pppoe-underlying-options]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Support at the <code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> pppoe-underlying-options]</code> and <code>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> pppoe-underlying-options]</code> hierarchy levels introduced in Junos OS Release 10.1. (MX Series routers with Trio MPCs only) The <code>[edit ... family pppoe]</code> hierarchies introduced in Junos OS Release 11.2.
<b>Description</b>	(J Series Services Routers with Point-to-Point Protocol over Ethernet (PPPoE) interfaces) Configure the name of the access concentrator.  (Intelligent Queuing 2 (IQ2) PICs on M120 and M320 routers; Trio MPCs on MX Series routers) Configure an alternative access concentrator name in the AC-NAME tag in a PPPoE control packet for use with a dynamic PPPoE subscriber interface. If you do not configure the access concentrator name, the AC-NAME tag contains the system name.
<b>Options</b>	<i>name</i> —Name of the access concentrator.
<b>Required Privilege Level</b>	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Identifying the Access Concentrator</li><li>Configuring the PPPoE Family for an Underlying Interface on page 486</li><li>Configuring Dynamic PPPoE Subscriber Interfaces Using Dynamic Profiles on page 535</li><li><i>Junos OS Interfaces and Routing Configuration Guide</i></li></ul>

## access-identifier

<b>Syntax</b>	<code>access-identifier <i>identifier-string</i> &lt;neighbor <i>ip-address</i>&gt;;</code>
<b>Hierarchy Level</b>	[edit protocols ancp interfaces <b>interface-set</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
<b>Description</b>	Associate the specified access node with the set of VLANs that carry traffic to the subscriber using that access node; identify a particular subscriber.
<b>Options</b>	<p><i>identifier-string</i>—Unique identifier string for the access node; also configured on the access node.</p> <p><i>ip-address</i>—IP address of the ANCP neighbor.</p>
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring ANCP on page 786</li> <li>Associating an Access Node with Subscribers for ANCP Operations on page 787</li> </ul>

## access-internal

<b>Syntax</b>	<pre>access-internal {   route <i>subscriber-ip-address</i> {     qualified-next-hop <i>underlying-interface</i> {       mac-address <i>address</i>;     }   } }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <b>routing-options</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	<p>Dynamically configure access-internal routes. Access-internal routes are optional, but are used instead of access routes if the next-hop address is not specified in the Framed-Route Attribute [22].</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management on page 207</li> <li>Configuring Dynamic Access-Internal Routes for PPP Subscriber Management on page 222</li> </ul>

## access-profile (Domain Maps)

---

<b>Syntax</b>	<code>access-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	[edit access domain map <i>domain-map-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Access profile that defines the AAA services and options for subscribers associated with the domain map.
<b>Options</b>	<i>profile-name</i> —Name of access profile.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Specifying an Access Profile in a Domain Map on page 82</li></ul>

## access-profile (Static Subscribers)

<b>Syntax</b>	<code>access-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services <b>static-subscribers</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers <b>group</b> <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services <b>static-subscribers</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers <b>group</b> <i>group-name</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services <b>static-subscribers</b>],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers <b>group</b> <i>group-name</i>],</p> <p>[edit system services <b>static-subscribers</b>],</p> <p>[edit system services static-subscribers <b>group</b> <i>group-name</i>]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify the access profile that triggers AAA services for all static subscribers on interfaces configured at the [edit system services static-subscribers interface] hierarchy level or for the static subscribers in a specific group. The group version of this statement overrides the global configuration.
<b>Options</b>	<i>profile-name</i> —Name of the static subscriber access profile.
<b>Required Privilege Level</b>	<p>access—To view this statement in the configuration.</p> <p>access-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Subscribers over Static Interfaces on page 288</li> <li>Specifying the Static Subscriber Global Access Profile on page 289</li> <li>Specifying the Static Subscriber Group Access Profile on page 293</li> </ul>

## access-type

---

<b>Syntax</b>	<pre>access-type {     (generic   wimax); }</pre>
<b>Hierarchy Level</b>	<pre>[edit services mobile-ip], [edit logical-systems <i>logical-system-name</i> services mobile-ip], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> services     mobile-ip], [edit routing-instances <i>routing-instance-name</i> services mobile-ip]</pre>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	<p>Configure the access type for Mobile IP.</p> <p>The remaining statements are explained separately.</p>
<b>Default</b>	The generic access type is used by default.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Mobile IP on page 357</li><li>• Configuring the Access Type for Mobile IP on page 361</li></ul>



## accounting (Access Profile)

<b>Syntax</b>	<pre> accounting {   accounting-stop-on-access-deny;   accounting-stop-on-failure;   coa-immediate-update;   immediate-update;   order [ <i>accounting-method</i> ];   statistics (time   volume-time);   update-interval <i>minutes</i>; }</pre>
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> ]
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p>
<b>Description</b>	<p>Configure RADIUS accounting parameters and enable RADIUS accounting for an access profile.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li> <li>Configuring Per-Subscriber Session Accounting on page 24</li> </ul>

## accounting (Dynamic IGMP Interface)

<b>Syntax</b>	(accounting   no-accounting);
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i> ],
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Enable or disable the collection of IGMP join and leave event statistics for an interface.
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring a Dynamic Profile for Client Access on page 395</li> <li>For information about recording IGMP join and leave events, see “Recording IGMP Join and Leave Events” in the <a href="#">Junos OS Multicast Protocols Configuration Guide</a></li> </ul>

## accounting (Dynamic MLD Interface)

---

<b>Syntax</b>	(accounting   no-accounting);
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols mld interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Enable or disable the collection of MLD join and leave event statistics for a dynamic interface.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Example: Recording MLD Join and Leave Events</li></ul>

## accounting-port

---

<b>Syntax</b>	accounting-port <i>port-number</i> ;
<b>Hierarchy Level</b>	[edit access radius-server <i>server-address</i> ], [edit access profile <i>profile-name</i> radius-server <i>server-address</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the port number on which to contact the accounting server.
<b>Options</b>	<i>port-number</i> —Port number on which to contact the accounting server. Most RADIUS servers use port number 1813 (as specified in RFC 2866).
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Router or Switch Interaction with RADIUS Servers on page 20</li><li>• Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li><li>• Configuring RADIUS Authentication for L2TP</li></ul>

## accounting-server

---

<b>Syntax</b>	<code>accounting-server [ <i>ip-address</i> ];</code>
<b>Hierarchy Level</b>	<code>[edit access profile <i>profile-name</i> radius]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Specify a list of the RADIUS accounting servers used for accounting for DHCP, L2TP, and PPP clients.
<b>Options</b>	<i>ip-address</i> —IP version 4 (IPv4) address.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li> </ul>

## accounting-session-id-format

---

<b>Syntax</b>	<code>accounting-session-id-format (decimal   description);</code>
<b>Hierarchy Level</b>	<code>[edit access profile <i>profile-name</i> radius options]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
<b>Description</b>	Configure the format the router or switch uses to identify the accounting session.
<b>Default</b>	decimal
<b>Options</b>	<p><b>decimal</b>—Use the decimal format.</p> <p><b>description</b>—Use the generic format, in the form: <code>jnpr <i>interface-specifier:subscriber-session-id</i></code>.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring RADIUS Server Options for Subscriber Access on page 29</li> <li>Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li> </ul>

## accounting-stop-on-access-deny

---

<b>Syntax</b>	accounting-stop-on-access-deny;
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> accounting]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
<b>Description</b>	Configure RADIUS accounting to send an Acct-Stop message when the AAA server refuses a client request for access.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li></ul>

## accounting-stop-on-failure

---

<b>Syntax</b>	accounting-stop-on-failure;
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> accounting]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
<b>Description</b>	Configure RADIUS accounting to send an Acct-Stop message when client access fails AAA but the AAA server grants access.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li></ul>

## active-server-group

<b>Syntax</b>	<code>active-server-group <i>server-group-name</i>;</code>
<b>Hierarchy Level</b>	<p>[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 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],          [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>]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	<p>Apply a DHCP relay agent configuration to the named group of DHCP server addresses.</p> <p>You can include the <b>active-server-group</b> statement at the [edit forwarding-options dhcp-relay] hierarchy level as a global DHCP relay agent configuration option, or at the [edit forwarding-options dhcp-relay group <i>group-name</i>] hierarchy level as a DHCP relay agent configuration option that applies only to a named group of interfaces.</p> <p>Including the <b>active-server-group</b> statement at the [edit forwarding-options dhcp-relay group <i>group-name</i>] hierarchy level as a group-specific option overrides use of the <b>active-server-group</b> statement at the [edit forwarding-options dhcp-relay] hierarchy level as a global option.</p>
<b>Options</b>	<i>server-group-name</i> —Name of the group of DHCP server addresses to which the DHCP relay agent configuration applies.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Extended DHCP Relay Agent Overview on page 154</li> </ul>

## address

---

<b>Syntax</b>	<code>address (<i>ip-address</i>   <i>ipv6-address</i>);</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>],</code> <code>[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family <i>family</i>],</code> <code>[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. The <code>[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i>]</code> hierarchy level introduced in Junos OS Release 10.1.
<b>Description</b>	Configure the interface address. Only the Internet Protocol version 4 (IPv4) protocol family is currently supported for dynamic PPPoE logical interfaces.
<b>Options</b>	<i>ip-address</i> —IPv4 address of the interface.  <i>ipv6-address</i> —IPv6 address of the interface. When configuring an IPv6 address on a dynamically created interface, use the <i>\$junos-ipv6-address</i> dynamic variable.
<b>Required Privilege Level</b>	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• “Configuring the Protocol Family,” in <i>Junos OS Network Interfaces Configuration Guide</i>.</li><li>• <i>Junos OS System Basics Configuration Guide</i></li></ul>

## address (Diameter Peer)

---

<b>Syntax</b>	<code>address <i>ip-address</i>;</code>
<b>Hierarchy Level</b>	<code>[edit diameter peer <i>peer-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Configure the IP address for a Diameter remote peer.
<b>Options</b>	<i>ip-address</i> —IP address of remote Diameter peer.
<b>Required Privilege Level</b>	<code>admin</code> —To view this statement in the configuration. <code>admin-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Diameter on page 259</li><li>• Configuring Diameter Peers on page 260</li></ul>

## address (Diameter Transport)

---

<b>Syntax</b>	<code>address <i>ip-address</i>;</code>
<b>Hierarchy Level</b>	<code>[edit diameter transport <i>transport-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Configure the source (local) IP address for the Diameter local transport connection.
<b>Options</b>	<i>ip-address</i> —IP address of remote Diameter peer.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Diameter on page 259</li> </ul>

## address (Tunnel Profile Remote Gateway)

---

<b>Syntax</b>	<code>address <i>server-ip-address</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i> remote-gateway]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the IP address of the remote gateway device at the L2TP tunnel endpoint, the LNS.
<b>Options</b>	<i>server-ip-address</i> —IP address of the remote gateway device. <b>Default:</b> 0.0.0.0.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring a Tunnel Profile for Subscriber Access on page 242</li> </ul>

## address (Tunnel Profile Source Gateway)

---

<b>Syntax</b>	<code>address <i>client-ip-address</i>;</code>
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i> source-gateway]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the IP address of the source gateway device at the local L2TP tunnel endpoint, the LAC. This value overrides the default address for the logical system or routing instance.
<b>Options</b>	<i>client-ip-address</i> —IP address of the source gateway device. <b>Default:</b> 0.0.0.0.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Tunnel Profile for Subscriber Access on page 242</li></ul>



## address-assignment (Address-Assignment Pools)

```
Syntax  address-assignment {
        abatedUtilization percentage;
        abatedUtilization-v6 percentage;
        highUtilization percentage;
        highUtilization-v6 percentage;
        neighbor-discovery-router-advertisement ndra-pool-name;
        pool pool-name {
            family family {
                dhcp-attributes {
                    protocol-specific attributes;
                }
                host hostname {
                    hardware-address mac-address;
                    ip-address ip-address;
                }
                network ip-prefix / <prefix-length>;
                prefix ipv6-prefix;
                range range-name {
                    high upper-limit;
                    low lower-limit;
                    prefix-length prefix-length;
                }
            }
            link pool-name;
        }
    }
```

**Hierarchy Level** [edit access]

**Release Information** Statement introduced in Junos OS 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 Documentation**

- Address-Assignment Pools Overview on page 67
- Configuring Address-Assignment Pools on page 68

## address-pool (Domain Maps)

---

<b>Syntax</b>	<code>address-pool <i>pool-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access domain map <i>domain-map-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the address pool used to assign addresses to subscribers associated with the domain map.
<b>Options</b>	<i>pool-name</i> —Name of address pool.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Specifying an Address Pool in a Domain Map on page 83</a></li></ul>

## adf (Dynamic Firewalls)

<b>Syntax</b>	<pre> adf {     counter;     input-precedence <i>precedence</i>;     output-precedence <i>precedence</i>;     rule <i>rule-value</i>; } </pre>
<b>Hierarchy Level</b>	[edit <b>dynamic-profiles</b> <i>profile-name</i> <b>interfaces</b> <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> <i>family</i> <b>filter</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Configure an Ascend-Data-Filter that the dynamic profile applies to a subscriber session.
<b>Options</b>	<p><b>counter</b>—Enable a counter that increments each time the Ascend-Data-Filter rule is used. Typically used for testing purposes.</p> <p><b><i>precedence</i></b>—Precedence value that sets the order in which dynamic service filters are applied on the interface. The lower the precedence value, the higher the precedence that is given. The precedence setting is used in conjunction with the precedence settings of all dynamic service filters configured (not only Ascend-Data-Filters) on the same interface to establish the order. For example, the order also includes any configured <b>input <i>filter-name</i> precedence <i>precedence</i></b> and <b>output <i>filter-name</i> precedence <i>precedence</i></b> statements.</p> <p><b>Range:</b> 0 through 255</p> <p><b>Default:</b> 0</p> <p><b><i>rule-value</i></b>—Ascend-Data-Filter rule. You can specify either a Junos predefined variable that maps the Ascend-Data-Filter actions to Junos filter functionality or you can manually configure the Ascend-Data-Filter rule. The router supports two predefined variables depending on family type: <b>\$junos-adf-rule-v4</b> for family <b>inet</b> and <b>\$junos-adf-rule-v6</b> for family <b>inet6</b>.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Dynamic Firewall Filters Overview on page 555</li> <li>Classic Filters Overview on page 556</li> <li>Basic Classic Filter Syntax on page 558</li> <li>For general information about configuring firewall filters, see the <a href="#">Junos OS Routing Policy Configuration Guide</a>.</li> </ul>

## adjacency-timer

---

<b>Syntax</b>	adjacency-timer <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit protocols ancp], [edit protocols ancp neighbor]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
<b>Description</b>	Specify the interval between adjacency messages sent to ANCP adjacency peer (access node) for all peers or a specific peer.
<b>Options</b>	<b><i>seconds</i></b> —Number of seconds between adjacency messages. <b>Range:</b> 1 through 25 seconds <b>Default:</b> 10 seconds
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring ANCP on page 786</li><li>• Specifying the Interval Between ANCP Adjacency Messages on page 788</li><li>• Configuring ANCP Neighbors on page 786</li></ul>

## aggregate-clients (DHCP Local Server)

<b>Syntax</b>	<code>aggregate-clients (merge   replace);</code>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>dynamic-profile</b> <i>profile-name</i>],</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> <b>dynamic-profile</b> <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server <b>dynamic-profile</b> <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> <b>dynamic-profile</b> <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>dynamic-profile</b> <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> <b>dynamic-profile</b> <i>profile-name</i>],</p> <p>[edit system services dhcp-local-server <b>dynamic-profile</b> <i>profile-name</i>],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> <b>dynamic-profile</b> <i>profile-name</i>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Options <b>merge</b> and <b>replace</b> introduced in Junos OS Release 9.5.</p>
<b>Description</b>	<p>Specify that the router merge (chain) client attributes such as firewall filters and CoS attributes or replace them when multiple client sessions exist on the same underlying VLAN.</p> <p>Not supported for IP demux subscriber interfaces.</p>
<b>Options</b>	<p><b>merge</b>—Aggregate multiple clients attributes for the same subscriber (logical interface)</p> <p><b>replace</b>—Replace the entire logical interface whenever a new client logs in to the network using the same VLAN logical interface</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125</li> </ul>

## aggregate-clients (DHCP Relay Agent)

---

<b>Syntax</b>	<code>aggregate-clients (merge   replace);</code>
<b>Hierarchy Level</b>	<code>[edit forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>],</code> <code>[edit forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. Options <b>merge</b> and <b>replace</b> introduced in Junos OS Release 9.5.
<b>Description</b>	Specify that the router merge (chain) client attributes such as firewall filters and CoS attributes or replace them when multiple client sessions exist on the same underlying VLAN.  Not supported for IP demux subscriber interfaces.
<b>Options</b>	<b>merge</b> —Aggregate multiple client attributes for the same subscriber (logical interface)  <b>replace</b> —Replace the entire logical interface whenever a new client logs in to the network using the same VLAN logical interface
<b>Required Privilege Level</b>	<b>system</b> —To view this statement in the configuration. <b>system-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125</li></ul>

## aggregate-clients (Static Subscribers)

<b>Syntax</b>	aggregate-clients (merge   replace);
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers <b>dynamic-profile</b> <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> <b>dynamic-profile</b> <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers <b>dynamic-profile</b> <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i> <b>dynamic-profile</b> <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers <b>dynamic-profile</b> <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> <b>dynamic-profile</b> <i>profile-name</i>],</p> <p>[edit system services static-subscribers <b>dynamic-profile</b> <i>profile-name</i>],</p> <p>[edit system services static-subscribers group <i>group-name</i> <b>dynamic-profile</b> <i>profile-name</i>]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	<p>Specify for all static subscribers or for a group of static subscribers that the router merge (chain) subscriber (client) attributes such as firewall filters and CoS attributes or replace them when multiple subscriber sessions exist on the same underlying VLAN. The group version of this statement overrides the global version.</p> <p>This statement is not supported for IP demux subscriber interfaces.</p>
<b>Default</b>	By default, multiple subscribers cannot be on the same logical interface.
<b>Options</b>	<p><b>merge</b>—Aggregate the attributes of multiple subscribers for the logical interface.</p> <p><b>replace</b>—Replace the entire logical interface whenever a new client logs in to the network using the same VLAN logical interface.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Subscribers over Static Interfaces on page 288</li> <li>Enabling Multiple Subscribers on a VLAN Logical Interface for All Static Subscribers on page 290</li> </ul>


## algorithm

---

<b>Syntax</b>	algorithm (hmac-md5   md5);
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> services mobile-ip peer nai <i>user@domain</i> spi <i>hexadecimal-value</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer nai <i>user@domain</i> spi <i>hexadecimal-value</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> services mobile-ip peer nai <i>user@domain</i> spi <i>hexadecimal-value</i>],</p> <p>[edit services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>],</p> <p>[edit services mobile-ip peer nai <i>user@domain</i> spi <i>hexadecimal-value</i>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.</p>
<b>Description</b>	Configure the algorithm used for authenticating Mobile IP messages.
<b>Default</b>	hmac-md5
<b>Options</b>	<p><b>hmac-md5</b>—Specifies algorithm hmac-md5</p> <p><b>md5</b>—Specifies algorithm md5</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Mobile IP on page 357</li><li>• Configuring the Mobile IP Home Agent on page 358</li></ul>



## allow-snooped-clients

<b>Syntax</b>	allow-snooped-clients;
<b>Hierarchy Level</b>	<p>[edit forwarding-options dhcp-relay overrides],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</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> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Explicitly enable DHCP snooping support on the router.
<div>  <p><b>NOTE:</b> In Junos OS Release 10.0 and earlier, DHCP snooping is <i>enabled</i> by default. In Release 10.1 and later, DHCP snooping is <i>disabled</i> by default.</p> </div>	
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Extended DHCP Relay Agent Overview on page 154</li> <li>Overriding the Default DHCP Relay Configuration Settings on page 168</li> <li>DHCP Snooping Support on page 174</li> </ul>

## always-write-giaddr

---

<b>Syntax</b>	always-write-giaddr;
<b>Hierarchy Level</b>	[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], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	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.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Extended DHCP Relay Agent Overview on page 154</li></ul>

## always-write-option-82

<b>Syntax</b>	<code>always-write-option-82;</code>
<b>Hierarchy Level</b>	<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],          [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	<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"> <li>• 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.</li> <li>• 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.</li> </ul>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.          interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Extended DHCP Relay Agent Overview on page 154</li> </ul>

## ancp

---

**Syntax**

```
ancp {
  adjacency-timer seconds;
  interfaces {
    interface-set interface-set-name {
      access-identifier identifier-string <neighbor ip-address>;
    }
    interface-name {
      access-identifier identifier-string <neighbor ip-address>;
    }
  }
  maximum-discovery-table-entries entry-number;
  maximum-helper-restart-time;
  neighbor ip-address {
    adjacency-timer;
    ietf-mode;
    maximum-discovery-table-entries entry-number;
    pre-ietf-mode;
  }
  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 protocols]

**Release Information** Statement introduced in Junos OS Release 9.4.

**Description** Configure Junos OS ANCP features.

The remaining statements are described separately.

**Required Privilege Level** routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.

**Related Documentation**

- Configuring ANCP on page 786

## application

---

<b>Syntax</b>	<code>application <i>application-name</i>;</code>
<b>Hierarchy Level</b>	[edit services application-identification rule <i>rule-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Identify the application for inclusion in a rule.
<b>Options</b>	<i>application-name</i> —Identifier for the application.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Redirecting HTTP Requests on page 613</li><li>• Configuring APPID Rules</li></ul>

## attempts (DHCP Local Server)

<b>Syntax</b>	<code>attempts <i>attempt-count</i>;</code>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 <b>reconfigure</b>],</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> <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>reconfigure</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 <b>reconfigure</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit system services dhcp-local-server <b>reconfigure</b>],</p> <p>[edit system services dhcp-local-server dhcpv6 <b>reconfigure</b>],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> <b>reconfigure</b>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Support at the [edit ... <b>dhcpv6</b> ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
<b>Description</b>	Configure how many attempts are made to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces before reconfiguration is considered to have failed. A group configuration takes precedence over a DHCP local server configuration.
<b>Options</b>	<p><b><i>attempt-count</i></b>—Maximum number of attempts.</p> <p><b>Range:</b> 1 through 10</p> <p><b>Default:</b> 8</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 133</li> <li>Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 134</li> </ul>

## attribute

---

<b>Syntax</b>	<code>attribute <i>attribute-number</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> variables radius vendor-id]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure a RADIUS attribute as a variable in a dynamic profile.
<b>Options</b>	<i>attribute-number</i> —Number of the RADIUS attribute.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 698</li></ul>

## attributes

<b>Syntax</b>	<pre> attributes {   exclude {     accounting-authentic [ accounting-on   accounting-off ];     accounting-delay-time [ accounting-on   accounting-off ];     accounting-session-id [ access-request   accounting-on   accounting-off   accounting-stop ];     accounting-terminate-cause [ accounting-off ];     called-station-id [ access-request   accounting-start   accounting-stop ];     calling-station-id [ access-request   accounting-start   accounting-stop ];     class [ accounting-start   accounting-stop ];     dhcp-gi-address [ access-request   accounting-start   accounting-stop ];     dhcp-mac-address [ access-request   accounting-start   accounting-stop ];     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 ];   }   ignore {     framed-ip-netmask;     input-filter;     logical-system-routing-instance;     output-filter;   } } </pre>
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> radius]
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p>
<b>Description</b>	<p>Specify how the router or switch processes RADIUS attributes.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring How RADIUS Attributes Are Used for Subscriber Access on page 31</li> </ul>



## authenticate

---

<b>Syntax</b>	<pre>authenticate {   order (aaa   local); }</pre>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> services <b>mobile-ip</b>],          [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services <b>mobile-ip</b>],          [edit routing-instances <i>routing-instances-name</i> services <b>mobile-ip</b>],          [edit services <b>mobile-ip</b>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3.          Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.</p>
<b>Description</b>	<p>Define the authentication method performed for Mobile IP.</p> <p>The remaining statement is explained separately.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.          system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Mobile IP on page 357</li> <li>Configuring the Access Type for Mobile IP on page 361</li> </ul>

## authentication (DHCP Local Server)

<b>Syntax</b>	<pre> authentication {   password <i>password-string</i>;   username-include {     circuit-type;     client-id;     delimiter <i>delimiter-character</i>;     domain-name <i>domain-name-string</i>;     logical-system-name;     mac-address;     option-60;     option-82 &lt;circuit-id&gt; &lt;remote-id&gt;;     relay-agent-interface-id;     relay-agent-remote-id;     relay-agent-subscriber-id;     routing-instance-name;     user-prefix <i>user-prefix-string</i>;   } }</pre>
<b>Hierarchy Level</b>	<pre> [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> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i>], [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], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 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], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 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], [edit system services dhcp-local-server dhcpv6], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i>], [edit system services dhcp-local-server group <i>group-name</i>]</pre>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	<p>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.</p> <p>The remaining statements are explained separately.</p>

<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Using External AAA Authentication Services with DHCP on page 110</li> </ul>

## authentication (DHCP Relay Agent)


<b>Syntax</b>	<pre>authentication {   password <i>password-string</i>;   username-include {     circuit-type;     delimiter <i>delimiter-character</i>;     domain-name <i>domain-name-string</i>;     logical-system-name;     mac-address;     option-60;     option-82 [circuit-id] [remote-id];     routing-instance-name;     user-prefix <i>user-prefix-string</i>;   } }</pre>
<b>Hierarchy Level</b>	<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>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	<p>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.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Using External AAA Authentication Services with DHCP on page 110</li> </ul>

## authentication (Static Subscribers)

---

<b>Syntax</b>	<pre>authentication {     password <i>password-string</i>;     username-include {         domain-name <i>domain-name</i>;         interface;         logical-system-name;         routing-instance-name;         user-prefix <i>user-prefix-string</i>;     } }</pre>
<b>Hierarchy Level</b>	<pre>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> system services static-subscribers], [edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i>], [edit routing-instances <i>routing-instances-name</i> system services static-subscribers], [edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i>], [edit system services static-subscribers], [edit system services static-subscribers group <i>group-name</i>]</pre>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	<p>Specify the authentication parameters that trigger the Access-Request message to AAA for all static subscribers on interfaces configured at the <b>[edit system services static-subscribers interface]</b> hierarchy level, or for the static subscribers in a specific group. The group version of this statement overrides the global configuration.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Subscribers over Static Interfaces on page 288</li><li>• Configuring the Static Subscriber Global Authentication Password on page 290</li><li>• Configuring the Static Subscriber Group Authentication Password on page 294</li></ul>

## authentication-order

<b>Syntax</b>	<code>authentication-order [ <i>authentication-methods</i> ];</code>
<b>Hierarchy Level</b>	<code>[edit access profile <i>profile-name</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Set the order in which the Junos OS tries different authentication methods when verifying that a client can access the router or switch. For each login attempt, the software tries the authentication methods in order, from first to last.
<b>Default</b>	<code>password</code>
<b>Options</b>	<p><i>authentication-methods</i></p> <ul style="list-style-type: none"> <li><b>password</b>—Verify the client using the information configured at the <code>[edit access profile <i>profile-name</i> client <i>client-name</i>]</code> hierarchy level.</li> <li><b>radius</b>—Verify the client using RADIUS authentication services.</li> </ul>
	<div>  <p><b>NOTE:</b> For subscriber access management, you must always specify the <b>radius</b> method. Subscriber access management does not support the <b>password</b> option (the default), and authentication fails when no method is specified.</p> </div>
<b>Required Privilege Level</b>	<p><code>admin</code>—To view this statement in the configuration.</p> <p><code>admin-control</code>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Example: Configuring CHAP Authentication with RADIUS</li> <li>Specifying the Authentication and Accounting Methods for Subscriber Access on page 21</li> <li>Configuring Access Profiles for L2TP or PPP Parameters</li> </ul>

## authentication-server

---

<b>Syntax</b>	authentication-server [ <i>ip-address</i> ];
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> radius]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	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.
<b>Options</b>	<i>ip-address</i> —IPv4 address.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring RADIUS Server Parameters for Subscriber Access on page 26</li></ul>

## authorization-order

---

<b>Syntax</b>	authorization-order jsrc;
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Configure AAA to use JSRC in an SRC environment to request authorization from the SAE when verifying that a DHCP subscriber can access the router. When you include this statement, AAA ignores any configured authentication order settings. This statement is ignored for non-DHCP subscribers.
<b>Options</b>	jsrc—Use JSRC application to communicate with the SAE for subscriber authorization. JSRC is the only application that is currently available.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring JSRC on page 279</li><li>Authorizing Subscribers with JSRC on page 281</li></ul>

## autonomous (Dynamic Router Advertisement)

<b>Syntax</b>	(autonomous   no-autonomous);
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols router-advertisement interface <i>interface-name</i> prefix <i>prefix</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Specify whether prefixes in the router advertisement messages are used for stateless address autoconfiguration: <ul style="list-style-type: none"> <li>• <b>autonomous</b>—Use prefixes for address autoconfiguration.</li> <li>• <b>no-autonomous</b>—Do not use prefixes for address autoconfiguration.</li> </ul>
<b>Default</b>	autonomous
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Configuring the Prefix Information Included in Neighbor Discovery Advertisements</li> </ul>

## boot-file

<b>Syntax</b>	boot-file <i>filename</i> ;
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	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.
<b>Options</b>	<i>filename</i> —Location of the boot file on the boot server. The filename can include a pathname.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Configuring Address-Assignment Pools on page 68</li> <li>• boot-server on page 874</li> </ul>

## boot-server

---

<b>Syntax</b>	<code>boot-server (<i>address</i>   <i>hostname</i>);</code>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	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.
<b>Options</b>	<p><i>address</i>—IPv4 address of a boot server.</p> <p><i>hostname</i>—Fully qualified hostname of a boot server.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Address-Assignment Pools on page 68</li><li><b>boot-file on page 873</b></li></ul>



## buffer-size (Dynamic Scheduling)

<b>Syntax</b>	<code>buffer-size (percent (<i>percentage</i>   <code>\$junos-cos-scheduler-bs</code>)   remainder   temporal (<i>microseconds</i>   <code>\$junos-cos-scheduler-bs</code>));</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. The <code>\$junos-cos-scheduler-bs</code> predefined variable introduced in Junos OS Release 9.4.
<b>Description</b>	Specify buffer size.
<b>Default</b>	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.
<b>Options</b>	<p><b>percent <i>percentage</i></b>—Buffer size as a percentage of total buffer.</p> <p><b>remainder</b>—Remaining buffer available.</p> <p><b>temporal <i>microseconds</i></b>—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><b>Range:</b> The ranges vary by platform as follows:</p> <ul style="list-style-type: none"> <li>For IQ PICs on M320 routers: 1 through 50,000 microseconds.</li> <li>For IQ PICs on other M Series routers: 1 through 100,000 microseconds.</li> <li>For other M Series routers: 1 through 200,000 microseconds.</li> </ul> <p><b><code>\$junos-scheduler-bs</code></b>—Junos predefined variable that is replaced with the buffer size obtained from the RADIUS server when a subscriber authenticates over the interface to which the dynamic profile is attached.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li> <li>Configuring Schedulers in a Dynamic Profile for Subscriber Access on page 679</li> <li><b>scheduler (Dynamic Scheduler Maps) on page 1174</b></li> </ul>

## captive-portal-content-delivery

---

**Syntax**    captive-portal-content-delivery {  
              rule *rule-name* {  
                  match-direction (input | output | input-output);  
                  term *term-name* {  
                      from {  
                          application [junos-http, junos-https, junos-httpproxy];  
                          destination-address *address* <except>;  
                          destination-prefix-list *list-name* <except>;  
                      }  
                      then {  
                          action;  
                          action-modifiers;  
                      }  
                  }  
              }  
              rule-set *rule-set-name* {  
                  [rule *rule-names*];  
              }  
          }

**Hierarchy Level**    [edit services]

**Release Information**    Statement introduced in Junos OS Release 10.4.

**Description**    Configure the HTTP redirect service by specifying the location to which a subscriber's initial Web browser session is redirected, enabling initial provisioning and service selection for the subscriber.

The remaining statements are explained separately.

**Required Privilege Level**    services—To view this statement in the configuration.  
                                  services—control—To add this statement to the configuration.

**Related Documentation**    • Redirecting HTTP Requests on page 613

## **captive-portal-content-delivery-rule**

---

<b>Syntax</b>	<code>captive-portal-content-delivery-rule <i>rule-name</i>;</code>
<b>Hierarchy Level</b>	[edit services]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the HTTP rule for inclusion in a service set.
<b>Options</b>	<i>rule-name</i> —Identifier for the rule.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Redirecting HTTP Requests on page 613</li></ul>

## **captive-portal-content-delivery-rule-set**

---

<b>Syntax</b>	<code>captive-portal-content-delivery-rule-set <i>rule-set-name</i>;</code>
<b>Hierarchy Level</b>	[edit services]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the HTTP rule set for inclusion in a service set.
<b>Options</b>	<i>rule-set-name</i> —Identifier for the rule set.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Redirecting HTTP Requests on page 613</li></ul>

## chap (Dynamic PPP)

---

<b>Syntax</b>	chap;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" ppp-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Specify CHAP authentication in a PPP dynamic profile.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Dynamic Profiles Overview on page 369</li><li>• Configuring Dynamic Authentication for PPP Subscribers on page 219</li><li>• Attaching Dynamic Profiles to Static PPP Subscriber Interfaces on page 223</li></ul>

## circuit-id (Address-Assignment Pools)

---

<b>Syntax</b>	circuit-id <i>value</i> range <i>named-range</i> ;
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes option-match option-82]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Configure the address-assignment pool named-range to use for a particular option 82 Agent Circuit ID value.
<b>Options</b>	<i>value</i> —String for the Agent Circuit ID suboption (suboption 1) of the DHCP relay agent information option (option 82) in DHCP packets.  <i>range named-range</i> —Name of the address-assignment pool range to use.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Address-Assignment Pools on page 68</li></ul>

## circuit-id (DHCP Relay Agent)

<b>Syntax</b>	<pre> circuit-id {     prefix <i>prefix</i>;     use-interface-description (logical   device); } </pre>
<b>Hierarchy Level</b>	<pre> [edit forwarding-options dhcp-relay relay-option-82], [edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-82], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay relay-option-82], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i>   relay-option-82], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>   forwarding-options dhcp-relay relay-option-82], [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], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay   relay-option-82], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group   <i>group-name</i> relay-option-82] </pre>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	<p>Specify the Agent Circuit ID suboption (suboption 1) of the DHCP relay agent information option (option 82) to include in DHCP packets destined for a DHCP server. Optionally specify that the suboption include a prefix or textual description, or both, instead of the circuit-id.</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 statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Enabling and Disabling Insertion of Option 82 Information on page 192</li> <li>Configuring Agent Circuit ID Information on page 193</li> </ul>

## circuit-type (DHCP Local Server)

<b>Syntax</b>	circuit-type;
<b>Hierarchy Level</b>	<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 dhcpv6 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 dhcpv6 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 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 dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> 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 dhcpv6 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 dhcpv6 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 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 dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> 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 dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication username-include]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Specify that the circuit type is concatenated with the username during the subscriber authentication process.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Using External AAA Authentication Services with DHCP on page 110</li> </ul>

## circuit-type (DHCP Relay Agent)

<b>Syntax</b>	circuit-type;
<b>Hierarchy Level</b>	<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>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Specify that the circuit type is concatenated with the username during the subscriber authentication process.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Using External AAA Authentication Services with DHCP on page 110</li> </ul>

## class-of-service (Dynamic Profiles)

---

<b>Syntax</b>	<code>class-of-service { ... }</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure Junos OS CoS features in a dynamic profile.
<b>Default</b>	If you do not configure any CoS features, all packets are transmitted from output transmission queue 0.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>Configuring Static Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 669</li><li>Configuring Dynamic Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access on page 671</li></ul>

## classifiers (Dynamic CoS Application)

---

<b>Syntax</b>	<pre>classifiers {   dscp (<i>classifier-name</i>   default);   dscp-ipv6 (<i>classifier-name</i>   default);   ieee-802.1 (<i>classifier-name</i>   default) vlan-tag (inner   outer)   inet-precedence (<i>classifier-name</i>   default); }</pre>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Apply a CoS behavior aggregate classifier to a dynamic interface. You can apply a default classifier or one that is previously defined.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>Applying a Classifier to a Subscriber Interface in a Dynamic Profile on page 687</li><li>classifiers (Definition)</li></ul>



## clear-on-abort (DHCP Local Server)

<b>Syntax</b>	clear-on-abort;
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 <b>reconfigure</b>],</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> <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>reconfigure</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 <b>reconfigure</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit system services dhcp-local-server <b>reconfigure</b>],</p> <p>[edit system services dhcp-local-server dhcpv6 <b>reconfigure</b>],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> <b>reconfigure</b>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
<b>Description</b>	Delete all DHCP clients or only the DHCP clients serviced by the specified group of interfaces when reconfiguration fails; that is, when the maximum number of retry attempts have been made without success. A group configuration takes precedence over a DHCP local server configuration.
<b>Default</b>	Restores the original client configuration when reconfiguration fails.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 133</li> <li>Configuring Deletion of the Client When Dynamic Reconfiguration Fails on page 135</li> </ul>

## client-accounting-algorithm

---

<b>Syntax</b>	client-accounting-algorithm (direct   round-robin);
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> radius options]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Configure the access method the router uses to access RADIUS accounting servers.
<b>Default</b>	direct
<b>Options</b>	<b>direct</b> —Use the direct method. <b>round-robin</b> —Use the round-robin method.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring RADIUS Server Parameters for Subscriber Access on page 26</li><li>Configuring RADIUS Server Options for Subscriber Access on page 29</li></ul>

## client-authentication-algorithm

---

<b>Syntax</b>	client-authentication-algorithm (direct   round-robin);
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> radius options]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Configure the access method the router uses to access RADIUS authentication servers.
<b>Default</b>	direct
<b>Options</b>	<b>direct</b> —Use the direct method. <b>round-robin</b> —Use the round-robin method.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring RADIUS Server Parameters for Subscriber Access on page 26</li><li>Configuring RADIUS Server Options for Subscriber Access on page 29</li></ul>

## client-discover-match (DHCP Local Server)

<b>Syntax</b>	client-discover-match <option60-and-option82>;
<b>Hierarchy Level</b>	<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> <p>[edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
<b>Description</b>	Configure DHCP local server to use option 60 and option 82 information to uniquely identify DHCP subscribers when primary subscriber identification fails. The statement always uses the <b>option60-and-option82</b> option. Specifying the option has no effect.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Extended DHCP Local Server Overview on page 98</li> <li>Overriding Default DHCP Local Server Configuration Settings on page 115</li> </ul>

## client-discover-match (DHCP Relay Agent)

---

<b>Syntax</b>	client-discover-match <option60-and-option82>;
<b>Hierarchy Level</b>	[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], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
<b>Description</b>	Configure DHCP relay to use option 60 and option 82 information to uniquely identify DHCP subscribers when primary subscriber identification fails. The statement always uses the <b>option60-and-option82</b> option. Specifying the option has no effect.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Extended DHCP Relay Agent Overview on page 154</li><li>Overriding the Default DHCP Relay Configuration Settings on page 168</li></ul>

## client-id

<b>Syntax</b>	client-id;
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 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 dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 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 dhcpv6 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 dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify that the DHCPv6 Client-ID option (option 1) in the client PDU name is concatenated with the username during the subscriber authentication process.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Creating Unique Usernames for DHCP Clients on page 128</li> </ul>

## client-idle-timeout

---

<b>Syntax</b>	<code>client-idle-timeout <i>minutes</i>;</code>
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> session-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. Support for MX Series routers introduced in Junos OS Release 11.1.
<b>Description</b>	Specify the grace period that begins after an authenticated user terminates all sessions and connections. Authentication is not required if a new connection is initiated during the grace period by the same user. This statement is supported on J Series, MX Series, and SRX Series devices.
<b>Default</b>	The timeout is not configured.
<b>Options</b>	<i>minutes</i> —Number of minutes of idle time that elapse before the session is terminated. <b>Range:</b> 10 through 1440 minutes
<b>Required Privilege Level</b>	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Understanding Session Options for Subscriber Access on page 54</li><li>• Configuring Subscriber Session Options on page 55</li></ul>

## client-session-timeout

---

<b>Syntax</b>	client-session-timeout <i>minutes</i> ;
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> session-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. Support for MX Series routers introduced in Junos OS Release 11.1.
<b>Description</b>	Specify the amount of time after which user sessions are terminated, regardless of user activity (also known as a forced or hard authentication timeout). This statement is supported on J Series, MX Series, and SRX Series devices.
<b>Default</b>	The timeout is not configured.
<b>Options</b>	<i>minutes</i> —Number of minutes after which user sessions are terminated. <b>Range:</b> 1 through 527040 minutes
<b>Required Privilege Level</b>	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Understanding Session Options for Subscriber Access on page 54</li> <li>Configuring Subscriber Session Options on page 55</li> </ul>

## coa-immediate-update

---

<b>Syntax</b>	coa-immediate-update;
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> accounting]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Configure the router to send an Acct-Update message to the RADIUS accounting server immediately following a CoA operation.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring RADIUS Server Parameters for Subscriber Access on page 26</li> <li>Configuring Per-Subscriber Session Accounting on page 24</li> </ul>

## connect-actively

---

<b>Syntax</b>	<code>connect-actively {     port <i>port-number</i>;     transport <i>transport-name</i>; }</code>
<b>Hierarchy Level</b>	[edit diameter peer <i>peer-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	<p>Define the destination port and transport connection used to establish active connections to Diameter peer.</p> <p>The remaining statements are explained separately.</p>
<b>Default</b>	Port 3868 and an automatically assigned local address are used to establish active connections to a peer.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Diameter on page 259</li><li>Configuring Diameter Peers on page 260</li></ul>

## current-hop-limit (Dynamic Router Advertisement)

---

<b>Syntax</b>	<code>current-hop-limit <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles protocols router-advertisement interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Default value placed in the hop count field of the IP header for outgoing packets.
<b>Options</b>	<p><i>number</i>—Hop limit. A value of 0 means the limit is unspecified by this router.</p> <p><b>Range:</b> 0 through 255</p> <p><b>Default:</b> 64</p>
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring the Hop Count in Outgoing Neighbor Discovery Packets</li></ul>



## database-replication (Subscriber Session Database)

<b>Syntax</b>	<pre>database-replication {   traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;     &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit system services]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	<p>Define operations for subscriber management session database replication processes.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 61</li> </ul>

## default-lifetime (Dynamic Router Advertisement)

<b>Syntax</b>	default-lifetime <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit protocols router-advertisement interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Lifetime associated with a default router.
<b>Options</b>	<p><b>seconds</b>—Default lifetime. A value of 0 means this router is not the default router.</p> <p><b>Range:</b> Maximum advertisement interval value through 9000 seconds</p> <p><b>Default:</b> Three times the maximum advertisement interval value</p>
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>max-advertisement-interval</li> <li>Configuring the Lifetime for the Default Neighbor Discovery Router</li> </ul>

## default-local-server-group

---

<b>Syntax</b>	<code>default-local-server-group <i>local-server-group-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit forwarding-options dhcp-relay relay-option-60 vendor-option],</code> <code>[edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option],</code> <code>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay relay-option-60 vendor-option],</code> <code>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-60 vendor-option],</code> <code>[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],</code> <code>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-60 vendor-option],</code> <code>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-60 vendor-option]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	<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 <b>dhcp-local-server</b> statement at the <b>[edit system services]</b> hierarchy level.</p>
<b>Options</b>	<b><i>local-server-group-name</i></b> —Name of the default extended DHCP local server group.
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 189</li></ul>

## default-relay-server-group

<b>Syntax</b>	<code>default-relay-server-group <i>server-group-name</i>;</code>
<b>Hierarchy Level</b>	<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>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	<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 <b>server-group</b> statement at the [edit forwarding-options dhcp-relay] hierarchy level.</p>
<b>Options</b>	<b><i>server-group-name</i></b> —Name of the default DHCP relay server group.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.  interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 189</li> </ul>

## default-value

---

<b>Syntax</b>	<code>default-value <i>default-value</i>;</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> variables <i>variable-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	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.
<b>Options</b>	<b><i>default-value</i></b> —Default value for the variable.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 698</li></ul>

## delay-buffer-rate (Dynamic Traffic Shaping)

---

<b>Syntax</b>	<code>delay-buffer-rate (percent <i>percentage</i>   <i>rate</i>   <code>\$junos-cos-delay-buffer-rate</code>);</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. The <code>\$junos-cos-delay-buffer-rate</code> variable introduced in Junos OS Release 9.4.
<b>Description</b>	Base the delay-buffer calculation on a delay-buffer rate.
<b>Default</b>	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.
<b>Options</b>	<b><i>rate</i></b> —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 <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000). <b>Range:</b> 1000 through 160,000,000,000 bps  <b><code>\$junos-cos-delay-buffer-rate</code></b> —Junos predefined variable that is replaced with the delay-buffer rate obtained from the RADIUS server when a subscriber authenticates over the interface to which the dynamic profile is attached.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>Configuring Traffic Scheduling and Shaping for Subscriber Access on page 677</li><li><b>output-traffic-control-profile</b> on page 1092</li></ul>

## delimiter (DHCP Local Server)

<b>Syntax</b>	<code>delimiter <i>delimiter-character</i>;</code>
<b>Hierarchy Level</b>	<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 dhcpv6 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 dhcpv6 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 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 dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> 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 dhcpv6 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 dhcpv6 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 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 dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> 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 dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication username-include]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Specify the character used as the delimiter between the concatenated components of the username.
<b>Options</b>	<i>delimiter-character</i> —Character that separates components that make up the concatenated username. You cannot use the semicolon (;) as a delimiter.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- Using External AAA Authentication Services with DHCP on page 110

## delimiter (DHCP Relay Agent)

---

<b>Syntax</b>	<code>delimiter <i>delimiter-character</i>;</code>
<b>Hierarchy Level</b>	<code>[edit forwarding-options dhcp-relay authentication username-include],</code> <code>[edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</code> <code>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include],</code> <code>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</code> <code>[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],</code> <code>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</code> <code>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Specify the character used as the delimiter between the concatenated components of the username.
<b>Options</b>	<b><i>delimiter-character</i></b> —Character that separates components that make up the concatenated username. You cannot use the semicolon (;) as a delimiter.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Using External AAA Authentication Services with DHCP on page 110</li></ul>

## delimiter (Domain Maps)

---

<b>Syntax</b>	<code>delimiter [<i>delimiter-character</i>];</code>
<b>Hierarchy Level</b>	[edit access domain]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the characters that the router uses to separate usernames from domain names.
<b>Default</b>	The @ character.
<b>Options</b>	<b><i>delimiter-character</i></b> —One or more characters used as delimiters. You can specify a maximum of eight delimiters. You cannot use the semicolon (;) as a delimiter. Do not include spaces between characters.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Specifying Domain Name Delimiters on page 87</li><li>• Configuring Domain Name Usage for Domain Maps on page 86</li></ul>

## demux0 (Dynamic Interface)

---

**Syntax**

```
demux0 {
  unit logical-unit-number {
    demux-options {
      underlying-interface interface-name
    }
    family family {
      access-concentrator name;
      address address;
      demux-source {
        source-prefix;
      }
      duplicate-protection;
      dynamic-profile profile-name;
      filter {
        input filter-name;
        output filter-name;
      }
      mac-validate (loose | strict):
      max-sessions number;
      service-name-table table-name
      unnumbered-address interface-name <preferred-source-address address>;
    }
    filter {
      input filter-name;
      output filter-name;
    }
    vlan-id number;
  }
}
```

**Hierarchy Level** [edit dynamic-profiles *profile-name* interfaces]

**Release Information** Statement introduced in Junos OS 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 Documentation**

- Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 445
- For information about static IP demux interfaces, see the [Junos OS Network Interfaces Configuration Guide](#)



## demux-options

---

<b>Syntax</b>	<code>demux-options {     underlying-interface <i>interface-name</i> }</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> interfaces demux0 <i>interface-name</i> unit     <i>logical-unit-number</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	<p>Configure logical demultiplexing (demux) interface options in a dynamic profile.</p> <p>The remaining statement is explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 445</li><li>• For information about static IP demux interfaces, see the <a href="#">Junos OS Network Interfaces Configuration Guide</a></li></ul>

## demux-source (Dynamic IP Demux Interface)

---

<b>Syntax</b>	<code>demux-source {     source-address; }</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family <i>family</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure a logical demultiplexing (demux) source address for a subscriber in a dynamic profile.
<b>Options</b>	<b>source-address</b> —Either the specific source address you want to assign to the subscriber interface or the source address variable. For IPv4, specify <b>\$junos-subscriber-ip-address</b> ; for IPv6, specify <b>\$junos-subscriber-ipv6-address</b> ). The source address for the interface is dynamically supplied by DHCP when the subscriber accesses the router.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 445</li><li>For information about static IP demux interfaces, see the <a href="#">Junos OS Network Interfaces Configuration Guide</a></li></ul>

## demux-source (Dynamic Underlying Interface)

<b>Syntax</b>	<code>demux-source <i>family</i>;</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Configure the logical demultiplexing (demux) source family type on the IP demux underlying interface within a dynamic profile.



**NOTE:** The IP demux interface feature currently supports only Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, or aggregated Ethernet underlying interfaces.

<b>Options</b>	<p><b><i>family</i></b>—Protocol family:</p> <ul style="list-style-type: none"> <li>• <b><i>inet</i></b>—Internet Protocol version 4 suite</li> <li>• <b><i>inet6</i></b>—Internet Protocol version 6 suite</li> </ul>
<b>Required Privilege Level</b>	<p><b><i>interface</i></b>—To view this statement in the configuration.</p> <p><b><i>interface-control</i></b>—To add this statement to the configuration.</p>

## destination (Diameter Network Element)

<b>Syntax</b>	<code>destination realm <i>realm-name</i> &lt;host <i>hostname</i>&gt;;</code>
<b>Hierarchy Level</b>	<code>[edit diameter network-element <i>element-name</i> forwarding route <i>dne-route-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Associate the route with all hosts of the specified realm or with a specific host of the specified realm. Together with the function and metric, defines a route reachable through a Diameter network element.
<b>Options</b>	<p><b><i>host hostname</i></b>—(Optional) Name of the destination host associated with the route.</p> <p><b><i>realm realm-name</i></b>—Name of the destination realm associated with the route.</p>
<b>Required Privilege Level</b>	<p><b><i>admin</i></b>—To view this statement in the configuration.</p> <p><b><i>admin-control</i></b>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Configuring Diameter on page 259</li> <li>• Configuring Diameter Network Elements on page 261</li> </ul>

## destination (Dynamic PPPoE)

---

<b>Syntax</b>	<code>destination address;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family inet unnumbered-address <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	For dynamic PPPoE interfaces, specify the IP address of the remote interface.
<b>Options</b>	<b>address</b> —IP address of the remote interface.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a PPPoE Dynamic Profile with Additional Options on page 539</li><li>For information about creating static PPPoE interfaces, see the <a href="#">Junos OS Network Interfaces Configuration Guide</a></li></ul>

## destination-address

---

<b>Syntax</b>	<code>destination-address address &lt;except&gt;;</code>
<b>Hierarchy Level</b>	[edit services captive-portal-content-delivery rule <i>rule-name</i> term <i>term-name</i> from]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4. Option <b>address</b> enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.
<b>Description</b>	Specify the destination address for rule matching.
<b>Options</b>	<b>address</b> —Destination IPv4 or IPv6 address or prefix value. <b>except</b> —(Optional) Exclude the specified prefix list from rule matching.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Redirecting HTTP Requests on page 613</li></ul>

## destination-host

---

<b>Syntax</b>	<code>destination-host <i>hostname</i></code>
<b>Hierarchy Level</b>	<code>[edit jsrc partition <i>partition-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Configure the host on which the SAE application resides.
<b>Options</b>	<i>hostname</i> —Host on which the SAE is installed.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring JSRC on page 279</li><li>Configuring the JSRC Partition on page 280</li></ul>

## destination-host (Gx-Plus)

---

<b>Syntax</b>	<code>destination-host <i>hostname</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access gx-plus partition <i>partition-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Configure the host on which the PCRF application resides.
<b>Options</b>	<i>hostname</i> —Host on which the PCRF is installed.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Gx-Plus on page 339</li><li>Configuring the Gx-Plus Partition on page 340</li></ul>

## destination-host (PTSP)

---

<b>Syntax</b>	<code>destination-host <i>hostname</i>;</code>
<b>Hierarchy Level</b>	<code>[edit system services packet-triggered-subscribers partition <i>partition-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Configure the host on which the SAE application resides.
<b>Options</b>	<i>hostname</i> —Host on which the SAE is installed.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring the PTSP Partition on page 312</li></ul>

## destination-prefix-list

---

<b>Syntax</b>	<code>destination-prefix-list <i>list-name</i> &lt;except&gt;;</code>
<b>Hierarchy Level</b>	<code>[edit services captive-portal-content-delivery rule <i>rule-name</i> term <i>term-name</i> from]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the destination prefix list for rule matching. You configure the prefix list by including the <b>prefix-list</b> statement at the <b>[edit policy-options]</b> hierarchy level.
<b>Options</b>	<i>list-name</i> —Destination prefix list.  <b>except</b> —(Optional) Exclude the specified prefix list from rule matching.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Redirecting HTTP Requests on page 613</li><li><a href="#">Junos OS Routing Policy Configuration Guide</a></li></ul>

## destination-realm (Gx-Plus)

---

<b>Syntax</b>	<code>destination-realm <i>realm</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access gx-plus partition <i>partition-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Configure the realm in which the PCRF host resides.
<b>Options</b>	<i>realm</i> —Realm in which the PCRF host resides.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Gx-Plus on page 339</li> <li>Configuring the Gx-Plus Partition on page 340</li> </ul>

## destination-realm (JSRC)

---

<b>Syntax</b>	<code>destination-realm <i>realm</i></code>
<b>Hierarchy Level</b>	<code>[edit jsrc partition <i>partition-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Configure the realm in which the SAE host resides.
<b>Options</b>	<i>realm</i> —Realm in which the SAE host resides.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring JSRC on page 279</li> <li>Configuring the JSRC Partition on page 280</li> </ul>

## destination-realm (PTSP)

---

<b>Syntax</b>	<code>destination-realm <i>realm</i></code>
<b>Hierarchy Level</b>	[edit system services packet-triggered-subscribers partition <i>partition-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Configure the realm in which the SAE host resides.
<b>Options</b>	<i>realm</i> —Realm in which the SAE host resides.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring the PTSP Partition on page 312</li></ul>



## dhcp-attributes (Address-Assignment Pools)

<b>Syntax</b>	<pre> dhcp-attributes {   boot-file <i>filename</i>;   boot-server (<i>address</i>   <i>hostname</i>);   dns-server [ <i>ipv6-address</i> ];   domain-name <i>domain-name</i>;   grace-period <i>seconds</i>;   maximum-lease-time <i>seconds</i>;   name-server [ <i>server-list</i> ];   netbios-node-type <i>node-type</i>;   option {     [ (<i>id-number</i> <i>option-type</i> <i>option-value</i>)       (<i>id-number</i> <i>array</i> <i>option-type</i> <i>option-value</i>) ];   }   option-match {     option-82 {       circuit-id <i>value</i> <i>range</i> <i>named-range</i>;       remote-id <i>value</i> <i>range</i> <i>named-range</i>;     }   }   router [ <i>router-address</i> ];   server-identifier <i>ip4-address</i>;   sip-server-address [ <i>ipv6-address</i> ];   sip-server-domain-name <i>domain-name</i>;   tftp-server <i>address</i>;   wins-server [ <i>servers</i> ]; } </pre>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family <i>family</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	<p>Configure address pools that can be used by different client applications.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Address-Assignment Pools Overview on page 67</li> <li>Configuring Address-Assignment Pools on page 68</li> <li>Configuring DHCP Client-Specific Attributes on page 72</li> </ul>

## 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;
            }
        }
        dhcpv6 {
            authentication {
                ...
            }
            group group-name {
                authentication {
                    ...
                }
                interface interface-name {
                    exclude;
                    overrides {
                        interface-client-limit number;
                    }
                    trace;
                    upto upto-interface-name;
                }
                overrides {
                    interface-client-limit number;
                }
            }
            overrides {
                interface-client-limit number;
            }
        }
        duplicate-clients-on-interface;
        dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
            primary-profile-name>;
        forward-snooped-clients (all-interfaces | configured-interfaces |
            non-configured-interfaces);
        group group-name {
            authentication {
                ...
            }
            dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
                primary-profile-name>;
            interface interface-name {
                exclude;
```

```

    overrides {
        client-discover-match <option60-and-option82>;
        interface-client-limit number;
        no-arp;
    }
    trace;
    upto upto-interface-name;
}
overrides {
    client-discover-match <option60-and-option82>;
    interface-client-limit number;
    no-arp;
}
}
interface-traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size>
        <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
overrides {
    client-discover-match <option60-and-option82>;
    interface-client-limit number;
    no-arp;
}
pool-match-order {
    external-authority;
    ip-address-first;
    option-82;
}
traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size>
        <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
}
}

```

**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 OS 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 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 DHCP server on J Series routers and so is not supported on J Series routers. Also, the DHCP local server and the DHCP/BOOTP relay server, 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.

The **dhcpv6** stanza configures the router to support Dynamic Host Configuration Protocol for IPv6 (DHCPv6). The DHCPv6 local server is fully compatible with the extended DHCP local server and 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 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 Documentation**

- Extended DHCP Local Server Overview on page 98
- DHCPv6 Local Server Overview on page 102

## 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;
            }
        }
        duplicate-clients-on-interface;
        dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
            primary-profile-name>;
        forward-snooped-clients (all-interfaces | configured-interfaces |
            non-configured-interfaces);
        interface-traceoptions {
            file filename <files number> <match regular-expression> <size maximum-file-size>
                <world-readable | no-world-readable>;
            flag flag;
            no-remote-trace;
        }
        overrides {
            allow-snooped-clients;
            always-write-giaddr;
            always-write-option-82;
            client-discover-match <option60-and-option82>;
            disable-relay;
            interface-client-limit number;
            layer2-unicast-replies;
            no-allow-snooped-clients;
            no-arp;
            no-bind-on-request;
            proxy-mode;
            replace-ip-source-with;
            send-release-on-delete;
            trust-option-82;
        }
        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 prefix;
      use-interface-description (logical | device);
    }
  }
  server-group {
    server-group-name {
      server-ip-address;
    }
  }
  active-server-group server-group-name;
  group group-name {
    active-server-group server-group-name;
    authentication {
      ...
    }
    dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
      primary-profile-name>;
    overrides {
      ...
    }
  }
  relay-option-60 {
    ...
  }
  relay-option-82 {
    ...
  }
  interface interface-name {
    exclude;
    overrides {
      ...
    }
    trace;
    upto upto-interface-name;
  }
}
traceoptions {
  file file-name {
    <files number>;
    <size maximum-file-size>;
    <match regular-expression>;
    <world-readable | no-world-readable>;
  }
  flag flag;
  no-remote-trace;
}
}
```

**Hierarchy Level** [edit forwarding-options],  
[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]

**Release Information** Statement introduced in Junos OS Release 8.3.

**Description** 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.

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.

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.

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 Documentation**

- Extended DHCP Relay Agent Overview on page 154
- DHCP Relay Proxy Overview on page 156
- Using External AAA Authentication Services with DHCP on page 110

## dhcpv6

```
Syntax  dhcpv6 {
        authentication {
            password password-string;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name-string;
                logical-system-name;
                relay-agent-interface-id;
                relay-agent-remote-id;
                relay-agent-subscriber-id;
                routing-instance-name;
                user-prefix user-prefix-string;
            }
        }
        group group-name {
            authentication {
                ...
            }
            interface interface-name {
                exclude;
                overrides {
                    interface-client-limit number;
                }
                trace;
                upto upto-interface-name;
            }
            overrides {
                interface-client-limit number;
            }
        }
        overrides {
            interface-client-limit number;
        }
    }
```

**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 OS Release 9.6.

**Description** Configure DHCPv6 local server options on the router and enable the router to function as a server for the DHCP protocol for IP version 6 (IPv6). The DHCPv6 local server sends and receives packets using the IPv6 protocol and informs IPv6 of the routing requirements of router clients. The local server works together with the AAA service framework to control subscriber access and accounting.

The DHCPv6 local server is fully compatible with the extended DHCP local server and DHCP relay agent.



The remaining statements are explained separately.

<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• DHCPv6 Local Server Overview on page 102</li></ul>

## diameter

```
Syntax  diameter {
        network-element element-name {
            forwarding {
                route dne-route-name {
                    destination realm realm-name <host hostname>;
                    function function-name <partition partition-name>;
                    metric route-metric;
                }
            }
            function function-name;
            peer peer-name {
                priority priority-number;
            }
        }
        origin {
            host hostname;
            realm realm-name;
        }
        peer peer-name {
            address ip-address;
            connect-actively {
                port port-number;
                transport transport-name;
            }
            logical-system logical-system-name <routing-instance routing-instance-name>;
            routing-instance routing-instance-name;
        }
        transport transport-name {
            address;
            logical-system logical-system-name <routing-instance routing-instance-name>;
            routing-instance routing-instance-name;
        }
    }
```

**Hierarchy Level** [edit]

**Release Information** Statement introduced in Junos OS Release 9.6.

**Description** Configure the Diameter base protocol for subscriber management.

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 Documentation**

- Configuring Diameter on page 259

## diameter-instance (Gx-Plus)

---

<b>Syntax</b>	<code>diameter-instance <i>instance-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access gx-plus partition <i>partition-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Specify the Diameter instance associated with the Gx-Plus partition.
<b>Options</b>	<i>instance-name</i> —Name of the Diameter instance. Currently, only <b>master</b> is supported.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Gx-Plus on page 339</li><li>• Configuring the Gx-Plus Partition on page 340</li></ul>

## diameter-instance (JSRC)

---

<b>Syntax</b>	<code>diameter-instance <i>instance-name</i></code>
<b>Hierarchy Level</b>	<code>[edit jsrc partition <i>partition-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify the Diameter instance associated with the JSRC partition.
<b>Options</b>	<i>instance-name</i> —Name of the Diameter instance. Currently, only <b>master</b> is supported.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring JSRC on page 279</li><li>• Configuring the JSRC Partition on page 280</li></ul>

## diameter-instance (PTSP)

---

<b>Syntax</b>	<code>diameter-instance <i>instance-name</i></code>
<b>Hierarchy Level</b>	[edit system services packet-triggered-subscribers partition <i>partition-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify the Diameter instance associated with the PTSP partition.
<b>Options</b>	<i>instance-name</i> —Name of the Diameter instance. Currently, only <b>master</b> is supported.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring the PTSP Partition on page 312</li></ul>

## disable (Dynamic IGMP)

---

<b>Syntax</b>	<code>"disable:\$junos-igmp-enable";</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols <b>igmp</b> interface <i>interface-name</i> ],
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	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).

<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Dynamic Profile for Client Access on page 395</li><li>For information about disabling IGMP, see “Disabling IGMP” in the <i>Junos OS Multicast Protocols Configuration Guide</i></li></ul>

## disable (Dynamic MLD)

---

<b>Syntax</b>	disable;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols mld interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Disable MLD on the dynamic interface.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Disabling MLD</li> </ul>

## disable-calling-number-avp (L2TP LAC)

---

<b>Syntax</b>	disable-calling-number-avp;
<b>Hierarchy Level</b>	[edit services l2tp]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Prevent the LAC from sending L2TP Calling Number AVP 22 in incoming-call request (ICRQ) packets to the LNS. By default, the LAC in an L2TP network generates this AVP from the Calling-Station-Id and sends it to the LNS.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Preventing the LAC from Sending Calling Number AVP 22 to the LNS on page 246</li> </ul>

## disable-failover-protocol (L2TP LAC)

---

<b>Syntax</b>	disable-failover-protocol;
<b>Hierarchy Level</b>	[edit services l2tp]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Configure the LAC to use only the silent failover method when resynchronizing with the peer LNS in the event of LAC failover. This command prevents the default behavior, wherein the LAC first attempts to use the failover protocol and then falls back on the silent failover method. This configuration can be useful when routers that act as the LNS are configured for silent failover or incorrectly negotiate use of the failover protocol even though they do not support it.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Preventing the LAC From Negotiating L2TP Failover Protocol on page 246</li></ul>

## disable-relay

---

<b>Syntax</b>	disable-relay;
<b>Hierarchy Level</b>	[edit forwarding-options dhcp-relay group <i>group-name</i> 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], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	Disable DHCP relay on specific interfaces in a group.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Extended DHCP Relay Agent Overview on page 154</li></ul>

## dns-server

---

<b>Syntax</b>	<code>dns-server <i>ipv6-address</i>;</code>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family inet6 dhcp-attributes]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Specify a DNS server to which clients can send DNS queries. This is equivalent to DHCPv6 option 23. To specify multiple DNS servers, add multiple <b>dns-server</b> statements in order of preference.
<b>Options</b>	<i>ipv6-address</i> —IPv6 address of a DNS server.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Address-Assignment Pools Overview on page 67</li><li>• Configuring Address-Assignment Pools on page 68</li></ul>

## domain (Domain Maps)

---

<b>Syntax</b>	<pre>domain {   delimiter [<i>delimiter-character</i>];   map <i>domain-map-name</i> {     aaa-logical-system <i>logical-system-name</i> {       aaa-routing-instance <i>routing-instance-name</i>;     }     aaa-routing-instance <i>routing-instance-name</i>;     access-profile <i>profile-name</i>;     address-pool <i>pool-name</i>;     dynamic-profile <i>profile-name</i>;     padn <i>destination-address</i> {       mask <i>destination-mask</i>;       metric <i>route-metric</i>;     }     strip-domain;     target-logical-system <i>logical-system-name</i> {       target-routing-instance <i>routing-instance-name</i>;     }     target-routing-instance <i>routing-instance-name</i>;     tunnel-profile <i>profile-name</i>;   }   parse-direction (left-to-right   right-to-left); }</pre>
<b>Hierarchy Level</b>	[edit access]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	<p>Configure domain maps, which are used to map access options and session parameters for subscriber sessions.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Domain Maps on page 81</li></ul>



## domain-name (Address-Assignment Pools)

---

<b>Syntax</b>	<code>domain-name <i>domain-name</i>;</code>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	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.
<b>Options</b>	<i>domain-name</i> —Name of the domain.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Address-Assignment Pools on page 68</li></ul>

## domain-name (DHCP Local Server)

<b>Syntax</b>	<code>domain-name <i>domain-name-string</i>;</code>
<b>Hierarchy Level</b>	<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 dhcpv6 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 dhcpv6 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 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 dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> 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 dhcpv6 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 dhcpv6 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 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 dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> 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 dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication username-include]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Specify the domain name that is concatenated with the username during the subscriber authentication process.
<b>Options</b>	<i>domain-name-string</i> —Domain name formatted string.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- Using External AAA Authentication Services with DHCP on page 110

## domain-name (DHCP Relay Agent)

<b>Syntax</b>	<code>domain-name <i>domain-name-string</i>;</code>
<b>Hierarchy Level</b>	<p>[edit forwarding-options dhcp-relay authentication <b>username-include</b>],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication <b>username-include</b>],</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 <b>username-include</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication <b>username-include</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication <b>username-include</b>]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Specify the domain name that is concatenated with the username during the subscriber authentication process.
<b>Options</b>	<i>domain-name-string</i> —Domain name formatted string.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Using External AAA Authentication Services with DHCP on page 110</li> </ul>

## domain-name (Static Subscribers)

---

<b>Syntax</b>	<code>domain-name <i>domain-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers authentication username-include],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</code> <code>[edit logical-systems <i>logical-system-name</i> system services static-subscribers authentication username-include],</code> <code>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</code> <code>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers authentication username-include],</code> <code>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</code> <code>[edit system services static-subscribers authentication username-include],</code> <code>[edit system services static-subscribers group <i>group-name</i> authentication username-include]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify the domain name that is included at the end of the username created for all static subscribers or for the static subscribers in a specified group. The group version of the statement takes precedence over the global version.
<b>Options</b>	<b><i>domain-name</i></b> —Domain name that ends the username created for all static subscribers. The username is also sent to RADIUS in the Access-Request message. The string can include the following characters: a through z, A through Z, 0 through 9, “-”, or “.”.
<b>Required Privilege Level</b>	<code>system</code> —To view this statement in the configuration. <code>system-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Subscribers over Static Interfaces on page 288</li><li>• Configuring the Static Subscriber Global Username on page 291</li><li>• Configuring the Static Subscriber Group Username on page 295</li></ul>

## drop

<b>Syntax</b>	drop;
<b>Hierarchy Level</b>	<p>[edit forwarding-options dhcp-relay relay-option-60 vendor-option],</p> <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 relay-option-60 vendor-option],</p> <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 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 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],</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],</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],</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],</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],</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>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	<p>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.</p> <p>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 <b>drop</b> statement at the [edit forwarding-options dhcp-relay relay-option-60 vendor-option (equals   starts-with) (ascii <i>match-string</i>   hexadecimal <i>match-hex</i>)] hierarchy level.</p> <p>To drop DHCP client packets that contain an option 60 string that does <i>not</i> match the ASCII or hexadecimal match string and match criteria (exact match or partial match)</p>

that you specify, include the **drop** statement at the **[edit forwarding-options dhcp-relay relay-option-60 vendor-option]** hierarchy level.

<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.

<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 189</a></li> </ul>
------------------------------	--

## drop-profile (Dynamic Schedulers)

<b>Syntax</b>	<code>drop-profile (<i>profile-name</i>   <i>predefined-variable</i>);</code>
<b>Hierarchy Level</b>	<code>[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)]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. The <code>\$junos-cos-scheduler-dropfile-low</code> , <code>\$junos-cos-scheduler-dropfile-medium-low</code> , <code>\$junos-cos-scheduler-dropfile-medium-high</code> , <code>\$junos-cos-scheduler-dropfile-high</code> , and <code>\$junos-cos-scheduler-dropfile-any</code> predefined variable introduced in Junos OS Release 9.4.
<b>Description</b>	<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 <code>[edit class-of-service drop-profiles]</code> hierarchy level).</p>
<b>Options</b>	<p><b><i>profile-name</i></b>—Name of the drop profile.</p> <p><b><i>predefined-variable</i></b>—One of the following Junos predefined variable that is replaced with a value obtained from the RADIUS server when a subscriber authenticates over the interface to which the dynamic profile is attached:</p> <ul style="list-style-type: none"> <li>• <b><code>\$junos-cos-scheduler-dropfile-low</code></b>—Name of the drop profile for PLP level <b>low</b> and protocol <b>any</b>, specified for a scheduler configured in a dynamic profile for subscriber access.</li> <li>• <b><code>\$junos-cos-scheduler-dropfile-medium-low</code></b>—Name of the drop profile for PLP level <b>medium-low</b> and protocol <b>any</b>, specified for a scheduler configured in a dynamic profile for subscriber access.</li> <li>• <b><code>\$junos-cos-scheduler-dropfile-medium-high</code></b>—Name of the drop profile for PLP level <b>medium-high</b> and protocol <b>any</b>, specified for a scheduler configured in a dynamic profile for subscriber access.</li> <li>• <b><code>\$junos-cos-scheduler-dropfile-high</code></b>—Name of the drop profile for PLP level <b>high</b> and protocol <b>any</b>, specified for a scheduler configured in a dynamic profile for subscriber access.</li> <li>• <b><code>\$junos-cos-scheduler-dropfile-lny</code></b>—Name of the drop profile for PLP level <b>any</b> and protocol <b>any</b>, specified for a scheduler configured in a dynamic profile for subscriber access.</li> </ul>

<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>Configuring Schedulers in a Dynamic Profile for Subscriber Access on page 679</li><li><b>scheduler (Dynamic Scheduler Maps) on page 1174</b></li><li>For more information about configuring drop profiles and drop-profile maps, see the <a href="#">Junos OS Class of Service Configuration Guide</a>.</li></ul>

---

## drop-profile-map (Dynamic Schedulers)

---

<b>Syntax</b>	drop-profile-map loss-priority (any   low   medium-low   medium-high   high) protocol (any   non-tcp   tcp) drop-profile ( <i>profile-name</i>   <i>predefined-variable</i> );
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Define loss priority value for drop profile.  The statements are explained separately.
<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>Configuring Schedulers in a Dynamic Profile for Subscriber Access on page 679</li><li><b>scheduler (Dynamic Scheduler Maps) on page 1174</b></li></ul>



## dscp (Dynamic Classifiers)

---

<b>Syntax</b>	<code>dscp (<i>classifier-name</i>   default);</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> classifiers]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	For IPv4 traffic, apply a Differentiated Services (DiffServ) code point (DSCP) classifier to a subscriber interface in a dynamic profile.
<b>Options</b>	<p><b><i>classifier-name</i></b>—Name of a <b>classifier</b> mapping configured at the [edit class-of-service classifier <b>dscp</b>] hierarchy level.</p> <p><b>default</b>—The default mapping.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>• Applying a Classifier to a Subscriber Interface in a Dynamic Profile on page 687</li><li>• classifiers (Definition)</li></ul>

## dscp (Dynamic Rewrite Rules)

---

<b>Syntax</b>	<code>dscp (<i>rewrite-name</i>   default);</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> rewrite-rules]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	For IPv4 traffic, apply a Differentiated Services (DiffServ) code point (DSCP) rewrite rule to a subscriber interface in a dynamic profile.
<b>Options</b>	<p><b><i>rewrite-name</i></b>—Name of a <b>rewrite-rules</b> mapping configured at the [edit class-of-service rewrite-rules dscp] hierarchy level.</p> <p><b>default</b>—The default mapping.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>Applying a Rewrite Rule Definition to a Subscriber Interface in a Dynamic Profile on page 686</li><li>rewrite-rules</li></ul>

## dscp-ipv6 (Dynamic Classifiers)

<b>Syntax</b>	<code>dscp-ipv6 (<i>classifier-name</i>   default);</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> classifiers]
<b>Release Information</b>	Statement introduced before Junos OS Release 10.1.
<b>Description</b>	For IPv6 traffic, apply a Differentiated Services (DiffServ) code point (DSCP) classifier to a subscriber interface in a dynamic profile.
<b>Options</b>	<p><b><i>classifier-name</i></b>—Name of a classifier mapping configured at the [edit class-of-service classifier <i>ieee-802.1</i>] hierarchy level.</p> <p><b>default</b>—The default mapping.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li> <li>Applying a Classifier to a Subscriber Interface in a Dynamic Profile on page 687</li> <li>classifiers (Definition)</li> </ul>

## dscp-ipv6 (Dynamic Rewrite Rules)

<b>Syntax</b>	<code>dscp-ipv6 (<i>rewrite-name</i>   default);</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> rewrite-rules]
<b>Release Information</b>	Statement introduced before Junos OS Release 10.1.
<b>Description</b>	For IPv6 traffic, apply a DSCP rewrite rule to a subscriber interface in a dynamic profile.
<b>Options</b>	<p><b><i>rewrite-name</i></b>—Name of a rewrite-rules mapping configured at the [edit class-of-service rewrite-rules <i>dscp-ipv6</i>] hierarchy level.</p> <p><b>default</b>—The default mapping.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li> <li>rewrite-rules</li> </ul>

## duplicate-clients-on-interface (DHCP Local Server)

---

<b>Syntax</b>	duplicate-clients-on-interface;
<b>Hierarchy Level</b>	[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]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Configure DHCP local server to include the client subinterface when distinguishing between duplicate DHCP clients (clients with the same MAC address or client ID) in the same subnet. By default, DHCP distinguishes clients by subnet. This feature is supported on DHCPv4 only.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring DHCP Duplicate Client Support on page 109</li></ul>

## duplicate-clients-on-interface (DHCP Relay Agent)

---

<b>Syntax</b>	duplicate-clients-on-interface;
<b>Hierarchy Level</b>	[edit forwarding-options dhcp-relay], [edit logical-systems <i>logical-system-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], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Configure DHCP relay agent to include the client subinterface when distinguishing between duplicate DHCP clients (clients with the same MAC address or client ID) in the same subnet. By default, DHCP relay distinguishes clients by subnet. This feature is supported on DHCPv4 only.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring DHCP Duplicate Client Support on page 109</li><li>Enabling and Disabling Insertion of Option 82 Information on page 192</li></ul>

## duplicate-protection (Dynamic PPPoE)

<b>Syntax</b>	duplicate-protection;
<b>Hierarchy Level</b>	<p>[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>family pppoe],</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> pppoe-underlying-options],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>family pppoe],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> pppoe-underlying-options]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 10.1.</p> <p>(MX Series routers with Trio MPCs only) The [edit ... family pppoe] hierarchies introduced in Junos OS Release 11.2.</p>
<b>Description</b>	Prevent the activation of another dynamic PPPoE logical interface on the same underlying interface when a dynamic PPPoE logical interface for a client with the same media access control (MAC) address is already active on that interface. Duplicate protection is disabled by default. Enabling duplicate protection has no effect on dynamic PPPoE logical interfaces that are already active.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring an Underlying Interface for Dynamic PPPoE Subscriber Interfaces on page 541</li> <li>Configuring the PPPoE Family for an Underlying Interface on page 486</li> <li>For information about creating static PPPoE interfaces, see the <a href="#">Junos OS Network Interfaces Configuration Guide</a></li> </ul>

## dynamic-home-assignment

---

<b>Syntax</b>	<pre>dynamic-home-assignment {   home-agent {     nai (name@domain.com   @domain.com) {       home-agent ip-address;     }   } }</pre>
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> services <b>mobile-ip</b> ], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services <b>mobile-ip</b> ], [edit routing-instances <i>routing-instances-name</i> services <b>mobile-ip</b> ], [edit services <b>mobile-ip</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.
<b>Description</b>	Define the dynamic assignment rule for the home agent.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Mobile IP on page 357</li><li>• Configuring Dynamic Home Assignment for the Mobile Node on page 360</li></ul>

## dynamic-profile (DHCP Local Server)

<b>Syntax</b>	<code>dynamic-profile <i>profile-name</i> &lt;aggregate-clients (merge   replace)   use-primary <i>primary-profile-name</i>&gt;;</code>
<b>Hierarchy Level</b>	<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> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i>],</p> <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> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i>],</p> <p>[edit system services dhcp-local-server],</p> <p>[edit system services dhcp-local-server group <i>group-name</i>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.2.</p> <p>Options <b>aggregate-clients</b> and <b>use-primary</b> introduced in Junos OS Release 9.3.</p>
<b>Description</b>	Specify the dynamic profile that is attached to a group of interfaces or to all interfaces.
<b>Options</b>	<p><b><i>profile-name</i></b>—Name of the dynamic profile.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125</li> </ul>

## dynamic-profile (DHCP Relay Agent)

---

<b>Syntax</b>	<code>dynamic-profile <i>profile-name</i> &lt;aggregate-clients (merge   replace)   use-primary <i>primary-profile-name</i>&gt;;</code>
<b>Hierarchy Level</b>	[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> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the dynamic profile that is attached to a group of interfaces or to all interfaces.
<b>Options</b>	<i>profile-name</i> —Name of the dynamic profile.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125</li></ul>

## dynamic-profile (Domain Maps)

---

<b>Syntax</b>	<code>dynamic-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	[edit access domain map <i>domain-map-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Dynamic profile that is used for subscriber sessions associated with the domain map.
<b>Options</b>	<i>profile-name</i> —Name of dynamic profile.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Specifying a Dynamic Profile in a Domain Map on page 83</li></ul>



## dynamic-profile (Dynamic PPPoE)

<b>Syntax</b>	<code>dynamic-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	<p>[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> pppoe-underlying-options],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> pppoe-underlying-options]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 10.1.</p> <p>(MX Series routers with Trio MPCs only) The [edit ... family pppoe] hierarchies introduced in Junos OS Release 11.2.</p>
<b>Description</b>	<p>Attach a PPPoE dynamic profile to an underlying Ethernet interface. This underlying interface is configured with either the <b>encapsulation ppp-over-ether</b> statement or the <b>family pppoe</b> statement; the two statements are mutually exclusive. When the router creates a dynamic PPPoE logical interface on the underlying interface, it uses the information in the dynamic profile to determine the properties of the dynamic PPPoE logical interface.</p>
<b>Options</b>	<p><b><i>profile-name</i></b>—Name of a previously configured PPPoE dynamic profile, up to 64 characters in length, defined at the [edit dynamic-profiles <i>profile-name</i> interfaces pp0] hierarchy level.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring an Underlying Interface for Dynamic PPPoE Subscriber Interfaces on page 541</li> <li>Configuring the PPPoE Family for an Underlying Interface on page 486</li> <li>For information about creating static PPPoE interfaces, see the <a href="#">Junos OS Network Interfaces Configuration Guide</a></li> </ul>

## dynamic-profile (PPP)

---


<b>Syntax</b>	<code>dynamic-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ppp-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. Support for MLPPP on LSQ interfaces introduced in Junos OS Release 10.2
<b>Description</b>	Specify the dynamic profile that is attached to the interface. On the MX Series routers, this statement is currently supported on PPPoE interfaces only. On the M120 and M320 routers, this statement is supported for MLPPP bundles only on LSQ interfaces on Adaptive Services PICs and Multiservices PICs.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Dynamic Profiles Overview on page 369</li><li>• Configuring a Basic Dynamic Profile on page 391</li><li>• Attaching Dynamic Profiles to Static PPP Subscriber Interfaces on page 223</li><li>• Attaching Dynamic Profiles to MLPPP Bundles on page 227</li><li>• For hardware requirements, see Hardware Requirements for PPP Subscriber Services on Non-Ethernet Interfaces on page 226</li></ul>

## dynamic-profile (PPPoE Service Name Tables)

<b>Syntax</b>	<code>dynamic-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	[ <code>edit protocols pppoe service-name-tables <i>table-name</i> service <i>service-name</i></code> ], [ <code>edit protocols pppoe service-name-tables <i>table-name</i> service <i>service-name</i> agent-specifier aci <i>circuit-id-string</i> ari <i>remote-id-string</i></code> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	<p>Specify a dynamic profile to instantiate a dynamic PPPoE interface. You can associate a dynamic profile with a named service entry, <b>empty</b> service entry, or <b>any</b> service entry configured in a PPPoE service name table, or with an agent circuit identifier/agent remote identifier (ACI/ARI) pair defined for these services.</p> <p>The dynamic profile associated with a service entry in a PPPoE service name table overrides the dynamic profile associated with the PPPoE underlying interface on which the dynamic PPPoE interface is created.</p> <p>If you include the <b>dynamic-profile</b> statement at the [<code>edit protocols pppoe service-name-tables <i>table-name</i> service <i>service-name</i> agent-specifier aci <i>circuit-id-string</i> ari <i>remote-id-string</i></code>] hierarchy level, you cannot also include the <b>static-interface</b> statement at this level. The <b>dynamic-profile</b> and <b>static-interface</b> statements are mutually exclusive for ACI/ARI pair configurations.</p>
<b>Options</b>	<b><i>profile-name</i></b> —Name of the dynamic profile that the router uses to instantiate a dynamic PPPoE interface.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring PPPoE Service Name Tables</li> <li>Assigning a Dynamic Profile and Routing Instance to a Service Name or ACI/ARI Pair for Dynamic PPPoE Interface Creation on page 543</li> </ul>

## dynamic-profile (Static Subscribers)

---

<b>Syntax</b>	<code>dynamic-profile <i>profile-name</i> {     aggregate-clients (merge   replace); }</code>
<b>Hierarchy Level</b>	<code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> system services static-subscribers],</code> <code>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i>],</code> <code>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers],</code> <code>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i>],</code> <code>[edit system services static-subscribers],</code> <code>[edit system services static-subscribers group <i>group-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify the dynamic client profile that is instantiated at login and de-instantiated at logout for all static subscribers on interfaces configured at the <b>[edit system services static-subscribers interface]</b> hierarchy level or for the static subscribers in a specific group. The group version of the statement takes precedence over the global version.
<div> <b>NOTE:</b> Do not specify a dynamic profile that creates a dynamic interface.</div>	
<b>Default</b>	By default, the <i>junos-default-profile</i> is used when you do not specify a global dynamic profile with this statement.
<b>Options</b>	<b><i>profile-name</i></b> —Name of the dynamic client profile profile.  The remaining statement is explained separately.
<b>Required Privilege Level</b>	<b>access</b> —To view this statement in the configuration. <b>access-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Subscribers over Static Interfaces on page 288</li><li>• Specifying the Static Subscriber Global Dynamic Profile on page 289</li><li>• Specifying the Static Subscriber Group Dynamic Profile on page 293</li></ul>

## dynamic-profiles

```

Syntax  dynamic-profiles {
        profile-name {
            class-of-service {
                interfaces {
                    interface-name ;
                }
                unit logical-unit-number {
                    classifiers {
                        type (classifier-name | default);
                    }
                    output-traffic-control-profile profile-name;
                    rewrite-rules {
                        dscp (rewrite-name | default);
                        dscp-ipv6 (rewrite-name | default);
                        ieee-802.1 (rewrite-name | default) vlan-tag (outer | outer-and-inner);
                        inet-precedence (rewrite-name | default);
                    }
                }
            }
        }
        scheduler-maps {
            map-name {
                forwarding-class class-name scheduler scheduler-name;
            }
        }
        schedulers {
            (scheduler-name) {
                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;
                excess-priority (low | high | $junos-cos-scheduler-excess-priority);
                excess-rate (percent percentage | percent $junos-cos-scheduler-excess-rate);
                overhead-accounting (shaping-mode) <bytes (byte-value)>;
                priority priority-level;
                shaping-rate (rate | predefined-variable);
                transmit-rate (percent percentage | rate | remainder) <exact | rate-limit>;
            }
        }
        traffic-control-profiles profile-name {
            delay-buffer-rate (percent percentage | rate | $junos-cos-delay-buffer-rate);
            excess-rate (percent percentage | proportion value | percent $junos-cos-excess-rate);
            guaranteed-rate (percent percentage | rate | $junos-cos-guaranteed-rate);
            overhead-accounting (shaping-mode) <bytes (byte-value)>;
            scheduler-map map-name;
            shaping-rate (rate | predefined-variable);
        }
    }
    firewall {
        family family {
            fast-update-filter filter-name {
                interface-specific;
                match-order [match-order];
            }
        }
    }

```

Copyright © 2011, Juniper Networks, Inc.

```

        service-filter filter-name;
    }
}
output-vlan-map {
    inner-tag-protocol-id tpid;
    inner-vlan-id number;
    (pop | swap);
    tag-protocol-id tpid;
    vlan-id number;
}
}
unnumbered-address interface-name <preferred-source-address address>;
}
ppp-options {
    chap;
    pap;
}
vlan-id number;
vlan-tags outer [tpid].vlan-id [inner [tpid].vlan-id];
}
}
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;
        }
    }
    mld {
        interface interface-name {
            disable;
            (accounting | no-accounting);
            group-policy;
            immediate-leave;
            oif-map;
            passive;
            ssm-map ssm-map-name;
            static {
                group multicast-group-address {
                    exclude;
                    group-count number;
                    group-increment increment;
                    source ip-address {
                        source-count number;
                        source-increment increment;
                    }
                }
            }
        }
    }
}

```

```

    }
  }
  version version;
}
}
router-advertisement {
  interface interface-name {
    current-hop-limit number;
    default-lifetime seconds;
    (managed-configuration | no-managed-configuration);
    max-advertisement-interval seconds;
    min-advertisement-interval seconds;
    (other-stateful-configuration | no-other-stateful-configuration);
    prefix prefix;
    reachable-time milliseconds;
    retransmit-timer milliseconds;
  }
}
}
routing-instances {
  interface interface-name;
}
routing-options {
  access {
    route prefix {
      next-hop next-hop;
      metric route-cost;
      preference route-distance;
      tag route-tag;
    }
  }
  access-internal {
    route subscriber-ip-address {
      qualified-next-hop underlying-interface {
        mac-address address;
      }
    }
  }
  multicast {
    interface interface-name {
      no-qos-adjust;
    }
  }
}
variables {
  variable-name {
    mandatory;
    default-value default-value;
    radius {
      vendor-id id {
        attribute attribute-number;
        tag tag-number;
      }
    }
  }
}
}

```



```

    }
  }
}

```

<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Create dynamic profiles for use with DHCP or PPP client access.
<b>Options</b>	<p><b><i>profile-name</i></b>—Name of the dynamic profile; string of up to 80 alphanumeric characters.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Dynamic Profiles Overview on page 369</li> <li>Configuring a Basic Dynamic Profile on page 391</li> </ul>

## enable-service

<b>Syntax</b>	<code>enable-service <i>interface-name</i>;</code>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip home-agent],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip home-agent],</p> <p>[edit routing-instances <i>routing-instances-name</i> services mobile-ip home-agent],</p> <p>[edit services mobile-ip home-agent]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.</p>
<b>Description</b>	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. Include the statement once for each interface to be enabled.
<b>Options</b>	<b><i>interface-name</i></b> —Interface on which the home agent can be enabled.
<b>Required Privilege Level</b>	<p>view—To view this statement in the configuration.</p> <p>view-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Mobile IP on page 357</li> <li>Configuring the Mobile IP Home Agent on page 358</li> </ul>

## encapsulation (Dynamic Interfaces)

---

<b>Syntax</b>	<code>encapsulation (atm-ccc-cell-relay   atm-ccc-vc-mux   atm-cisco-nlpid   atm-tcc-vc-mux   atm-mlppp-llc   atm-nlpid   atm-ppp-llc   atm-ppp-vc-mux   atm-snap   atm-tcc-snap   atm-vc-mux   ether-over-atm-llc   ether-vpls-over-atm-llc   ether-vpls-over-fr   ether-vpls-over-ppp   ethernet   frame-relay-ccc   frame-relay-ppp   frame-relay-tcc   frame-relay-ether-type   frame-relay-ether-type-tcc   multilink-frame-relay-end-to-end   multilink-ppp   ppp-over-ether   ppp-over-ether-over-atm-llc   vlan-bridge   vlan-ccc   vlan-vci-ccc   vlan-tcc   vlan-vpls);</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Dynamic interface configuration of the logical link-layer encapsulation type.
<b>Options</b>	<p><b>atm-ccc-cell-relay</b>—Use ATM cell-relay encapsulation.</p> <p><b>atm-ccc-vc-mux</b>—Use ATM virtual circuit (VC) multiplex encapsulation on circuit cross-connect (CCC) circuits. When you use this encapsulation type, you can configure the <b>ccc</b> family only.</p> <p><b>atm-cisco-nlpid</b>—Use Cisco ATM network layer protocol ID (NLPID) encapsulation. When you use this encapsulation type, you can configure the <b>inet</b> family only.</p> <p><b>atm-mlppp-llc</b>—For ATM2 IQ interfaces only, use Multilink Point-to-Point Protocol (MLPPP) over AAL5 LLC. For this encapsulation type, your router must be equipped with a link services or voice services PIC. MLPPP over ATM encapsulation is not supported on ATM2 IQ OC48 interfaces.</p> <p><b>atm-nlpid</b>—Use ATM NLPID encapsulation. When you use this encapsulation type, you can configure the <b>inet</b> family only.</p> <p><b>atm-ppp-llc</b>—For ATM2 IQ interfaces only, use PPP over AAL5 LLC encapsulation.</p> <p><b>atm-ppp-vc-mux</b>—For ATM2 IQ interfaces only, use PPP over ATM AAL5 multiplex encapsulation.</p> <p><b>atm-snap</b>—Use ATM subnetwork attachment point (SNAP) encapsulation.</p> <p><b>atm-tcc-snap</b>—Use ATM SNAP encapsulation on translational cross-connect (TCC) circuits.</p> <p><b>atm-tcc-vc-mux</b>—Use ATM VC multiplex encapsulation on TCC circuits. When you use this encapsulation type, you can configure the <b>tcc</b> family only.</p> <p><b>atm-vc-mux</b>—Use ATM VC multiplex encapsulation. When you use this encapsulation type, you can configure the <b>inet</b> family only.</p> <p><b>ether-over-atm-llc</b>—For interfaces that carry IPv4 traffic, use Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure multipoint interfaces.</p>

**ether-vpls-over-atm-llc**—For ATM2 IQ interfaces only, use the Ethernet virtual private LAN service (VPLS) over ATM LLC encapsulation to bridge Ethernet interfaces and ATM interfaces over a VPLS routing instance (as described in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*). Packets from the ATM interfaces are converted to standard ENET2/802.3 encapsulated Ethernet frames with the frame check sequence (FCS) field removed.

**ether-vpls-over-fr**—For E1, T1, E3, T3, and SONET interfaces only, use the Ethernet virtual private LAN service (VPLS) over Frame Relay encapsulation to support Bridged Ethernet over Frame Relay encapsulated TDM interfaces for VPLS applications, as per *Multiprotocol Interconnect over Frame Relay* (RFC 2427 [1490]).

**ether-vpls-over-ppp**—For E1, T1, E3, T3 and SONET interfaces only, use the Ethernet virtual private LAN service (VPLS) over PPP encapsulation to support Bridged Ethernet over PPP encapsulated TDM interfaces for VPLS applications.

**ethernet**—Use Ethernet II encapsulation (as described in RFC 894, *A Standard for the Transmission of IP Datagrams over Ethernet Networks*).

**ethernet-vpls**—Use Ethernet VPLS encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard Tag Protocol ID (TPID) values.

**extended-vlan-vpls**—Use extended virtual LAN (VLAN) VPLS encapsulation on Ethernet interfaces that have VLAN 802.1Q tagging and VPLS enabled and that must accept packets carrying TPIDs 0x8100, 0x9100, and 0x9901.



**NOTE:** The built-in Gigabit Ethernet PIC on an M7i router does not support extended VLAN VPLS encapsulation.

**frame-relay-ccc**—Use Frame Relay encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

**frame-relay-ppp**—Use PPP over Frame Relay circuits. When you use this encapsulation type, you can configure the **ppp** family only. J Series routers do not support **frame-relay-ppp** encapsulation.

**frame-relay-tcc**—Use Frame Relay encapsulation on TCC circuits for connecting unlike media. When you use this encapsulation type, you can configure the **tcc** family only.

**frame-relay-ether-type**—Use Frame Relay ether type encapsulation for compatibility with Cisco Frame Relay. The physical interface must be configured with **flexible-frame-relay** encapsulation.

**frame-relay-ether-type-tcc**—Use Frame Relay ether type TCC for Cisco-compatible Frame Relay on TCC circuits to connect unlike media. The physical interface must be configured with **flexible-frame-relay** encapsulation.

**multilink-frame-relay-end-to-end**—Use MLFR FRF.15 encapsulation. This encapsulation is used only on multilink, link services, and voice services interfaces and their constituent T1 or E1 interfaces, and is supported on LSQ and redundant LSQ interfaces.

**multilink-ppp**—Use MLPPP encapsulation. This encapsulation is used only on multilink, link services, and voice services interfaces and their constituent T1 or E1 interfaces.

**ppp-over-ether**—For underlying Ethernet interfaces on J Series Services routers, use PPP over Ethernet encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead, configure the interface address on the PPP interface. You also use PPP over Ethernet encapsulation to configure an underlying Ethernet interface for a dynamic PPPoE logical interface on M120 and M320 Series routers with Intelligent Queuing 2 (IQ2) PICs, and on MX Series routers with Trio MPC/MIC interfaces.

**ppp-over-ether-over-atm-llc**—For underlying ATM interfaces on J Series Services routers only, use PPP over Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead, configure the interface address on the PPP interface.

**vlan-bridge**—Use Ethernet VLAN bridge encapsulation on Ethernet interfaces that have IEEE 802.1Q tagging, flexible ethernet services, and bridging enabled, and that must accept packets carrying TPID 0x8100 or a user-defined TPID.

**vlan-ccc**—Use Ethernet virtual LAN (VLAN) encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

**vlan-vci-ccc**—Use ATM-to-Ethernet interworking encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

**vlan-tcc**—Use Ethernet VLAN encapsulation on TCC circuits. When you use this encapsulation type, you can configure the **tcc** family only.

**vlan-vpls**—Use Ethernet VLAN encapsulation on VPLS circuits.

<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
---------------------------------	---

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Retail Dynamic Profile for Use in the Layer 2 Wholesale Solution</li><li><a href="#">Junos OS Services Interfaces Configuration Guide</a></li></ul>
------------------------------	---

## entity-type

<b>Syntax</b>	entity-type (host   mobility-agent);
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> services mobile-ip peer spi <i>hexadecimal-value</i> ], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer spi <i>hexadecimal-value</i> ], [edit routing-instances <i>routing-instances-name</i> services mobile-ip peer spi <i>hexadecimal-value</i> ], [edit services mobile-ip peer spi <i>hexadecimal-value</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.
<b>Description</b>	Configure the security parameter for the peer entity—, either a mobile node, home agent, or foreign agent.
<b>Options</b>	<b>host</b> —Use the mobile node in home agent  <b>mobility-agent</b> —Use the home agent or foreign agent
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Mobile IP on page 357</li> <li>Configuring the Mobile IP Home Agent on page 358</li> </ul>

## ethernet-port-type-virtual

<b>Syntax</b>	ethernet-port-type-virtual;
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> radius options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
<b>Description</b>	Specify the physical port type the router or switch uses to authenticate clients. The router or switch passes a port type of <b>ethernet</b> in RADIUS attribute 61 (NAS-Port-Type) by default. This statement specifies a port type of <b>virtual</b> .
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring RADIUS Server Options for Subscriber Access on page 29</li> <li>Configuring RADIUS Server Parameters for Subscriber Access on page 26</li> </ul>

## excess-priority (Dynamic Schedulers)

---

<b>Syntax</b>	<code>excess-priority (low   high   \$junos-cos-scheduler-excess-priority);</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Determine the priority of excess bandwidth traffic on a scheduler in a dynamic profile.
<b>Options</b>	<p><b>low</b>—Excess traffic for this scheduler has low priority.</p> <p><b>high</b>—Excess traffic for this scheduler has high priority.</p> <p><b>\$junos-cos-scheduler-excess-priority</b>—Variable for the excess-priority that is replaced with a value obtained from the RADIUS server when a subscriber authenticates over the interface to which the dynamic profile is attached.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Managing Excess Bandwidth Distribution for Dynamic CoS on page 757</li><li><b>scheduler on page 1174</b></li></ul>

## excess-rate (Dynamic Schedulers)

---

<b>Syntax</b>	<code>excess-rate percent (<i>percentage</i>   \$junos-cos-scheduler-excess-rate);</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Determine the percentage of excess bandwidth traffic to share.
<b>Options</b>	<p><b><i>percentage</i></b>—Percentage of the excess bandwidth to share.</p> <p><b>Range:</b> 0 through 100 percent</p> <p><b>\$junos-cos-scheduler-excess-rate</b>—Variable for the excess rate that is specified for a scheduler. The variable is replaced with a value obtained from the RADIUS server when a subscriber authenticates over the interface to which the dynamic profile is attached.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>Managing Excess Bandwidth Distribution for Dynamic CoS on page 757</li><li><b>output-traffic-control-profile on page 1092</b></li></ul>

## excess-rate (Dynamic Traffic Shaping)

<b>Syntax</b>	<code>excess-rate ( (percent <i>percentage</i>   \$junos-cos-excess-rate)   proportion <i>value</i> );</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Determine the percentage or proportion of excess bandwidth traffic to share.
<b>Options</b>	<p><b><i>percentage</i></b>—Percentage of the excess bandwidth to share.  <b>Range:</b> 0 through 100 percent</p> <p><b><i>value</i></b>—Proportion of the excess bandwidth to share.  <b>Range:</b> 0 through 1000</p> <p><b>\$junos-cos-excess-rate</b>—Variable for the excess rate that is specified for the logical interface. The variable is replaced with a value obtained from the RADIUS server when a subscriber authenticates over the interface to which the dynamic profile is attached.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li> <li>Managing Excess Bandwidth Distribution for Dynamic CoS on page 757</li> <li><b>output-traffic-control-profile on page 1092</b></li> </ul>

## 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 ];  
          event-timestamp [ accounting-on | accounting-off | accounting-start | accounting-stop  
                              ];  
          framed-ip-address [ accounting-start | accounting-stop ];  
          framed-ip-netmask [ accounting-start | accounting-stop ];  
          input-filter [ accounting-start | accounting-stop ];  
          input-gigapackets [ accounting-stop ];  
          input-gigawords [ accounting-stop ];  
          interface-description [ access-request | accounting-start | accounting-stop ];  
          nas-identifier [ access-request | accounting-on | accounting-off | accounting-start |  
                              accounting-stop ];  
          nas-port [ access-request | accounting-start | accounting-stop ];  
          nas-port-id [ access-request | accounting-start | accounting-stop ];  
          nas-port-type [ access-request | accounting-start | accounting-stop ];  
          output-filter [ accounting-start | accounting-stop ];  
          output-gigapackets [ accounting-stop ];  
          output-gigawords [ accounting-stop ];  
          }  
          }`

**Hierarchy Level**    [edit access profile *profile-name* radius attributes]

**Release Information**    Statement introduced in Junos OS Release 9.1.  
                              Statement introduced in Junos OS Release 9.1 for EX Series switches.

**Description**    Configure the router or switch 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 or switch 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  
Documentation**

- Configuring RADIUS Server Parameters for Subscriber Access on page 26

## exclude (Dynamic MLD Interface)

---

<b>Syntax</b>	exclude;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols mld interface <i>interface-name</i> static group <i>multicast-group-address</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Configure the group to operate in exclude mode on the dynamic interface. In exclude mode all sources except the address configured are accepted for the group. By default, the group operates in include mode.
<b>Required Privilege Level</b>	view-level—To view this statement in the configuration. control-level—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Enabling MLD Static Group Membership</li></ul>

## external-authority

---

<b>Syntax</b>	external-authority;
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>pool-match-order</b> ], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server <b>pool-match-order</b> ], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>pool-match-order</b> ], [edit system services dhcp-local-server <b>pool-match-order</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	<p>Specify that an external authority (for example, RADIUS or Diameter) provides the address assignment.</p> <p>When RADIUS is the external authority, the router uses the Framed-IPv6-Pool attribute (RADIUS attribute 100) to select the pool. When Diameter is the external authority, the router uses the Diameter counterpart of RADIUS Framed-IPv6-Pool attribute.</p>
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 111</li><li>Extended DHCP Local Server Overview on page 98</li><li>Address-Assignment Pools Overview on page 67</li></ul>

## fail-over-within-preference (L2TP LAC)

---

<b>Syntax</b>	fail-over-within-preference;
<b>Hierarchy Level</b>	[edit services l2tp]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Enable L2TP LAC tunnel selection within a preference level. When the router is unable to connect to a destination at a given preference level, it attempts to connect to another destination at the same level. By default, when a connection attempt fails at one preference level, the next attempt is made at the next lower level.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring LAC Tunnel Selection Failover Within a Preference Level on page 244</a></li><li>• <a href="#">Configuring the L2TP LAC Tunnel Selection Parameters on page 244</a></li></ul>

## family (Address-Assignment Pools)

---

**Syntax**    family *family* {  
              dhcp-attributes {  
                  [*protocol-specific attributes*]  
              }  
              host *hostname* {  
                  hardware-address *mac-address*;  
                  ip-address *ip-address*;  
              }  
              network *ip-prefix* / <*prefix-length*>;  
              prefix *ipv6-prefix*;  
              range *range-name* {  
                  high *upper-limit*;  
                  low *lower-limit*;  
                  prefix-length *prefix-length*;  
              }  
          }

**Hierarchy Level**    [edit access address-assignment pool *pool-name*]

**Release Information**    Statement introduced in Junos OS Release 9.0.

**Description**    Configure the protocol family for the address-assignment pool.

**Options**    *family*—Protocol family:

- **inet**—Internet Protocol version 4 suite
- **inet6**—Internet Protocol version 6 suite

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 Documentation**    • Address-Assignment Pools Overview on page 67  
                                  • Configuring Address-Assignment Pools on page 68

## family (Dynamic Firewalls)

**Syntax**

```
family family {
    fast-update-filter filter-name {
        interface-specific;
        match-order [match-order];
        term term-name {
            from {
                match-conditions;
            }
            then {
                action;
                action-modifiers;
            }
            only-at-create;
        }
    }
}
```

**Hierarchy Level** [edit dynamic-profiles *profile-name* firewall]

**Release Information** Statement introduced in Junos OS Release 9.6.

**Description** Configure protocol family information for firewall filters in a dynamic profile.

**Options** *family*—Protocol family:

- **inet**—Internet Protocol version 4 suite
- **inet6**—Internet Protocol version 6 suite

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 Documentation**

- Configuring Fast Update Filters on page 581

## family (Dynamic Demux Interface)

**Syntax**    `family family {`  
                   `access-concentrator name;`  
                   `address address;`  
                   `demux-source {`  
                     `source-address;`  
                   `}`  
                   `duplicate-protection;`  
                   `dynamic-profile profile-name;`  
                   `filter {`  
                     `input filter-name;`  
                     `output filter-name;`  
                   `}`  
                   `mac-validate (loose | strict):`  
                   `max-sessions number;`  
                   `service-name-table table-name`  
                   `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 in Junos OS Release 9.3.  
                               Option **pppoe** introduced in Junos OS Release 11.2.

**Description**    Configure protocol family information for the logical interface.



**NOTE:** Not all subordinate stanzas are available to every protocol family. See the [Junos OS Configuration Statements and Commands](#) for details about each protocol family.

**Options**    *family*—Protocol family:

- **inet**—Internet Protocol version 4 suite
- **inet6**—Internet Protocol version 6 suite
- **pppoe**—(MX Series routers with Trio MPCs only) Point-to-Point Protocol over Ethernet

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 Documentation**    • Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 445

• For information about static IP demux interfaces, see the [Junos OS Network Interfaces Configuration Guide](#)

## family (Dynamic PPPoE)

```
Syntax  family family {
        unnumbered-address interface-name destination address;
        address address;
        service {
            input {
                service-set service-set-name {
                    service-filter filter-name;
                }
                post-service-filter filter-name;
            }
            output {
                service-set service-set-name {
                    service-filter filter-name;
                }
            }
        }
        filter {
            input filter-name {
                precedence precedence;
            }
            output filter-name {
                precedence precedence;
            }
        }
    }
```

**Hierarchy Level** [edit dynamic-profiles *profile-name* interfaces pp0 unit "\$junos-interface-unit"]

**Release Information** Statement introduced in Junos OS Release 10.1.

**Description** Configure protocol family information for the logical interface. Only the Internet Protocol version 4 (IPv4) protocol family is currently supported for dynamic PPPoE logical interfaces.

**Options** *family*—Protocol family:

- **inet**—Internet Protocol version 4 suite

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 Documentation**

- Configuring a Basic PPPoE Dynamic Profile on page 536
- Configuring a PPPoE Dynamic Profile with Additional Options on page 539
- For information about creating static PPPoE interfaces, see the [Junos OS Network Interfaces Configuration Guide](#)

## family (Dynamic Standard Interface)

```
Syntax  family family {
        access-concentrator name;
        address address;
        duplicate-protection;
        dynamic-profile profile-name;
        filter {
            adf {
                counter;
                input-precedence precedence;
                output-precedence precedence;
                rule rule-value;
            }
            input filter-name {
                precedence precedence;
            }
            output filter-name {
                precedence precedence;
            }
        }
        max-sessions number;
        service {
            input {
                service-set service-set-name {
                    service-filter filter-name;
                }
                post-service-filter filter-name;
            }
            output {
                service-set service-set-name {
                    service-filter filter-name;
                }
            }
        }
        service-name-table table-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 in Junos OS Release 9.2.  
Option **pppoe** introduced in Junos OS Release 11.2.

**Description** Configure protocol family information for the logical interface.



**NOTE:** Not all subordinate stanzas are available to every protocol family. See the *Junos OS Configuration Statements and Commands* for details about each protocol family.



**Options**    *family*—Protocol family:

- **inet**—IP version 4 suite
- **inet6**—IP version 6 suite
- **pppoe**—(MX Series routers with Trio MPCs only) Point-to-Point Protocol over Ethernet
- **vpls**—Virtual private LAN service

The remaining statements are explained separately.

**Required Privilege**    interface—To view this statement in the configuration.  
**Level**                    interface-control—To add this statement to the configuration.

**Related**                • For general information about configuring static interfaces, see the [Junos OS Network](#)  
**Documentation**        [Interfaces Configuration Guide](#).  
                              • “Configuring the Protocol Family,” in the [Junos OS Network Interfaces Configuration Guide](#).

## fast-update-filter (Dynamic Firewalls)

---

**Syntax**    `fast-update-filter filter-name {  
                  interface-specific;  
                  match-order [match-order];  
                  term term-name {  
                      from {  
                          match-conditions;  
                      }  
                      then {  
                          action;  
                          action-modifiers;  
                      }  
                      only-at-create;  
                  }  
          }`

**Hierarchy Level**    `[edit dynamic-profiles profile-name firewall family family]`

**Release Information**    Statement introduced in Junos OS Release 9.6.

**Description**    Configure fast update firewall filters in a dynamic profile.

**Options**    *filter-name*—Name that identifies the filter. The name can contain letters, numbers, and hyphens (-) and can be up to 64 characters long. To include spaces in the name, enclose it in quotation marks (" ").

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 Documentation**    • Configuring Fast Update Filters on page 581

## filter (Dynamic Firewalls)

<b>Syntax</b>	<pre> filter {   adf {     counter;     input-precedence <i>precedence</i>;     output-precedence <i>precedence</i>;     rule <i>rule-value</i>;   }   input <i>filter-name</i> (     precedence <i>precedence</i>;   )   output <i>filter-name</i> {     precedence <i>precedence</i>;   } } </pre>
<b>Hierarchy Level</b>	<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 dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.2.</p> <p>The [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i>] hierarchy introduced in Junos 10.1.</p>
<b>Description</b>	<p>Apply a dynamic filter to an interface. You can configure filters for either <b>family inet</b> or <b>family inet6</b>, and the filters can be classic filters, fast update filters, or (for the <b>adf</b> statement) Ascend-Data-Filters. Only the Internet Protocol version 4 (IPv4) protocol family is currently supported for dynamic PPPoE logical interfaces.</p>
<b>Options</b>	<p><b>input <i>filter-name</i></b>—Name of one filter to evaluate when packets are received on the interface.</p> <p><b>output <i>filter-name</i></b>—Name of one filter to evaluate when packets are transmitted on the interface.</p> <p>The remaining statement is explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>For general information about configuring firewall filters, see the <a href="#">Junos OS Routing Policy Configuration Guide</a></li> <li>Dynamic Firewall Filters Overview on page 555</li> <li>Classic Filters Overview on page 556</li> <li>Basic Classic Filter Syntax on page 558</li> </ul>

## firewall (Dynamic Firewalls)

---

**Syntax**    firewall {  
              family *family* {  
                  fast-update-filter *filter-name* {  
                      interface-specific;  
                      match-order [*match-order*];  
                      term *term-name* {  
                          from {  
                              *match-conditions*;  
                          }  
                          then {  
                              *action*;  
                              *action-modifiers*;  
                          }  
                          only-at-create;  
                      }  
                  }  
              }  
          }

**Hierarchy Level**    [edit **dynamic-profiles** *profile-name*]

**Release Information**    Statement introduced in Junos OS Release 9.6.

**Description**    Configure firewall filters 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 Documentation**    • Configuring Fast Update Filters on page 581

## forward-snooped-clients (DHCP Local Server)

<b>Syntax</b>	forward-snooped-clients (all-interfaces   configured-interfaces   non-configured-interfaces);
<b>Hierarchy Level</b>	[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]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Configure how the DHCP local server handles DHCP snooped packets on specific interfaces.
<b>Options</b>	<p><b>all-interfaces</b>—Perform the action on all interfaces.</p> <p><b>configured-interfaces</b>—Perform the action only on configured interfaces.</p> <p><b>non-configured-interfaces</b>—Perform the action only on nonconfigured interfaces.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>DHCP Snooping Support on page 174</li> <li>Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server on page 119</li> </ul>

## forward-snooped-clients (DHCP Relay Agent)

---

<b>Syntax</b>	forward-snooped-clients (all-interfaces   configured-interfaces   non-configured-interfaces);
<b>Hierarchy Level</b>	[edit forwarding-options dhcp-relay], [edit logical-systems <i>logical-system-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], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	<p>Configure how DHCP relay agent handles DHCP snooped packets on specific interfaces. The router determines the DHCP snooping action to perform based on a combination of the <b>forward-snooped-clients</b> configuration and the configuration of either the <b>allow-snooped-clients</b> statement or the <b>no-allow-snooped-clients</b> statement.</p> <p>The router also uses this statement to determine how to handle snooped BOOTREPLY packets received on nonconfigured interfaces.</p>
<b>Options</b>	<p><b>all-interfaces</b>—Perform the action on all interfaces.</p> <p><b>configured-interfaces</b>—Perform the action only on configured interfaces.</p> <p><b>non-configured-interfaces</b>—Perform the action only on nonconfigured interfaces.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• DHCP Snooping Support on page 174</li><li>• Configuring DHCP Snooping for DHCP Relay Agent on page 175</li></ul>

## forwarding (Diameter Network Element)

<b>Syntax</b>	<pre>forwarding {   route <i>dne-route-name</i> {     destination realm <i>realm-name</i> &lt;host <i>hostname</i>&gt;;     function <i>function-name</i> &lt;partition <i>partition-name</i>&gt;;     metric <i>route-metric</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit diameter network-element <i>element-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	<p>Define the criteria that specify which destinations are reachable through the Diameter network element.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Diameter on page 259</li> <li>Configuring Diameter Network Elements on page 261</li> </ul>

## forwarding-class (Dynamic Scheduler Maps)

<b>Syntax</b>	forwarding-class <i>class-name</i> ;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service scheduler-maps <i>map-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Associate a scheduler with a scheduler map.
<b>Options</b>	<i>class-name</i> —Name of the forwarding class.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li> <li>Configuring Schedulers in a Dynamic Profile for Subscriber Access on page 679</li> </ul>

## forwarding-class (Subscriber Secure Policy)

---

<b>Syntax</b>	<code>forwarding-class class-name;</code>
<b>Hierarchy Level</b>	<code>[edit services radius-flow-tap]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
<b>Description</b>	Specify forwarding class that is applied to mirrored packets sent to a mediation device.
<b>Options</b>	<i>class-name</i> —Name of the forwarding class.
<b>Required Privilege Level</b>	flow-tap—To view this statement in the configuration. flow-tap-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Subscriber Secure Policy Overview on page 625</li><li>Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 635</li></ul>

## from

---

<b>Syntax</b>	<pre>from {   applications [ <i>application-names</i> ];   destination-address <i>address</i> &lt;except&gt;;   destination-prefix-list <i>list-name</i> &lt;except&gt;; }</pre>
<b>Hierarchy Level</b>	<code>[edit services captive-portal-content-delivery rule <i>rule-name</i> term <i>term-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify input conditions for a captive portal term.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Redirecting HTTP Requests on page 613</li><li>For information on match conditions, see the description of firewall filter match conditions in the <a href="#">Junos OS Routing Policy Configuration Guide</a>.</li></ul>



## function (Diameter Network Element)

---

<b>Syntax</b>	<code>function <i>function-name</i>;</code>
<b>Hierarchy Level</b>	[edit diameter network-element <i>element-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1. Support for PTSP introduced in Junos OS Release 10.2. Support for Gx-Plus introduced in Junos OS Release 11.2.
<b>Description</b>	Specify the application (function) associated with a Diameter network element.
<b>Default</b>	By default, all functions are associated with (supported by) the network element.
<b>Options</b>	<i>function-name</i> —Application (function) associated with the route. Gx-Plus, JSRC, and packet-triggered subscribers are the applications currently supported.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Diameter on page 259</li><li>• Configuring Diameter Network Elements on page 261</li></ul>

## function (Diameter Route)

---

<b>Syntax</b>	<code>function <i>function-name</i> &lt;partition <i>partition-name</i>&gt;;</code>
<b>Hierarchy Level</b>	[edit diameter network-element <i>element-name</i> forwarding route <i>dne-route-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6. Support for PTSP introduced in Junos OS Release 10.2. Support for Gx-Plus introduced in Junos OS Release 11.2.
<b>Description</b>	Specify the application (function) associated with a destination and metric. Together, these three elements define a route reachable through a Diameter network element.
<b>Default</b>	All functions are associated with the route.
<b>Options</b>	<b><i>function-name</i></b> —Application (function) associated with the route. Gx-Plus, JSRC, and packet-triggered-subscribers are the applications currently supported.  <b><i>partition partition-name</i></b> —(Optional) Partition associated with the application (function).
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Diameter on page 259</li><li>Configuring Diameter Network Elements on page 261</li></ul>

## gateway-name (Tunnel Profile Remote Gateway)

---

<b>Syntax</b>	<code>gateway-name <i>server-name</i>;</code>
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i> remote-gateway]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the hostname expected by the remote gateway—the LNS—from the source gateway—the LAC—when you set up a tunnel.
<b>Options</b>	<b><i>server-name</i></b> —Name of the LNS.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Tunnel Profile for Subscriber Access on page 242</li></ul>

## gateway-name (Tunnel Profile Source Gateway)

<b>Syntax</b>	<code>gateway-name <i>client-name</i>;</code>
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i> source-gateway]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the hostname provided by the source gateway—the LAC—to the remote gateway—the LNS—when you set up a tunnel.
<b>Options</b>	<i>client-name</i> —Name of the LAC.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring a Tunnel Profile for Subscriber Access on page 242</li> </ul>

## generic

<b>Syntax</b>	<code>generic;</code>
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> services <b>mobile-ip</b> access-type], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> services <b>mobile-ip</b> access-type], [edit routing-instances <i>routing-instance-name</i> services <b>mobile-ip</b> access-type], [edit services <b>mobile-ip</b> access-type]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Disable WiMAX features for Mobile IP home agent, preventing interoperability in a WiMAX environment.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Mobile IP on page 357</li> <li>Configuring the Access Type for Mobile IP on page 361</li> </ul>

## global (Gx-Plus)

---

<b>Syntax</b>	<code>global {     max-outstanding-requests <i>number</i>; }</code>
<b>Hierarchy Level</b>	[edit access gx-plus]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Configure global attributes for the Gx-Plus application.  The remaining statement is explained separately.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Gx-Plus on page 339</li></ul>

## grace-period

---

<b>Syntax</b>	<code>grace-period <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family (inet   inet6) dhcp-attributes]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	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.
<b>Options</b>	<b><i>seconds</i></b> —Number of seconds the lease is retained. <b>Range:</b> 0 through 4,294,967,295 seconds <b>Default:</b> 0 (no grace period)
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Address-Assignment Pools on page 68</li></ul>

## group (DHCP Local Server)

**Syntax**

```
group group-name {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      logical-system-name;
      mac-address;
      option-60;
      option-82 <circuit-id> <remote-id>;
      relay-agent-interface-id
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
    primary-profile-name>;
  interface interface-name {
    exclude;
    overrides {
      client-discover-match <option60-and-option82>;
      interface-client-limit number;
      no-arp;
    }
    trace;
    upto upto-interface-name;
  }
  overrides {
    client-discover-match <option60-and-option82>;
    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 dhcpv6],
[edit logical-systems logical-system-name system services dhcp-local-server],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6],
[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6]
```

**Release Information** Statement introduced in Junos OS Release 9.0.

<b>Description</b>	Configure a group of interfaces that have a common configuration, such as authentication parameters. A group must contain at least one interface.
<b>Options</b>	<p><i>group-name</i>—Name of the group.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Extended DHCP Local Server Overview on page 98</li><li>• Grouping Interfaces with Common DHCP Configurations on page 112</li><li>• Using External AAA Authentication Services with DHCP on page 110</li><li>• Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125</li></ul>

## group (DHCP Relay Agent)

```
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 (merge | replace) | use-primary
        primary-profile-name>;
    overrides {
        allow-snooped-clients;
        always-write-giaddr;
        always-write-option-82;
        client-discover-match <option60-and-option82>;
        disable-relay;
        interface-client-limit number;
        layer2-unicast-replies;
        no-allow-snooped-clients;
        no-arp;
        proxy-mode;
        replace-ip-source-with;
        send-release-on-delete;
        trust-option-82;
    }
    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 prefix;
            use-interface-description (logical | device);
        }
    }
    interface interface-name {
```

```
exclude;  
overrides {  
  ...  
}  
trace;  
upto upto-interface-name;  
}  
}
```

**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 OS 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 Documentation**

- Extended DHCP Relay Agent Overview on page 154
- Grouping Interfaces with Common DHCP Configurations on page 112
- Using External AAA Authentication Services with DHCP on page 110
- Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125



## group (Dynamic IGMP Interface)

**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],

**Release Information** Statement introduced in Junos OS 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 Documentation**

- Configuring a Dynamic Profile for Client Access on page 395
- For information about configuring static group membership, see “Enabling IGMP Static Group Membership” in the *Junos OS Multicast Protocols Configuration Guide*

## group (Dynamic MLD Interface)

---

**Syntax**    `group multicast-group-address {  
              exclude;  
              group-count number;  
              group-increment increment;  
              source ip-address {  
                    source-count number;  
                    source-increment increment;  
              }  
              }  
              }`

**Hierarchy Level**    [edit dynamic-profiles *profile-name* protocols mld interface *interface-name* static]

**Release Information**    Statement introduced in Junos OS Release 10.1.

**Description**    The MLD multicast group address and (optionally) the source address for the multicast group being dynamically configured on an interface.

**Options**    *multicast-group-address*—Address of the group.



.....  
**NOTE:** You must specify a unique address for each group.  
.....

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 Documentation**    • Enabling MLD Static Group Membership

## group (Static Subscribers)

**Syntax**

```
group group-name {
  access-profile profile-name;
  dynamic-profile profile-name {
    aggregate-clients (merge | replace);
  }
  authentication {
    password password-string;
    username-include {
      domain-name domain-name;
      interface;
      logical-system-name;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  interface interface-name <exclude> <upto upto-interface-name>;
}
```

**Hierarchy Level** [edit logical-systems *logical-system-name* system services **static-subscribers**],  
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system  
services **static-subscribers**],  
[edit routing-instances *routing-instances-name* system services **static-subscribers**],  
[edit system services **static-subscribers**]

**Release Information** Statement introduced in Junos OS Release 9.6.

**Description** Configure a static subscriber group with values that override the values configured at the [edit system services **static-subscribers**] hierarchy level for subscribers outside the group. Includes the subscriber access and dynamic profiles, the authentication parameters that trigger the Access-Request message to AAA for static subscribers in the group, and the statically configured interfaces that form the group.



**NOTE:** The logical system and routing instance in which the group is configured must match the logical system and routing instance where the static interfaces are configured.

**Options** *group-name*—Name of a group that defines authentication parameters for static subscribers to override the global authentication 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 Documentation**

- Configuring Subscribers over Static Interfaces on page 288
- Creating a Static Subscriber Group on page 292

## group-count (Dynamic MLD Interface)

---

<b>Syntax</b>	<code>group-count <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols mld interface <i>interface-name</i> static group <i>multicast-group-address</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Configure the number of static groups to be created over the dynamic interface.
<b>Options</b>	<i>number</i> —Number of static groups. <b>Default:</b> 1 <b>Range:</b> 1 through 512
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Enabling MLD Static Group Membership</li></ul>

## group-increment (Dynamic MLD Interface)

---

<b>Syntax</b>	<code>group-increment <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols mld interface <i>interface-name</i> static group <i>multicast-group-address</i> source]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Configure the number of times the address should be incremented for each static group created on a dynamic interface. The increment is specified in a format similar to an IPv6 address.
<b>Options</b>	<i>increment</i> —Number of times the address should be incremented. <b>Default:</b> ::1 <b>Range:</b> ::1 through ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff;
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Enabling MLD Static Group Membership</li></ul>

## group-limit (Dynamic IGMP Interface)

<b>Syntax</b>	<code>group-limit <i>policy-name</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i> ],
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Configure a limit for the number of multicast groups (or [S,G] channels in IGMPv3) allowed on a dynamic logical interface. After this limit is reached, new reports will be ignored and all related flows are not flooded on the logical interface.
<b>Default</b>	By default, there is no limit to the number of multicast groups that can join the interface.
<b>Options</b>	<i>limit</i> —group limit value for the interface. <b>Range:</b> 1 through 32767
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring a Dynamic Profile for Client Access on page 395</li> <li>For information about limiting the number of multicast group joins for an IGMP logical interface, see “Limiting the Number of IGMP Multicast Group Joins on Logical Interfaces” in the <i>Junos OS Multicast Protocols Configuration Guide</i></li> </ul>

## group-limit (Dynamic MLD Interface)

---

<b>Syntax</b>	<code>group-limit <i>limit</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols mld interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Configure a limit for the number of multicast groups (or [S,G] channels in MLDv2) allowed on a dynamic logical interface. After this limit is reached, new reports will be ignored and all related flows are not flooded on the logical interface.
<b>Default</b>	By default, there is no limit to the number of multicast groups that can join the interface.
<b>Options</b>	<i>limit</i> —group limit value for the interface. <b>Range:</b> 1 through 32767
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring a Dynamic Profile for Client Access on page 395</li><li>• For information about limiting the number of multicast group joins for an MLD logical interface, see “Configuring the Number of MLD Multicast Group Joins on Logical Interfaces” in the <a href="#">Junos OS Multicast Protocols Configuration Guide</a></li></ul>

## group-policy (Dynamic IGMP Interface)

<b>Syntax</b>	<code>group-policy <i>policy-name</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols <b>igmp</b> interface <i>interface-name</i> ],
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	<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>
<b>Options</b>	<i>policy-name</i> —Name of the group policy.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring a Dynamic Profile for Client Access on page 395</li> <li>For information about rejecting unwanted reports for an IGMP interface, see “Filtering Unwanted IGMP Reports at the IGMP Interface Level” in the <i>Junos OS Multicast Protocols Configuration Guide</i></li> </ul>

## group-policy (Dynamic MLD Interface)

<b>Syntax</b>	<code>group-policy <i>policy-name</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols <b>mld</b> interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	<p>When this statement is enabled on a router running MLD version 1 (MLDv1), after the router receives an MLD report, the router compares 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 MLD version 2 (MLDv2), after the router receives an MLD report, the router compares the group against the specified group policy and performs the action configured in that policy (for example, rejects the report).</p>
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Filtering Unwanted MLD Reports at the MLD Interface Level</li> </ul>

## guaranteed-rate (Dynamic Traffic Shaping)

---

<b>Syntax</b>	<code>guaranteed-rate (rate   \$junos-cos-guaranteed-rate);</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. The <b>\$junos-cos-guaranteed-rate</b> variable introduced in Junos OS Release 9.4.
<b>Description</b>	Configure a guaranteed minimum rate for a logical interface.
<b>Default</b>	If you do not include this statement and you do not include the <b>delay-buffer-rate</b> statement, the logical interface receives a minimal delay-buffer rate and minimal bandwidth equal to 2 MTU-sized packets.
<b>Options</b>	<b>rate</b> —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 <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000). <b>Range:</b> 1000 through 160,000,000,000 bps  <b>\$junos-cos-guaranteed-rate</b> —Junos predefined variable that is replaced with the guaranteed rate obtained from the RADIUS server when a subscriber authenticates over the interface to which the dynamic profile is attached.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>Configuring Traffic Scheduling and Shaping for Subscriber Access on page 677</li><li><b>output-traffic-control-profile</b> on page 1092</li></ul>



## gx-plus (Gx-Plus)

<b>Syntax</b>	<pre> gx-plus {   global {     max-outstanding-requests <i>number</i>;   }   partition <i>partition-name</i> {     diameter-instance <i>instance-name</i>;     destination-host <i>hostname</i>;     destination-realm <i>realm</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit access]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	<p>Configure the Gx-Plus application to interact with a PCRF to authorize and provision subscribers.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Gx-Plus on page 339</li> </ul>

## hardware-address

<b>Syntax</b>	<code>hardware-address <i>mac-address</i>;</code>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family (inet   inet6) host <i>hostname</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Specify the MAC address of the client. This is the hardware address that identifies the client on the network.
<b>Options</b>	<i>mac-address</i> —MAC address of the client.
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Address-Assignment Pools on page 68</li> </ul>

## highUtilization (Address-Assignment Pools)

---

<b>Syntax</b>	<code>highUtilization <i>percentage</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access address-assignment]</code> <code>[edit routing-instances <i>routing-instance-name</i> address-assignment]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Generate an SNMP trap when the DHCP address pool or linked set of address pools use surpasses the specified percentage.
<b>Default</b>	High utilization is not set. Delete the highUtilization value to unset.
<b>Options</b>	<b><i>percentage</i></b> —Percentage used to generate a trap. <b>Range:</b> 2 through 99
<b>Required Privilege Level</b>	<code>admin</code> —To view this statement in the configuration. <code>admin-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Address-Assignment Pools Overview on page 67</li><li>Configuring Address-Assignment Pool Usage Threshold Traps on page 71</li></ul>

## highUtilization-v6 (Address-Assignment Pools)

---

<b>Syntax</b>	<code>highUtilization-v6 <i>percentage</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access address-assignment]</code> <code>[edit routing-instances <i>routing-instance-name</i> address-assignment]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Generate an SNMP trap when the DHCPv6 address pool or linked set of address pools use surpasses the specified percentage.
<b>Default</b>	High utilization is not set. Delete the highUtilization value to unset.
<b>Options</b>	<b><i>percentage</i></b> —Percentage used to generate a trap. <b>Range:</b> 2 through 99
<b>Required Privilege Level</b>	<code>admin</code> —To view this statement in the configuration. <code>admin-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Address-Assignment Pools Overview on page 67</li><li>Configuring Address-Assignment Pool Usage Threshold Traps on page 71</li></ul>

## home-agent (Mobile IP Dynamic Assignment)

<b>Syntax</b>	<pre>home-agent {   nai (name@domain   @domain) {     home-agent ip-address;   } }</pre>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip dynamic-home-assignment],          [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services          mobile-ip dynamic-home-assignment],          [edit routing-instances <i>routing-instances-name</i> services mobile-ip          dynamic-home-assignment],          [edit services mobile-ip dynamic-home-assignment]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3.          Support at the [edit logical-systems <i>logical-system-name</i> services mobile-ip          dynamic-home-assignment], [edit logical-systems <i>logical-system-name</i> routing-instances  <i>routing-instances-name</i> services mobile-ip dynamic-home-assignment], and [edit          routing-instances <i>routing-instances-name</i> services mobile-ip dynamic-home-assignment]          hierarchy levels introduced in Junos OS Release 9.5.</p>
<b>Description</b>	<p>Configure the IP address to which registration requests are sent as part of the home          agent's dynamic assignment rule.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.          system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Mobile IP on page 357</li> <li>Configuring Dynamic Home Assignment for the Mobile Node on page 360</li> </ul>

## home-agent (Mobile IP Network Address Identifier)

---

<b>Syntax</b>	home-agent <i>ip-address</i> ;
<b>Hierarchy Level</b>	[edit services mobile-ip dynamic-home-assignment home-agent nai <i>name@domain</i> ], [edit logical-systems <i>logical-system-name</i> services mobile-ip dynamic-home-assignment home-agent nai <i>name@domain</i> ], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> services mobile-ip dynamic-home-assignment home-agent nai <i>name@domain</i> ], [edit routing-instances <i>routing-instance-name</i> services mobile-ip dynamic-home-assignment home-agent nai <i>name@domain</i> ], [edit services mobile-ip dynamic-home-assignment home-agent nai <i>@domain</i> ], [edit logical-systems <i>logical-system-name</i> services mobile-ip dynamic-home-assignment home-agent nai <i>@domain</i> ], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> services mobile-ip dynamic-home-assignment home-agent nai <i>@domain</i> ], [edit routing-instances <i>routing-instance-name</i> services mobile-ip dynamic-home-assignment home-agent nai <i>@domain</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure the IP address to which registration requests are sent as part of the home agent's dynamic assignment rule.
<b>Options</b>	<i>ip-address</i> —IP address of the home agent
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Mobile IP on page 357</li><li>Configuring Dynamic Home Assignment for the Mobile Node on page 360</li></ul>

## home-agent (Mobile IP Networks)

<b>Syntax</b>	<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>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> services <b>mobile-ip</b>],  [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services <b>mobile-ip</b>],  [edit routing-instances <i>routing-instances-name</i> services <b>mobile-ip</b>],  [edit services <b>mobile-ip</b>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit logical-systems <i>logical-system-name</i> services <b>mobile-ip</b>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services <b>mobile-ip</b>], and [edit routing-instances <i>routing-instances-name</i> services <b>mobile-ip</b>] hierarchy levels introduced in Junos OS Release 9.5.</p>
<b>Description</b>	<p>Define the virtual networks and non-virtual networks for the Mobile IP home agent.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Mobile IP on page 357</li> </ul>

## home-agent-address

---

<b>Syntax</b>	<code>home-agent-address <i>ip-address</i> {     registration-lifetime <i>seconds</i>;     revocation-required;     timestamp-tolerance <i>seconds</i>; }</code>
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> services mobile-ip home-agent virtual-network], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network], [edit routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network], [edit services mobile-ip home-agent virtual-network]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> services mobile-ip home-agent virtual-network], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network], and [edit routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network] hierarchy levels introduced in Junos OS Release 9.5.
<b>Description</b>	Defines addressing for the virtual network of the Mobile IP home agent.
<b>Options</b>	<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.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Mobile IP on page 357</li><li>• Configuring the Mobile IP Home Agent on page 358</li></ul>

## host (Address-Assignment Pools)

<b>Syntax</b>	<pre>host <i>hostname</i> {     hardware-address <i>mac-address</i>;     ip-address <i>ip-address</i>; }</pre>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family (inet   inet6)]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Configure a static binding for the specified client.
<b>Options</b>	<p><b><i>hostname</i></b>—Name of the client.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Address-Assignment Pools Overview on page 67</li> <li>Configuring Address-Assignment Pools on page 68</li> </ul>

## host (Diameter Origin)

<b>Syntax</b>	host <i>hostname</i> ;
<b>Hierarchy Level</b>	[edit diameter origin]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify the name of the host that originates the Diameter message.
<b>Options</b>	<p><b><i>hostname</i></b>—Name of the message origin host. Supplied as the value of Origin-Host AVP for all messages sent by the Diameter master instance.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Diameter on page 259</li> <li>Configuring the Origin Attributes of the Diameter Instance on page 260</li> </ul>

## identification (Tunnel Profile)

---

<b>Syntax</b>	<code>identification name;</code>
<b>Hierarchy Level</b>	<code>[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the assignment ID of an L2TP tunnel. L2TP sessions with the same tunnel assignment identification and destination are grouped into the same tunnel.
<b>Options</b>	<b>name</b> —Tunnel assignment ID; string of up to 32 alphanumeric characters.
<b>Required Privilege Level</b>	<b>admin</b> —To view this statement in the configuration. <b>admin-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Tunnel Profile for Subscriber Access on page 242</li></ul>

## ieee-802.1 (Dynamic Classifiers)

---

<b>Syntax</b>	<code>ieee-802.1 (<i>classifier-name</i>   default) vlan-tag (inner   outer);</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> classifiers]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Apply an IEEE-802.1 classifier to a subscriber interface in a dynamic profile.
<b>Options</b>	<b>classifier-name</b> —Name of a <b>classifier</b> mapping configured at the <code>[edit class-of-service classifier ieee-802.1]</code> hierarchy level.  <b>default</b> —The default mapping.  The remaining statement is explained separately.
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>Applying a Classifier to a Subscriber Interface in a Dynamic Profile on page 687</li><li>classifiers (Definition)</li></ul>



## ieee-802.1 (Dynamic Rewrite Rules)

<b>Syntax</b>	ieee-802.1 ( <i>rewrite-name</i>   default) vlan-tag (outer   outer-and-inner);
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> rewrite-rules]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Apply an IEEE-802.1 rewrite rule to a subscriber interface in a dynamic profile.
<b>Options</b>	<p><b>rewrite-name</b>—Name of a <b>rewrite-rules</b> mapping configured at the [edit class-of-service <b>rewrite-rules</b> <b>ieee-802.1</b>] hierarchy level.</p> <p><b>default</b>—The default mapping.</p> <p>The remaining statement is explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li> <li>Applying a Rewrite Rule Definition to a Subscriber Interface in a Dynamic Profile on page 686</li> <li>rewrite-rules</li> </ul>

## ietf-mode

<b>Syntax</b>	pre-ietf-mode
<b>Hierarchy Level</b>	[edit protocols ancp neighbor]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Configure ANCP to run in a mode that is not backward compatible with Internet draft draft-ietf-ancp-protocol-00.txt, <i>Protocol for Access Node Control Mechanism in Broadband Networks</i> . Include this statement when pre-ietf mode has been configured globally for ANCP, but you want one or more neighbors to run ANCP in the default mode.
<b>Default</b>	ANCP does not run in a backward-compatible mode.
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring ANCP on page 786</li> <li>Configuring ANCP Neighbors on page 786</li> </ul>

## igmp (Dynamic Profiles)

---

<b>Syntax</b>	<pre>igmp {   interface <i>interface-name</i> {     accounting;     disable;     group-limit <i>policy-name</i>;     group-policy;     immediate-leave;     no-accounting;     oif-map;     passive &lt;allow-receive&gt; &lt;send-general-query&gt; &lt;send-group-query&gt;;     promiscuous-mode;     ssm-map <i>ssm-map-name</i>;     static {       group <i>group</i> {         source <i>source</i>;       }     }     version <i>version</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols], [edit logical-systems <i>logical-system-name</i> protocols], [edit protocols]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Enable IGMP on the router. IGMP must be enabled for the router to receive multicast packets.
<b>Default</b>	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).
<b>Options</b>	The statements are explained separately.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Dynamic Profile for Client Access on page 395</li><li>For general information about configuring IGMP, see the <a href="#">Junos OS Multicast Protocols Configuration Guide</a></li><li>For information about enabling IGMP, see “Enabling IGMP” in the <a href="#">Junos OS Multicast Protocols Configuration Guide</a></li></ul>


## ignore

---


<b>Syntax</b>	<pre>ignore {     framed-ip-netmask;     input-filter;     logical-system-routing-instance;     output-filter; }</pre>
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> radius attributes]
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p>
<b>Description</b>	Configure the router or switch to ignore the specified attributes in RADIUS Access-Accept messages. By default, the router or switch processes the attributes it receives from the external server.
<b>Options</b>	<p><b>framed-ip-netmask</b>—Ignore Framed-IP-Netmask (RADIUS attribute 9).</p> <p><b>input-filter</b>—Ignore Ingress-Policy-Name (VSA 26-10).</p> <p><b>logical-system-routing-instance</b>—Ignore Virtual-Router (VSA 26-1).</p> <p><b>output-filter</b>—Ignore Egress-Policy-Name (VSA 26-11).</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring RADIUS Server Parameters for Subscriber Access on page 26</li> </ul>

## immediate-leave (Dynamic IGMP Interface)

---

<b>Syntax</b>	immediate-leave;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i> ],
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	<p>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.</p> <p>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.</p>
	<div><p><b>NOTE:</b> 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.</p></div>
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Dynamic Profile for Client Access on page 395</li><li>For information about configuring IGMP immediate leave, see “Specifying Immediate-Leave Host Removal” in the <a href="#">Junos OS Multicast Protocols Configuration Guide</a></li></ul>

## immediate-leave (Dynamic MLD Interface)

<b>Syntax</b>	immediate-leave;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols mld interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	<p>When this statement is enabled on a router running MLDv1, after the router receives a multicast listener done message from a host associated with the interface, the router immediately removes the group membership from the interface and suppresses the sending of any group-specific queries for the multicast group.</p> <p>When this statement is enabled on a router running MLDv2, after the router receives a report with the type BLOCK_OLD_SOURCES, the router suppresses the sending of group-and-source queries but relies on the Junos-supported host tracking mechanism to determine whether or not it removes a particular source group membership from the interface.</p>
	<div>  <p><b>NOTE:</b> Use this statement only on MLD interfaces to which one MLD host is connected. If more than one MLD 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 properly remain in the multicast group until they send join requests in response to the router's next general multicast listener query.</p> </div>
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Specifying Immediate-Leave Host Removal for MLD</li> </ul>

## immediate-update

---

<b>Syntax</b>	<code>immediate-update;</code>
<b>Hierarchy Level</b>	<code>[edit access profile <i>profile-name</i> accounting]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
<b>Description</b>	Configure the router or switch 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.
<b>Required Privilege Level</b>	<code>admin</code> —To view this statement in the configuration. <code>admin-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring RADIUS Server Parameters for Subscriber Access on page 26</li><li>Configuring Per-Subscriber Session Accounting on page 24</li></ul>

## inet-precedence (Dynamic Classifiers)

---

<b>Syntax</b>	<code>inet-precedence (<i>classifier-name</i>   default);</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> classifiers]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Apply a IPv4 precedence classifier to a subscriber interface in a dynamic profile.
<b>Options</b>	<b><i>classifier-name</i></b> —Name of a <b>classifier</b> mapping configured at the <code>[edit class-of-service classifier <b>ieee-802.1</b>]</code> hierarchy level.  <b>default</b> —The default mapping.
<b>Required Privilege Level</b>	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>Applying a Classifier to a Subscriber Interface in a Dynamic Profile on page 687</li><li>classifiers (Definition)</li></ul>

## inet-precedence (Dynamic Rewrite Rules)

<b>Syntax</b>	<code>inet-precedence (rewrite-name   default);</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles profile-name class-of-service interfaces interface-name unit logical-unit-number rewrite-rules]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Apply a IPv4 precedence rewrite rule.
<b>Options</b>	<p><b>rewrite-name</b>—Name of a <b>rewrite-rules</b> mapping configured at the <code>[edit class-of-service rewrite-rules inet-precedence]</code> hierarchy level.</p> <p><b>default</b>—The default mapping. By default, IP precedence rewrite rules alter the first three bits on the type of service (ToS) byte while leaving the last three bits unchanged.</p>
<b>Required Privilege Level</b>	<p><b>interface</b>—To view this statement in the configuration.</p> <p><b>interface-control</b>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li> <li>Applying a Rewrite Rule Definition to a Subscriber Interface in a Dynamic Profile on page 686</li> <li>rewrite-rules</li> </ul>

## inner-tag-protocol-id (Dynamic VLANs)

<b>Syntax</b>	<code>inner-tag-protocol-id tpid;</code>
<b>Hierarchy Level</b>	<p><code>[edit dynamic-profiles profile-name interfaces interface-name unit logical-unit-number input-vlan-map]</code></p> <p><code>[edit dynamic-profiles profile-name interfaces interface-name unit logical-unit-number output-vlan-map]</code></p>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	For dynamic VLAN interfaces, configure the IEEE 802.1Q TPID value to rewrite for the inner tag. All TPIDs you include in input and output VLAN maps must be among those you specify at the <code>[edit interfaces interface-name gigether-options ethernet-switch-profile tag-protocol-id tpids ]</code> hierarchy level.
<b>Default</b>	If the <b>inner-tag-protocol-id</b> statement is not configured, the TPID value is 0x8100.
<b>Required Privilege Level</b>	<p><b>interface</b>—To view this statement in the configuration.</p> <p><b>interface-control</b>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Inner and Outer TPIDs and VLAN IDs</li> </ul>

## inner-vlan-id (Dynamic VLANs)

---

<b>Syntax</b>	<code>inner-vlan-id <i>number</i>;</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map]</code> <code>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	<p>For dynamic VLAN interfaces, specify the VLAN ID to rewrite for the inner tag of the final packet.</p> <p>You cannot include the <b>inner-vlan-id</b> statement with the <b>swap</b> statement, <b>swap-push</b> statement, <b>push-push</b> statement, or <b>push-swap</b> statement and the <b>inner-vlan-id</b> statement at the <code>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]</code> hierarchy level. If you include any of those statements in the output VLAN map, the VLAN ID in the outgoing frame is rewritten to the <b>inner-vlan-id</b> statement you include at the <code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</code> hierarchy level.</p>
<b>Options</b>	<p><i>number</i>—VLAN ID number.</p> <p><b>Range:</b> 0 through 4094</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Inner and Outer TPIDs and VLAN IDs</li></ul>



## input (Dynamic Service Sets)

<b>Syntax</b>	<pre>input {   service-set <i>service-set-name</i> {     service-filter <i>filter-name</i>;   }   post-service-filter <i>filter-name</i>; }</pre>
<b>Hierarchy Level</b>	<p>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> service],</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i> service]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.5.</p> <p>Support at the [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i> service] hierarchy level introduced in Junos OS Release 10.1.</p>
<b>Description</b>	<p>Define the input service sets and filters to be applied to traffic by a dynamic profile. Only the Internet Protocol version 4 (IPv4) protocol family is currently supported for dynamic PPPoE logical interfaces.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Dynamic Service Sets Overview on page 569</li> <li>Associating Service Sets with Interfaces in a Dynamic Profile on page 595</li> </ul>

## input-vlan-map (Dynamic Interfaces)

---

<b>Syntax</b>	<pre>input-vlan-map {     inner-tag-protocol-id <i>tpid</i>;     inner-vlan-id <i>number</i>;     (push   swap);     tag-protocol-id <i>tpid</i>;     vlan-id <i>number</i>; }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	<p>For dynamic interfaces, define the rewrite profile to be applied to incoming frames on this logical interface.</p> <p>The statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution</li></ul>

## interface (DHCP Local Server)

**Syntax** interface *interface-name* {  
 exclude;  
 overrides {  
 client-discover-match <option60-and-option82>;  
 interface-client-limit *number*;  
 no-arp;  
 }  
 trace;  
 upto *upto-interface-name*;  
 }

**Hierarchy Level** [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* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name*],  
 [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name*],  
 [edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name*],  
 [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name*],  
 [edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name*],  
 [edit system services dhcp-local-server group *group-name*],  
 [edit system services dhcp-local-server dhcpv6 group *group-name*]

**Release Information** Statement introduced in Junos OS Release 9.0.  
 Options **upto** and **exclude** introduced in Junos OS 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 *interface-name*** 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.



**NOTE:** DHCP values are supported in Integrated Routing and Bridging (IRB) configurations. When you configure an IRB interface in a network that is using DHCP, the DHCP information (for example, authentication, address assignment, and so on) is propagated in the associated bridge domain. This enables the DHCP server to configure client IP addresses residing within the bridge domain. IRB currently only supports static DHCP configurations. For additional information about how to configure IRB, see the [Junos OS MX Series 3D Universal Edge Routers Solutions Guide](#).

**Options** **exclude**—Exclude an interface or a range of interfaces from the group. This option and the **overrides** option are mutually exclusive.

***interface-name***—Name of the interface. You can repeat this option multiple times.

***upto-interface-name***—Upper end of the range of interfaces; the lower end of the range is the *interface-name* entry. The interface device name of the ***upto-interface-name*** must be the same as the device name of the ***interface-name***.

The remaining statements are explained separately.

<b>Required Privilege</b>	system—To view this statement in the configuration.
<b>Level</b>	system-control—To add this statement to the configuration.

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Extended DHCP Local Server Overview on page 98</li><li>• Grouping Interfaces with Common DHCP Configurations on page 112</li><li>• Using External AAA Authentication Services with DHCP on page 110</li></ul>
------------------------------	---

## interface (DHCP Relay Agent)

<b>Syntax</b>	<pre> interface <i>interface-name</i> {   exclude;   overrides {     allow-snooped-clients;     always-write-giaddr;     always-write-option-82;     client-discover-match &lt;option60-and-option82&gt;;     disable-relay;     interface-client-limit <i>number</i>;     layer2-unicast-replies;     no-allow-snooped-clients;     no-arp;     proxy-mode;     replace-ip-source-with;     send-release-on-delete;     trust-option-82;   }   trace;   upto <i>upto-interface-name</i>; } </pre>
<b>Hierarchy Level</b>	<pre> [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>] </pre>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Options <b>upto</b> and <b>exclude</b> introduced in Junos OS Release 9.1.</p>
<b>Description</b>	<p>Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP relay agent is enabled. You can repeat the <b>interface <i>interface-name</i></b> 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 local server.</p>



**NOTE:** DHCP values are supported in Integrated Routing and Bridging (IRB) configurations. When you configure an IRB interface in a network that is using DHCP, the DHCP information (for example, authentication, address assignment, and so on) is propagated in the associated bridge domain. This enables the DHCP server to configure client IP addresses residing within the bridge domain. IRB currently only supports static DHCP configurations. For additional information about how to configure IRB, see the [Junos OS MX Series 3D Universal Edge Routers Solutions Guide](#).

**Options**    **exclude**—Exclude an interface or a range of interfaces from the group. This option and the **overrides** option are mutually exclusive.

**interface-name**—Name of the interface. You can repeat this option multiple times.

**overrides**—Override the specified default configuration settings for the interface. The **overrides** statement is described separately.

**upto-interface-name**—Upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the **upto-interface-name** must be the same as the device name of the **interface-name**.

The remaining statements are explained separately.

**Required Privilege**    interface—To view this statement in the configuration.

**Level**                interface-control—To add this statement to the configuration.

**Related  
Documentation**

- Extended DHCP Relay Agent Overview on page 154
- Grouping Interfaces with Common DHCP Configurations on page 112
- Using External AAA Authentication Services with DHCP on page 110

## interface (Dynamic IGMP)

<b>Syntax</b>	<pre> interface <i>interface-name</i> {     accounting;     disable;     group-policy;     immediate-leave     no-accounting;     oif-map;     passive;     promiscuous-mode;     ssm-map <i>ssm-map-name</i>;     static {         group <i>group</i> {             source <i>source</i>;         }     }     version <i>version</i>; } </pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols igmp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Enable IGMP on an interface and configure interface-specific properties.
<b>Options</b>	<p><b><i>interface-name</i></b>—Variable for the interface. Specify the interface variable (\$junos-interface-name) to indicate that the dynamic profile chooses an interface for the accessing DHCP client.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring a Dynamic Profile for Client Access on page 395</li> <li>For information about configuring IGMP interfaces, see “Enabling IGMP” in the <a href="#">Junos OS Multicast Protocols Configuration Guide</a></li> </ul>

## interface (Dynamic Interface Sets)

---

<b>Syntax</b>	<code>interface <i>interface-name</i> {     unit <i>logical-unit-number</i>; }</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> interfaces interface-set <i>interface-set-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Add a subscriber interface to a dynamic interface set.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>Configuring an Interface Set of Subscribers in a Dynamic Profile on page 712</li></ul>



## interface (Dynamic MLD)

<b>Syntax</b>	<pre> interface <i>interface-name</i> {     disable;     (accounting   no-accounting);     group-policy;     immediate-leave;     oif-map;     passive;     ssm-map <i>ssm-map-name</i>;     static {         group <i>mcast-group-address</i> {             exclude;             group-count <i>number</i>;             group-increment <i>increment</i>;             source <i>ip-address</i> {                 source-count <i>number</i>;                 source-increment <i>increment</i>;             }         }     }     version <i>version</i>; } </pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols mld]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Enable MLD on a dynamic interface and configure interface-specific properties.
<b>Options</b>	<p><b><i>interface-name</i></b>—Variable for the interface. Specify the interface variable (\$junos-interface-name) to indicate that the dynamic profile chooses an interface for the accessing client.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Enabling MLD</li> </ul>

## interface (Dynamic Profiles)

---

<b>Syntax</b>	<code>interface <i>interface-name</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> routing-instances <i>routing-instance-name</i> ] [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> ], [edit routing-instances <i>routing-instance-name</i> ]
<b>Release Information</b>	Statement introduced prior to Junos OS Release 7.4. [edit dynamic-profiles <i>profile-name</i> routing-instances <i>routing-instance-name</i> ] support introduced in Junos OS Release 9.6.
<b>Description</b>	Assign the specified interface to the current routing instance. When used in the [edit dynamic-profiles <i>profile-name</i> routing-instances <i>routing-instance-name</i> ] hierarchy, specify the <i>\$junos-routing-instance</i> predefined variable.
<b>Options</b>	<i>interface-name</i> —Name of the interface.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Routing Instances</li></ul>

## interface (Dynamic Router Advertisement)

**Syntax**    `interface interface-name {  
                   current-hop-limit number;  
                   default-lifetime seconds;  
                   (managed-configuration | no-managed-configuration);  
                   max-advertisement-interval seconds;  
                   min-advertisement-interval seconds;  
                   (other-stateful-configuration | no-other-stateful-configuration);  
                   prefix prefix {  
                       (autonomous | no-autonomous);  
                       (on-link | no-on-link);  
                       preferred-lifetime seconds;  
                       valid-lifetime seconds;  
                   }  
                   reachable-time milliseconds;  
                   retransmit-timer milliseconds;  
                   }`

**Hierarchy Level**    [edit dynamic-profiles protocols router-advertisement]

**Release Information**    Statement introduced in Junos OS Release 10.1.

**Description**    Dynamically configure router advertisement properties on an interface. To dynamically configure interface properties, include the *\$junos-interface-name* dynamic variable for the interface name.

**Options**    *interface-name*—Name of an interface. Specify the *\$junos-interface-name* dynamic variable or the full, static interface name, including the physical and logical address components.



**NOTE:** Even though you can specify the static interface name when defining the interface, we recommend using dynamic variable when configuring this statement.

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 Documentation**    • Configuring an Interface to Send Neighbor Discovery Advertisements

## interface (Dynamic Routing Options)

---

<b>Syntax</b>	<code>interface <i>interface-names</i> {     no-qos-adjust; }</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> routing-options multicast], [edit dynamic-profiles <i>profile-name</i> routing-instances <i>routing-instance-name</i> routing-options multicast]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Define the maximum bandwidth for a dynamic interface on which you want to apply bandwidth management.
<b>Options</b>	<b><i>interface-name</i></b> —Names of the physical or logical interface. For details about specifying interfaces, see the <a href="#">Junos OS Network Interfaces Configuration Guide</a> .  The remaining statements are explained separately.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

## interface (Static Subscriber Group)

<b>Syntax</b>	<code>interface <i>interface-name</i> &lt;exclude&gt; &lt;upto <i>upto-interface-name</i>&gt;;</code>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i>],</p> <p>[edit system services static-subscribers group <i>group-name</i>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.6.</p> <p>Support for IPv6 and IPv4 demux static interfaces introduced in Junos OS Release 11.2.</p>
<b>Description</b>	Specify one or more interfaces, or a range of interfaces, that are within a specified group on which static subscribers are created. You can repeat the <b>interface <i>interface-name</i></b> statement to specify multiple interfaces within a group. You must configure each interface in only one group.
<div>  <p><b>NOTE:</b> The logical system and routing instance in which the static interfaces are configured must match the logical system and routing instance where the group is configured.</p> </div>	
<b>Options</b>	<p><b>exclude</b>—(Optional) Exclude an interface or a range of interfaces from the group.</p> <p><b><i>interface-name</i></b>—Name of the interface on which static subscribers are created. If you do not specify a unit number for the interface, then .0 is assumed. For example, <b>ge-0/1/0</b> is interpreted as <b>ge-0/1/0.0</b>.</p> <p><b><i>upto-interface-name</i></b>—(Optional) The upper end of the range of interfaces; the lower end of the range is the <i>interface-name</i> entry. The interface device name of <i>upto-interface-name</i> must be the same as the device name of <i>interface-name</i>.</p>
<b>Required Privilege Level</b>	<p><b>interface</b>—To view this statement in the configuration.</p> <p><b>interface-control</b>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Subscribers over Static Interfaces on page 288</li> <li>Creating a Static Subscriber Group on page 292</li> </ul>

## interface (Static Subscriber Username)

---

<b>Syntax</b>	interface;
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i> authentication <b>username-include</b>],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers authentication <b>username-include</b>],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication <b>username-include</b>],</p> <p>[edit system services static-subscribers authentication <b>username-include</b>],</p> <p>[edit system services static-subscribers group <i>group-name</i> authentication <b>username-include</b>]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify that a modified version of the interface name is included as part of the username created for all static subscribers or for the static subscribers in a specified group. The group version of the statement takes precedence over the global version. The username is also sent to RADIUS in the Access-Request message. The interface name is modified by replacing the "/" character with the "-" character. For example, ge-0/1/2.50 is converted to ge-0-1-2.50.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Subscribers over Static Interfaces on page 288</li><li>• Configuring the Static Subscriber Global Username on page 291</li><li>• Configuring the Static Subscriber Group Username on page 295</li></ul>

## interface-client-limit (DHCP Local Server)

<b>Syntax</b>	<code>interface-client-limit <i>number</i>;</code>
<b>Hierarchy Level</b>	<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 dhcpv6 overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 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 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 dhcpv6 overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> 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 dhcpv6 overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 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 dhcpv6 overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> 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 dhcpv6 overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group interface <i>interface-name</i> <i>group-name</i> overrides],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Set 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.
<b>Default</b>	No limit
<b>Options</b>	<p><i>number</i>—Maximum number of clients allowed.</p> <p><b>Range:</b> 1 through 500,000</p>

<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Extended DHCP Local Server Overview on page 98</li><li>Overriding Default DHCP Local Server Configuration Settings on page 115</li></ul>

---

## interface-client-limit (DHCP Relay Agent)

---

<b>Syntax</b>	interface-client-limit <i>number</i> ;
<b>Hierarchy Level</b>	[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], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Set 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.
<b>Default</b>	No limit
<b>Options</b>	<i>number</i> —Maximum number of clients allowed. <b>Range:</b> 1 through 500,000
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Extended DHCP Relay Agent Overview on page 154</li><li>Overriding the Default DHCP Relay Configuration Settings on page 168</li></ul>



## interface-delete (Subscriber Management)

<b>Syntax</b>	interface-delete;
<b>Hierarchy Level</b>	[edit system services subscriber-management maintain-subscriber]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1.
<b>Description</b>	Configure the router to maintain, rather than log out, subscribers when the subscriber interface is deleted. By default, the router logs out subscribers when the subscriber interface is deleted.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 124</li> </ul>

## interface-description-format

<b>Syntax</b>	interface-description-format { exclude-adapter; exclude-sub-interface; }
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> radius options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches. Options <b>exclude-adapter</b> and <b>exclude-sub-interface</b> introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the information that is excluded from the interface description that the device passes to RADIUS for inclusion in the RADIUS attribute 87 (NAS-Port-Id). By default, the device includes both the subinterface and the adapter in the interface description.
<b>Options</b>	<b>exclude-adapter</b> —Exclude the adapter from the interface description.  <b>exclude-sub-interface</b> —Exclude the subinterface from the interface description.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring RADIUS Server Options for Subscriber Access on page 29</li> <li>RADIUS Server Options for Subscriber Access on page 28</li> </ul>

## interface-set (Dynamic CoS)

---

<b>Syntax</b>	<pre>interface-set <i>interface-set-name</i> {     interface <i>interface-name</i> {         unit <i>logical-unit-number</i>;     } }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	For MX Series routers with Enhanced Queuing DPCs or Trio MPC/MIC interfaces, configure an interface set for dynamic CoS.
<b>Options</b>	<p><b><i>interface-set-name</i></b>—Name of the scheduler to be configured or the Junos predefined variable (\$junos-interface-set-name). The predefined variable is replaced with the interface-set obtained from the RADIUS server when a subscriber authenticates over the interface to which the dynamic profile is attached.</p> <p>The remaining statement is explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring an Interface Set of Subscribers in a Dynamic Profile on page 712</li></ul>

## interface-traceoptions (DHCP Local Server)

<b>Syntax</b>	<pre>interface-traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;     &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>;     no-remote-trace; }</pre>
<b>Hierarchy Level</b>	<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>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Configure extended DHCP local server tracing operations that can be enabled on a specific interface or group of interfaces. You use the <b>interface <i>interface-name</i> trace</b> statement at the [edit system services group <i>group-name</i> ] hierarchy level to enable the tracing operation on the specific interfaces.
<b>Options</b>	<p><b>file <i>filename</i></b>—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 <i>/var/log</i>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, 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 <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can include the following flags:</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Trace all events</li> <li>• <b>dhcpv6-packet</b>—Trace DHCPv6 packet decoding operations.</li> <li>• <b>dhcpv6-packet-option</b>—Trace DHCPv6 option decoding operations.</li> <li>• <b>dhcpv6-state</b>—Trace changes in state for DHCPv6 operations.</li> <li>• <b>packet</b>—Trace packet decoding operations</li> <li>• <b>packet-option</b>—Trace DHCP option decoding operations</li> <li>• <b>state</b>—Trace changes in state</li> </ul> <p><b>match <i>regular-expression</i></b>—(Optional) Refine the output to include lines that contain the regular expression.</p>

**no-remote-trace**—Disable remote tracing.

**no-world-readable**—(Optional) Disable unrestricted file access.

**size *maximum-file-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.

**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.

<b>Required Privilege Level</b>	trace—To view this statement in the configuration. trace-control—To add this statement to the configuration.
---------------------------------	---

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Tracing Extended DHCP Operations on page 139</li><li>• Tracing Extended DHCP Operations for Specific Interfaces on page 144</li></ul>
------------------------------	---

## interface-traceoptions (DHCP Relay Agent)

<b>Syntax</b>	<pre>interface-traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;     &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>;     no-remote-trace; }</pre>
<b>Hierarchy Level</b>	<pre>[edit forwarding-options dhcp-relay], [edit logical-systems <i>logical-system-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], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay]</pre>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Configure extended DHCP relay agent tracing operations that can be enabled on a specific interface or group of interfaces. You use the <b>interface <i>interface-name</i> trace</b> statement at the <b>[edit forwarding-options dhcp-relay group <i>group-name</i>]</b> hierarchy level to enable the tracing operation on the specific interfaces.
<b>Options</b>	<p><b>file <i>filename</i></b>—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 <b>/var/log</b>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, 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 <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can include the following flags:</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Trace all events</li> <li>• <b>dhcpv6-packet</b>—Trace DHCPv6 packet decoding operations.</li> <li>• <b>dhcpv6-packet-option</b>—Trace DHCPv6 option decoding operations.</li> <li>• <b>dhcpv6-state</b>—Trace changes in state for DHCPv6 operations.</li> <li>• <b>packet</b>—Trace packet decoding operations</li> <li>• <b>packet-option</b>—Trace DHCP option decoding operations</li> <li>• <b>state</b>—Trace changes in state</li> </ul> <p><b>match <i>regular-expression</i></b>—(Optional) Refine the output to include lines that contain the regular expression.</p>

**no-remote-trace**—Disable remote tracing.

**no-world-readable**—(Optional) Disable unrestricted file access.

**size *maximum-file-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.

**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.

<b>Required Privilege Level</b>	trace—To view this statement in the configuration. trace-control—To add this statement to the configuration.
---------------------------------	---

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Tracing Extended DHCP Operations on page 139</li><li>• Tracing Extended DHCP Operations for Specific Interfaces on page 144</li></ul>
------------------------------	---

---

## interfaces (Subscriber Secure Policy)

---

<b>Syntax</b>	interfaces <i>interface-name</i> ;
---------------	------------------------------------

<b>Hierarchy Level</b>	[edit services radius-flow-tap]
------------------------	---------------------------------

<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
----------------------------	---

<b>Description</b>	Specify tunnel interfaces that are used to send mirrored packets to a mediation device.
--------------------	---

<b>Options</b>	<i>interface-name</i> —Name of the interface.
----------------	---

<b>Required Privilege Level</b>	flow-tap—To view this statement in the configuration. flow-tap-control—To add this statement to the configuration.
---------------------------------	---

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Subscriber Secure Policy Overview on page 625</li><li>• Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 635</li></ul>
------------------------------	--

## interfaces (ANCP)

---

<b>Syntax</b>	<pre> interfaces {   interface-set <i>interface-set-name</i> {     access-identifier <i>identifier-string</i> &lt;neighbor <i>ip-address</i>&gt;;   }   interface-name {     access-identifier <i>identifier-string</i> &lt;neighbor <i>ip-address</i>&gt;   } } </pre>
<b>Hierarchy Level</b>	[edit protocols ancp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
<b>Description</b>	Identify the subscribers whose traffic is monitored and shaped by ANCP.
<b>Options</b>	<p><b><i>interface-name</i></b>—Name of a logical interface supporting a single VLAN that carries traffic to the subscriber identified by the access node identifier.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring ANCP on page 786</li> <li>Associating an Access Node with Subscribers for ANCP Operations on page 787</li> </ul>

## interfaces (Dynamic CoS Definition)

---

**Syntax**

```
interfaces {
  interface-name {
    unit logical-unit-number {
      classifiers {
        dscp (classifier-name | default);
        dscp-ipv6 (classifier-name | default);
        ieee-802.1 (classifier-name | default) vlan-tag (inner | outer)
        inet-precedence (classifier-name | default);
      }
      output-traffic-control-profile profile-name;
      rewrite-rules {
        dscp (rewrite-name | default);
        dscp-ipv6 (rewrite-name | default);
        ieee-802.1 (rewrite-name | default) vlan-tag (outer | outer-and-inner);
        inet-precedence (rewrite-name | default);
      }
    }
  }
}
```

**Hierarchy Level** [edit dynamic-profiles *profile-name* class-of-service]

**Release Information** Statement introduced in Junos OS 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 Documentation**

- Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660
- Applying Traffic Shaping and Scheduling to a Subscriber Interface in a Dynamic Profile on page 685



## interfaces (Static and Dynamic Subscribers)

```

Syntax  interfaces {
        interface-name {
            unit logical-unit-number {
                family family {
                    access-concentrator name;
                    address address;
                    duplicate-protection;
                    dynamic-profile profile-name;
                    filter {
                        adf {
                            counter;
                            input-precedence precedence;
                            output-precedence precedence;
                            rule rule-value;
                        }
                        input filter-name (
                            precedence precedence;
                        )
                        output filter-name {
                            precedence precedence;
                        }
                    }
                    max-sessions number;
                    rpf-check {
                        mode loose;
                    }
                    service {
                        input {
                            service-set service-set-name {
                                service-filter filter-name;
                            }
                            post-service-filter filter-name;
                        }
                        output {
                            service-set service-set-name {
                                service-filter filter-name;
                            }
                        }
                    }
                    service-name-table table-name
                    unnumbered-address interface-name <preferred-source-address address>;
                }
                filter {
                    input filter-name;
                    output filter-name;
                }
                ppp-options {
                    chap;
                    pap;
                }
                proxy-arp;
                vlan-id;
            }
        }
    }

```

```
        vlan-tags outer [tpid].vlan-id [inner [tpid].vlan-id];
    }
    vlan-tagging;
}
interface-set interface-set-name {
    interface interface-name {
        unit logical-unit-number;
    }
}
demux0 {
    unit logical-unit-number {
        demux-options {
            underlying-interface interface-name
        }
        family family {
            access-concentrator name;
            address address;
            duplicate-protection;
            dynamic-profile profile-name;
            demux-source {
                source-prefix;
            }
            filter {
                input filter-name (
                    precedence precedence;
                )
                output filter-name {
                    precedence precedence;
                }
            }
            mac-validate (loose | strict):
            max-sessions number;
            rpf-check {
                mode loose;
            }
            service-name-table table-name
            unnumbered-address interface-name <preferred-source-address address>;
        }
        filter {
            input filter-name;
            output filter-name;
        }
        vlan-id number;
        vlan-tags outer [tpid].vlan-id [inner [tpid].vlan-id];
    }
}
pp0 {
    unit logical-unit-number {
        keepalives interval seconds;
        no-keepalives;
        pppoe-options {
            underlying-interface interface-name;
            server;
        }
        ppp-options {
            chap;
        }
    }
}
```

```

    pap;
  }
  family inet {
    unnumbered-address interface-name destination address;
    address address;
    service {
      input {
        service-set service-set-name {
          service-filter filter-name;
        }
        post-service-filter filter-name;
      }
      output {
        service-set service-set-name {
          service-filter filter-name;
        }
      }
    }
  }
  filter {
    input filter-name {
      precedence precedence;
    }
    output filter-name {
      precedence precedence;
    }
  }
}
}
}

```

**Hierarchy Level** [edit dynamic-profiles *profile-name*]

**Release Information** Statement introduced in Junos OS 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 Documentation**
- Configuring Static Subscriber Interfaces in Dynamic Profiles on page 439
  - Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 445
  - Relationship Between Subscribers and Interfaces in an Access Network on page 5
  - Subscriber Interface Overview on page 433
  - Configuring Dynamic PPPoE Subscriber Interfaces Using Dynamic Profiles on page 535
  - For general information about configuring static interfaces, see the [Junos OS Network Interfaces Configuration Guide](#)
  - For information about static IP demux interfaces, see the [Junos OS Network Interfaces Configuration Guide](#)

---

## interface-set

---

- Syntax** `interface-set interface-set-name {  
    access-identifier identifier-string <neighbor ip-address>;  
}`
- Hierarchy Level** [edit protocols ancp interfaces]
- Release Information** Statement introduced in Junos OS Release 9.4.
- Description** Identify a group of VLANs on which traffic is sent to a subscriber identified by the access identifier.
- Options** *interface-set-name*—Name of a group of VLANs that carry traffic to the subscriber identified by the access node identifier.
- The remaining statement is explained separately.
- Required Privilege Level** routing—To view this statement in the configuration.  
routing-control—To add this statement to the configuration.
- Related Documentation**
- Configuring ANCP on page 786
  - Associating an Access Node with Subscribers for ANCP Operations on page 787

## interface-specific (Dynamic Firewalls)

---

<b>Syntax</b>	interface-specific;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> firewall family <i>family</i> fast-update-filter <i>filter-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Configure interface-specific names for firewall counters that are based on fast update filters.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Fast Update Filters on page 581</li> </ul>

## ip-address

---

<b>Syntax</b>	ip-address <i>ip-address</i> ;
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family inet host <i>hostname</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Specify the reserved IP address assigned to the client.
<b>Options</b>	<i>ip-address</i> —IP version 4 (IPv4) address.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Address-Assignment Pools on page 68</li> <li>Configuring Static Address Assignment on page 71</li> </ul>

## ip-address-first

---

<b>Syntax</b>	ip-address-first;
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server <b>pool-match-order</b> ], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>pool-match-order</b> ], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>pool-match-order</b> ], [edit system services dhcp-local-server <b>pool-match-order</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	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 gateway IP address if one is present in the DHCP client PDU. If no gateway IP address 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.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 111</li><li>• Extended DHCP Local Server Overview on page 98</li><li>• Address-Assignment Pools Overview on page 67</li></ul>

## jsrc (JSRC)

---

<b>Syntax</b>	<pre>jsrc {     partition <i>partition-name</i> {         diameter-instance <i>instance-name</i>;         destination-host <i>hostname</i>;         destination-realm <i>realm-name</i>;     } }</pre>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	<p>Configure JSRC to interact with an SAE in an SRC environment to authorize and provision subscribers.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring JSRC on page 279</li> </ul>

## jsrc-partition

---

<b>Syntax</b>	jsrc-partition <i>partition-name</i> ;
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify the JSRC partition to use.
<b>Options</b>	<p><b><i>partition-name</i></b>—Name of the JSRC partition that you want JSRC to use. The name is defined with the <b>partition</b> statement at the <b>[edit jsrc]</b> hierarchy level.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring JSRC on page 279</li> <li>Configuring the JSRC Partition on page 280</li> </ul>

## keepalives (Dynamic Profiles)

---

<b>Syntax</b>	<pre>keepalives {     interval <i>seconds</i>; }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ] [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit"]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. The [edit dynamic-profiles <i>profile-name</i> ] hierarchy introduced in Junos OS Release 9.5. The [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit"] hierarchy introduced in Junos OS Release 10.1.
<b>Description</b>	Specify the keepalive interval in a PPP dynamic profile.
<b>Default</b>	Sending of keepalives is enabled by default. The default keepalive interval is 10 seconds for PPP.
<b>Options</b>	<b>interval <i>seconds</i></b> —The time in seconds between successive keepalive requests. <b>Range:</b> 1 through 32767 seconds <b>Default:</b> 10 seconds
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Dynamic Profiles Overview on page 369</li><li>Configuring Dynamic Authentication for PPP Subscribers on page 219</li></ul>



## key

<b>Syntax</b>	<code>key (hex   ascii) <i>string</i>;</code>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> services mobile-ip peer nai <i>name@domain</i> spi <i>hexadecimal-value</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i> ],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer nai <i>name@domain</i> spi <i>hexadecimal-value</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> services mobile-ip peer nai <i>name@domain</i> spi <i>hexadecimal-value</i>],</p> <p>[edit services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>],</p> <p>[edit services mobile-ip peer nai <i>name@domain</i> spi <i>hexadecimal-value</i>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.</p>
<b>Description</b>	<p>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.</p>
<b>Options</b>	<p><b>hex <i>string</i></b>—Key specified in HEX format</p> <p><b>ascii <i>string</i></b>—Key specified in ASCII format</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Mobile IP on page 357</li> <li>Configuring the Mobile IP Home Agent on page 358</li> </ul>

## layer2-unicast-replies

---

<b>Syntax</b>	layer2-unicast-replies;
<b>Hierarchy Level</b>	[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], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	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.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Extended DHCP Relay Agent Overview on page 154</li></ul>

## link (Address-Assignment Pools)

---

<b>Syntax</b>	link <i>pool-name</i> ;
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Configure the name of the secondary address-assignment pool that is linked to a primary address-assignment pool. The secondary pool provides backup pool for local address assignment.
<b>Options</b>	<i>pool-name</i> —Name assigned to the address-assignment pool.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Address-Assignment Pools Overview on page 67</li><li>• Configuring Address-Assignment Pools on page 68</li><li>• Configuring Address-Assignment Pool Linking on page 70</li></ul>

## local-server-group

<b>Syntax</b>	<code>local-server-group <i>local-server-group-name</i>;</code>
<b>Hierarchy Level</b>	<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>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	<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 <b>dhcp-local-server</b> statement at the [edit system services] hierarchy level.</p>
<b>Options</b>	<b><i>local-server-group-name</i></b> —Name of the extended DHCP local server group.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 189</li> </ul>

## logical-interface-fpc-redundancy (Aggregated Ethernet Subscriber Interfaces)

<b>Syntax</b>	logical-interface-fpc-redundancy;
<b>Hierarchy Level</b>	[edit interfaces <i>aenumber</i> aggregated-ether-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	<p>Provide module redundancy for demux subscribers on aggregated Ethernet bundles configured with targeted distribution. Backup links for a subscriber are chosen on a different EQ DPC or Trio MPC from the primary link, based on the link with the fewest number of subscribers among the links on different modules. If all links are on a single module when this is configured, backup links are not provisioned.</p> <p>By default, link redundancy is provided for the aggregated Ethernet bundle.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Link and Module Redundancy for Demux Subscribers in an Aggregated Ethernet Interface on page 484</li> </ul>

## logical-system (Diameter Peer)

<b>Syntax</b>	logical-system <i>logical-system-name</i> <routing-instance <i>routing-instance-name</i> > ;
<b>Hierarchy Level</b>	[edit diameter peer <i>peer-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	<p>Specify a logical system and optionally a routing instance for a Diameter peer. Alternatively, you can include the <b>routing-instance</b> statement at the [edit diameter peer <i>peer-name</i>] hierarchy level to configure only a routing instance.</p>
<b>Options</b>	<p><b><i>logical-system-name</i></b>— Name of the logical system.</p> <p><b>Default:</b> Default logical system</p> <p><b><i>routing-instance routing-instance-name</i></b>—(Optional) Name of the routing instance.</p> <p><b>Default:</b> Master routing instance</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Diameter on page 259</li> <li>Configuring Diameter Peers on page 260</li> </ul>

## logical-system (Diameter Transport)

---

<b>Syntax</b>	<code>logical-system <i>logical-system-name</i> &lt;routing-instance <i>routing-instance-name</i> &gt;;</code>
<b>Hierarchy Level</b>	[edit diameter transport <i>transport-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Specify a logical system and optionally a routing instance for the transport layer connection.



**NOTE:** The logical system and routing instance must match that for the peer or a configuration error is reported.

<b>Options</b>	<b><i>logical-system-name</i></b> —Name of the logical system. <b>Default:</b> Default logical system  <b><i>routing-instance routing-instance-name</i></b> —(Optional) Name of the routing instance. <b>Default:</b> Master routing instance
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Diameter on page 259</li><li>Configuring the Diameter Transport on page 262</li></ul>

## logical-system (Tunnel Profile)

---

<b>Syntax</b>	<code>logical-system <i>logical-system-name</i>;</code>
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify a logical system for a tunnel. When you specify a logical system, you must also specify a routing instance.
<b>Options</b>	<b><i>logical-system-name</i></b> — Name of the logical system. <b>Default:</b> Logical system <i>default</i>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Tunnel Profile for Subscriber Access on page 242</li></ul>

## logical-system-name (DHCP Local Server)

<b>Syntax</b>	logical-system-name;
<b>Hierarchy Level</b>	<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 dhcpv6 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 dhcpv6 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 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 dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> 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 dhcpv6 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 dhcpv6 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 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 dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> 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 dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication username-include]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Specify that the logical system name be concatenated with the username during the subscriber authentication process. No logical system name is concatenated if the configuration is in the default logical system.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Using External AAA Authentication Services with DHCP on page 110</li> </ul>

## logical-system-name (DHCP Relay Agent)

---

<b>Syntax</b>	logical-system-name;
<b>Hierarchy Level</b>	[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]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	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.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Using External AAA Authentication Services with DHCP on page 110</li></ul>



## logical-system-name (Static Subscribers)

<b>Syntax</b>	logical-system-name;
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i> authentication <b>username-include</b>],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers authentication <b>username-include</b>],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication <b>username-include</b>],</p> <p>[edit system services static-subscribers authentication <b>username-include</b>],</p> <p>[edit system services static-subscribers group <i>group-name</i> authentication <b>username-include</b>]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify that the name of the logical system is included as part of the username created for all static subscribers or for the static subscribers in a specified group. The group version of the statement takes precedence over the global version. The username is also sent to RADIUS in the Access-Request message.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Subscribers over Static Interfaces on page 288</li> <li>Configuring the Static Subscriber Global Username on page 291</li> <li>Configuring the Static Subscriber Group Username on page 295</li> </ul>

## loss-priority (Dynamic Schedulers)

---

<b>Syntax</b>	loss-priority (any   low   medium-low   medium-high   high);
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i> drop-profile-map]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	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.
<b>Options</b>	<p><b>any</b>—The drop profile applies to packets with any PLP.</p> <p><b>high</b>—The drop profile applies to packets with high PLP.</p> <p><b>medium</b>—The drop profile applies to packets with medium PLP.</p> <p><b>low</b>—The drop profile applies to packets with low PLP.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>Configuring Schedulers in a Dynamic Profile for Subscriber Access on page 679</li></ul>

## mac-address (DHCP Local Server)

<b>Syntax</b>	mac-address;
<b>Hierarchy Level</b>	<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>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Specify that the MAC address from the client PDU be concatenated with the username during the subscriber authentication process.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Using External AAA Authentication Services with DHCP on page 110</li> </ul>

## mac-address (DHCP Relay Agent)

---

<b>Syntax</b>	mac-address;
<b>Hierarchy Level</b>	[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]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Specify that the MAC address from the client PDU be concatenated with the username during the subscriber authentication process.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Using External AAA Authentication Services with DHCP on page 110</li></ul>

## mac-address (Dynamic Access-Internal Routes)

---

<b>Syntax</b>	<code>mac-address <i>address</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles routing-options access-internal route <i>subscriber-ip-address</i> qualified-next-hop <i>underlying-interface</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Dynamically configure the MAC address variable for an access-internal route for unnumbered interfaces such as DHCP subscriber interfaces.
<b>Options</b>	<i>address</i> —Either the specific MAC address you want to assign to the access-internal route or the MAC address variable ( <code>\$junos-subscriber-mac-address</code> ). The MAC address variable is dynamically replaced with the value supplied by DHCP when a subscriber logs in.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management on page 207</li></ul>

## mac-validate (Dynamic IP Demux Interface)

---

<b>Syntax</b>	mac-validate (loose   strict);
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family <i>family</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Enable IP and MAC address validation for dynamic IP demux interfaces in a dynamic profile. Supported on MX Series routers only.
<b>Options</b>	<p><b>loose</b>—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><b>strict</b>—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>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring MAC Address Validation for Subscriber Interfaces on page 447</li></ul>

## maintain-subscriber (Subscriber Management)

---

<b>Syntax</b>	maintain-subscriber { interface-delete; }
<b>Hierarchy Level</b>	[edit system services subscriber-management]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1.
<b>Description</b>	<p>Configure the router to maintain, rather than log out, subscribers when the specified type of event occurs (such as when an interface is deleted).</p> <p>The remaining statement is explained separately.</p>
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 124</li></ul>

## managed-configuration (Dynamic Router Advertisement)

<b>Syntax</b>	(managed-configuration   no-managed-configuration);
<b>Hierarchy Level</b>	[edit dynamic-profiles protocols router-advertisement interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Specify whether to enable the dynamic host to use a stateful autoconfiguration protocol for address autoconfiguration, along with any stateless autoconfiguration already configured: <ul style="list-style-type: none"> <li>• <b>managed-configuration</b>—Enable host to use stateful autoconfiguration.</li> <li>• <b>no-managed-configuration</b>—Disable host from using stateful autoconfiguration.</li> </ul>
<b>Default</b>	The configured object is disabled unless explicitly enabled.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Enabling Stateful Autoconfiguration with Neighbor Discovery</li> </ul>

## mandatory

<b>Syntax</b>	mandatory;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> variables <i>variable-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	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.  When a dynamic profile has mandatory and non-mandatory variables, configure mandatory variables first in the profile.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 698</li> </ul>

## map (Domain Maps)

---

**Syntax**    `map domain-map-name {  
          aaa-logical-system logical-system-name {  
            aaa-routing-instance routing-instance-name;  
          }  
          aaa-routing-instance routing-instance-name;  
          access-profile profile-name;  
          address-pool pool-name;  
          dynamic-profile profile-name;  
          padn destination-address {  
            mask destination-mask;  
            metric route-metric;  
          }  
          strip-domain;  
          target-logical-system logical-system-name {  
            target-routing-instance routing-instance-name;  
          }  
          target-routing-instance routing-instance-name;  
          tunnel-profile profile-name;  
          }  
}`

**Hierarchy Level**    [edit access domain]

**Release Information**    Statement introduced in Junos OS Release 10.4.

**Description**    Specify the domain map to use to map options and parameters to subscriber sessions based on the subscriber domain.

**Options**    *domain-map-name*—Name of the domain map. The name is the same as the subscriber domain to which it will apply. For example, for the username `user1@xyz.com`, the domain map name is `xyz.com`.

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 Documentation**

- Configuring Domain Maps on page 81



## match-direction

---

<b>Syntax</b>	<code>match-direction (input   output   input-output);</code>
<b>Hierarchy Level</b>	<code>[edit services captive-portal-content-delivery rule <i>rule-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the direction in which the rule match is applied.
<b>Options</b>	<p><b>input</b>—Apply the rule match on the input side of the interface.</p> <p><b>output</b>—Apply the rule match on the output side of the interface.</p> <p><b>input-output</b>—Apply the rule match bidirectionally.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Redirecting HTTP Requests on page 613</li> </ul>

## mask (Domain Maps)

---

<b>Syntax</b>	<code>mask <i>destination-mask</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access domain map <i>domain-map-name</i> padn <i>destination-address</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Configure the IP mask of the destination used in the PADN parameters for a domain map.
<b>Options</b>	<b><i>destination-mask</i></b> —Subnet mask of the destination.
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Configuring PADN Parameters for a Domain Map on page 89</li> </ul>

## match-order (Dynamic Firewalls)

---

<b>Syntax</b>	<code>match-order [<i>match-order</i>];</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> firewall family <i>family</i> fast-update-filter <i>filter-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify the match conditions and the order in which the conditions are examined. Enclose a string of multiple conditions in brackets. The router examines only the conditions you specify, and examines them in the specified order.
<b>Options</b>	<p><b><i>match-order</i></b>—One or more of the following conditions. “Fast Update Filter Match Conditions” on page 584 describes the match conditions.</p> <ul style="list-style-type: none"><li>• destination-address</li><li>• destination-port</li><li>• dscp (IPv4 only)</li><li>• protocol (IPv4 only)</li><li>• source-address</li><li>• source-port</li></ul>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Fast Update Filters on page 581</li><li>• Configuring the Match Order for Fast Update Filters on page 582</li><li>• Fast Update Filter Match Conditions on page 584</li></ul>

## max-advertisement-interval (Dynamic Router Advertisement)

<b>Syntax</b>	max-advertisement-interval <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit dynamic-profiles protocols router-advertisement interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Maximum interval between each router advertisement message.
<b>Options</b>	<i>seconds</i> —Maximum interval. <b>Range:</b> 4 through 1800 seconds <b>Default:</b> 600 seconds
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>min-advertisement-interval</li> <li>Configuring the Frequency of Neighbor Discovery Advertisements</li> </ul>

## maximum-discovery-table-entries

<b>Syntax</b>	maximum-discovery-table-entries <i>entry-number</i> ;
<b>Hierarchy Level</b>	[edit protocols ancp], [edit protocols ancp neighbor]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Specify the maximum number of discovery table entries accepted from a particular neighbor. The neighbor can continue to update previously created entries when the maximum has been exceeded, but no new entries are accepted.
<b>Default</b>	No limit on the number of table entries
<b>Options</b>	<i>entry-number</i> —Maximum number of discovery table entries. <b>Range:</b> 1 through 100,000
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring ANCP on page 786</li> <li>Configuring ANCP Neighbors on page 786</li> </ul>

## maximum-helper-restart-time

---

<b>Syntax</b>	maximum-helper-restart-time <i>seconds</i>
<b>Hierarchy Level</b>	[edit protocols ancpx]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
<b>Description</b>	Specify how long other router processes wait for ANCP to restart before considering it to be down.
<b>Options</b>	<b>seconds</b> —Number of seconds other processes wait for ANCP to restart. <b>Range:</b> 45 through 600 seconds <b>Default:</b> 45 seconds
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring ANCP on page 786</li><li>Specifying How Long Processes Wait for ANCP Restart to Complete on page 789</li></ul>

## maximum-lease-time

---

<b>Syntax</b>	maximum-lease-time <i>seconds</i> ;
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family (inet   inet6) dhcp-attributes]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	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.
<b>Options</b>	<b>seconds</b> —Maximum number of seconds the lease can be held. <b>Range:</b> 30 through 4,294,967,295 seconds <b>Default:</b> 86,400 (24 hours)
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Address-Assignment Pools on page 68</li></ul>

## max-outstanding-requests (Gx-Plus)

---

<b>Syntax</b>	max-outstanding-requests <i>number</i> ;
<b>Hierarchy Level</b>	[edit access gx-plus global]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Limit the number of outstanding requests to the PCRF that Gx-Plus can retry when the requests are improperly answered. Too many requests risks overloading the PCRF and increases the chance of losing messages.
<b>Options</b>	<b>number</b> —Number of outstanding requests from Gx-Plus to the PCRF that can exist at any time. <b>Default:</b> 40 <b>Range:</b> 2 through 40
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Gx-Plus on page 339</li></ul>

## max-sessions (Dynamic PPPoE)

<b>Syntax</b>	<code>max-sessions <i>number</i>;</code>
<b>Hierarchy Level</b>	<p>[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> pppoe-underlying-options],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> pppoe-underlying-options]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 10.1.</p> <p>(MX Series routers with Trio MPCs only) The [edit ... family pppoe] hierarchies introduced in Junos OS Release 11.2.</p>
<b>Description</b>	Configure the maximum number of dynamic PPPoE logical interfaces that the router can activate on the underlying interface. The <b>max-sessions</b> value does not affect the maximum number of static PPPoE logical interfaces that can be configured on the underlying interface.
<b>Options</b>	<p><b>number</b>—Maximum number of dynamic PPPoE logical interfaces (sessions) that the router can activate on the underlying interface. The default value is equal to the maximum number of PPPoE sessions supported on your routing platform. You can configure from 1 to the platform-specific default for your routing platform. Changing the <b>max-sessions</b> value has no effect on dynamic PPPoE logical interfaces that are already active.</p> <p><b>Range:</b></p> <p>For Intelligent Queuing 2 (IQ2) PICs on M120 and M320 Series routers, 1 through 4000.</p> <p>For Trio MPCs on MX Series routers, 1 through 32000.</p> <p><b>Default:</b></p> <p>For Intelligent Queuing 2 (IQ2) PICs on M120 and M320 Series routers, 4000.</p> <p>For Trio MPCs on MX Series routers, 32000.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring an Underlying Interface for Dynamic PPPoE Subscriber Interfaces on page 541</li> <li>Configuring the PPPoE Family for an Underlying Interface on page 486</li> <li>For information about creating static PPPoE interfaces, see the <a href="#">Junos OS Network Interfaces Configuration Guide</a></li> </ul>

## max-sessions (PPPoE Service Name Tables)

<b>Syntax</b>	<code>max-sessions <i>number</i>;</code>
<b>Hierarchy Level</b>	<code>[edit protocols pppoe service-name-tables <i>table-name</i> service <i>service-name</i>],</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	<p>Configure the maximum number of active PPPoE sessions using either static or dynamic PPPoE interfaces that the router can establish with the specified named service, <b>empty</b> service, or <b>any</b> service entry in a PPPoE service name table. The router maintains a count of active PPPoE sessions for each service entry to determine when the maximum sessions limit has been reached.</p> <p>The router uses the <b>max-sessions</b> value for a PPPoE service name table entry in conjunction with the <b>max-sessions</b> value configured for the PPPoE underlying interface, and with the maximum number of PPPoE sessions supported on your router. If your configuration exceeds any of these maximum session limits, the router is unable to establish the PPPoE session.</p>
<b>Options</b>	<p><b><i>number</i></b>—Maximum number of active PPPoE sessions that the router can establish with the specified PPPoE service name table entry, in the range 1 to the platform-specific maximum PPPoE sessions supported for your router. The default value is equal to the maximum number of PPPoE sessions supported on your routing platform.</p> <p><b>Range:</b> Specify the range according to the PIC type and router.</p> <p>For Intelligent Queuing 2 (IQ2) PICs on M120 and M320 Series routers, 1 through 16000.</p> <p>For Trio MPC/MIC interfaces on MX Series routers, 1 through 64000.</p> <p><b>Default:</b> The default value is determined by the PIC type and router.</p> <p>For Intelligent Queuing 2 (IQ2) PICs on M120 and M320 Series routers, 16000.</p> <p>For Trio MPC/MIC interfaces on MX Series routers, 64000.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring PPPoE Service Name Tables</li> <li>Limiting the Number of Active PPPoE Sessions Established with a Specified Service Name</li> <li><b>max-sessions (Dynamic PPPoE) on page 1056</b></li> </ul>

## max-sessions (Tunnel Profile)

---

<b>Syntax</b>	<code>max-sessions <i>number</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the maximum number of sessions allowed in the tunnel.
<b>Default</b>	0
<b>Options</b>	<i>number</i> —Maximum number of sessions allowed in the tunnel.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Tunnel Profile for Subscriber Access on page 242</li></ul>

## medium (Tunnel Profile)

---

<b>Syntax</b>	<code>medium <i>type</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the medium type for the tunnel.
<b>Default</b>	ipv4
<b>Options</b>	<i>type</i> —Medium type for the tunnel. The only value currently available is <b>ipv4</b> .
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Tunnel Profile for Subscriber Access on page 242</li></ul>



## metric (Dynamic Access-Internal Routes)

<b>Syntax</b>	<code>metric route-cost;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles routing-options access route <i>prefix</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Dynamically configure the cost for an access route.
<b>Options</b>	<i>route-cost</i> —Either the specific cost you want to assign to the access route or the cost variable ( <code>\$junos-framed-route-cost</code> ). The cost variable is dynamically replaced with the value in Framed-Route Attribute [22].
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Dynamic Access Routes for Subscriber Management on page 206</li> </ul>

## metric (Diameter Route)

<b>Syntax</b>	<code>metric route-metric;</code>
<b>Hierarchy Level</b>	[edit diameter network-statement <i>element-name</i> forwarding route <i>dne-route-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify the metric associated with a destination and function. Together, these three elements define a route reachable through a Diameter network element. A lower metric makes a route more preferred.
<b>Options</b>	<i>route-metric</i> —Metric assigned to the route. <b>Range:</b> 0 through 255
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Diameter on page 259</li> <li>Configuring Diameter Network Elements on page 261</li> </ul>

## metric (Domain Maps)

---

<b>Syntax</b>	<code>metric route-metric;</code>
<b>Hierarchy Level</b>	[edit access domain map <i>domain-map-name</i> padn <i>destination-address</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Configure the route metric PADN parameter for a domain map.
<b>Options</b>	<b>route-metric</b> —Value assigned to the route. <b>Range:</b> 0 through 255
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring PADN Parameters for a Domain Map on page 89</li></ul>

## min-advertisement-interval (Dynamic Router Advertisement)

---

<b>Syntax</b>	<code>min-advertisement-interval seconds;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles protocols router-advertisement interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Minimum interval between each router advertisement message.
<b>Options</b>	<b>seconds</b> —Minimum interval. <b>Range:</b> 3 seconds through three-quarter times the maximum advertisement interval value <b>Default:</b> One-third the maximum advertisement interval value
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>max-advertisement-interval</li><li>Configuring the Frequency of Neighbor Discovery Advertisements</li></ul>

## mld (Dynamic Profiles)

```

Syntax  mld {
        interface interface-name {
            disable;
            (accounting | no-accounting);
            group-policy;
            immediate-leave;
            oif-map;
            passive;
            ssm-map ssm-map-name;
            static {
                group multicast-group-address {
                    exclude;
                    group-count number;
                    group-increment increment;
                    source ip-address {
                        source-count number;
                        source-increment increment;
                    }
                }
            }
            version version;
        }
    }

```

**Hierarchy Level** [edit dynamic-profiles *profile-name* protocols]

**Release Information** Statement introduced in Junos OS Release 10.1.

**Description** Configure interface-specific MLD values on dynamic interfaces.

**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 Documentation**

- Enabling MLD

## mobile-ip

Syntax	<pre> mobile-ip {   access-type {     (generic   wimax);   }   authenticate {     order (aaa   local);   }   dynamic-home-assignment {     home-agent {       nai (name@domain   @domain) {         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 name@domain) {       spi hexadecimal-value {         algorithm (hmac-md5   md5);         entity-type (host   mobility-agent);         key (hex   ascii) string;         replay-method (none   timestamp seconds);       }     }   }   traceoptions {     file filename &lt;files number&gt; &lt;match regular-expression &gt; &lt;size maximum-file-size&gt;       &lt;world-readable   no-world-readable&gt;;     flag flag;     level (all   error   info   notice   verbose   warning);     no-remote-trace;   } } </pre>
Hierarchy Level	<p>[edit services],  [edit logical-systems <i>logical-system-name</i> services],  [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services],  [edit routing-instances <i>routing-instances-name</i> services]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3.  Support at the [edit logical-systems <i>logical-system-name</i> services], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services], and [edit</p>

	<b>routing-instances <i>routing-instances-name</i> services</b> ] hierarchy levels introduced in Junos OS Release 9.5.
<b>Description</b>	Configure Junos Mobile IP features.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring the Mobile IP Home Agent on page 358</li> </ul>

## mode

<b>Syntax</b>	mode loose;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family (inet) <b>rpf-check</b> ],
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Check whether the packet has a source address with a corresponding prefix in the routing table. If a corresponding prefix is not found, unicast reverse path forwarding (RPF) loose mode does not accept the packet. Unlike strict mode, loose mode does not check whether the interface expects to receive a packet with a specific source address prefix.
<b>Default</b>	If you do not include this statement, unicast RPF is in strict mode.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Unicast RPF</li> </ul>

## multicast (Dynamic Routing Options)

---

**Syntax**    multicast {  
              interface *interface-name* {  
                  no-qos-adjust;  
              }  
          }

**Hierarchy Level**    [edit dynamic-profiles *profile-name* routing-options],  
                      [edit dynamic-profiles *profile-name* routing-instances *routing-instance-name* routing-options]



**NOTE:** You cannot apply a scope policy to a specific routing instance. That is, all scoping policies are applied to all routing instances. However, the *scope* statement does apply individually to a specific routing instance.

**Release Information**    Statement introduced in Junos OS Release 9.6.

**Description**    Dynamically configure interface-specific multicast routing options properties.  
  
                      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 Documentation**

- Example: Configuring the Multicast Forwarding Cache
- Example: Configuring a Multicast Flow Map
- Example: Configuring Source-Specific Multicast Groups with Any-Source Override

## nai

<b>Syntax</b>	<code>nai (name@domain   @domain) {     home-agent ip-address; }</code>
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> services mobile-ip dynamic-home-assignment home-agent], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip dynamic-home-assignment home-agent], [edit routing-instances <i>routing-instances-name</i> services mobile-ip dynamic-home-assignment home-agent], [edit services mobile-ip dynamic-home-assignment home-agent]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.
<b>Description</b>	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*—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.

<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Mobile IP on page 357</li> <li>Configuring Dynamic Home Assignment for the Mobile Node on page 360</li> </ul>

## name-server

---

<b>Syntax</b>	<code>name-server [ <i>server-names</i> ];</code>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	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.
<b>Options</b>	<i>server-names</i> —IP addresses of the domain name servers, listed in order of preference.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Address-Assignment Pools on page 68</li></ul>


## nas-identifier

---

<b>Syntax</b>	<code>nas-identifier <i>identifier-value</i>;</code>
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> radius options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
<b>Description</b>	Configure the value for the client RADIUS attribute 32 (NAS-Identifier). This attribute is used for authentication and accounting requests.
<b>Options</b>	<i>identifier-value</i> —String to use for authentication and accounting requests. <b>Range:</b> 1 through 64 characters
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring RADIUS Server Options for Subscriber Access on page 29</li><li>Configuring RADIUS Server Parameters for Subscriber Access on page 26</li></ul>



## nas-port-extended-format

<b>Syntax</b>	<pre>nas-port-extended-format {   adapter-width <i>width</i>;   port-width <i>width</i>;   slot-width <i>width</i>;   stacked-vlan-width <i>width</i>;   vlan-width <i>width</i>; }</pre>
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> radius options]
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p>
<b>Description</b>	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.
<b>Options</b>	<p><b>adapter-width <i>width</i></b>—Number of bits in the adapter field.</p> <p><b>port-width <i>width</i></b>—Number of bits in the port field.</p> <p><b>slot-width <i>width</i></b>—Number of bits in the slot field.</p> <p><b>stacked-vlan-width <i>width</i></b>—Number of bits in the SVLAN ID field.</p> <p><b>vlan-width <i>width</i></b>—Number of bits in the VLAN ID field.</p>
	<div>  <p><b>NOTE:</b> The total of the widths must not exceed 32 bits, or the configuration will fail.</p> </div>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring RADIUS Server Options for Subscriber Access on page 29</li> <li>Configuring RADIUS Server Parameters for Subscriber Access on page 26</li> </ul>

## neighbor (Associate with Access Identifier)

---

<b>Syntax</b>	<code>neighbor ip-address;</code>
<b>Hierarchy Level</b>	[edit protocols ancp interfaces interface-set <i>interface-set-name</i> access-identifier <i>identifier-string</i> ], [edit protocols ancp interfaces <i>interface-name</i> access-identifier <i>identifier-string</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Configure an ANCP neighbor to be monitored.
<b>Options</b>	<i>ip-address</i> —IP address of the ANCP neighbor.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring ANCP on page 786</li><li>Associating an Access Node with Subscribers for ANCP Operations on page 787</li></ul>

## neighbor (Define)

---

<b>Syntax</b>	<code>neighbor ip-address {     adjacency-timer <i>seconds</i>;     ietf-mode;     maximum-discovery-table-entries;     pre-ietf-mode; }</code>
<b>Hierarchy Level</b>	[edit protocols ancp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
<b>Description</b>	Configure an ANCP neighbor to be monitored.
<b>Options</b>	<i>ip-address</i> —IP address of the ANCP neighbor.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring ANCP on page 786</li><li>Configuring ANCP Neighbors on page 786</li></ul>

## neighbor-discovery-router-advertisement (Address-Assignment Pools)

<b>Syntax</b>	<code>neighbor-discovery-router-advertisement <i>ndra-pool-name</i>;</code>
<b>Hierarchy Level</b>	[edit access address-assignment]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Configure the name of the address-assignment pool used to assign the router advertisement prefix.
<b>Options</b>	<i>ndra-pool-name</i> —Name of the address-assignment pool.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Address-Assignment Pools Overview on page 67</li> <li>Configuring an Address-Assignment Pool for Router Advertisement</li> </ul>

## netbios-node-type

<b>Syntax</b>	<code>netbios-node-type <i>node-type</i>;</code>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Specify the NetBIOS node type. This is equivalent to DHCP option 46.
<b>Options</b>	<i>node-type</i> —One of the following node types: <ul style="list-style-type: none"> <li><b>b-node</b>—Broadcast node</li> <li><b>h-node</b>—Hybrid node</li> <li><b>m-node</b>—Mixed node</li> <li><b>p-node</b>—Peer-to-peer node</li> </ul>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Address-Assignment Pools on page 68</li> </ul>

## network

---

<b>Syntax</b>	<code>network <i>ip-prefix</i>&lt;/<i>prefix-length</i>&gt;;</code>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family inet]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Configure subnet information for an IPv4 address-assignment pool.
<b>Options</b>	<ul style="list-style-type: none"><li>• <i>ip-prefix</i>—IP version 4 address or prefix value.</li><li>• <i>prefix-length</i>—(Optional) Subnet mask.</li></ul>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Address-Assignment Pools on page 68</li></ul>

## network-element (Diameter Base Protocol)

```
Syntax  network-element element-name {
        forwarding {
            route dne-route-name {
                destination realm realm-name <host hostname> ;
                function function-name <partition partition-name>;
                metric route-metric;
            }
        }
        function function-name;
        peer peer-name {
            priority priority-number;
        }
    }
```

**Hierarchy Level** [edit diameter]

**Release Information** Statement introduced in Junos OS Release 9.6.

**Description** Specify the transport layer Diameter configuration. The Diameter network element includes a list of routes reachable through the Diameter instance, associated functions, and prioritized Diameter peers.

**Options** *element-name*—Name of the network element.  
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 Documentation**

- Configuring Diameter on page 259
- Configuring Diameter Network Elements on page 261

## next-hop (Dynamic Access-Internal Routes)

---


<b>Syntax</b>	<code>next-hop <i>next-hop</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles routing-options access route <i>prefix</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Dynamically configure the next-hop address for an access route. Access routes are typically unnumbered interfaces.
<b>Options</b>	<p><i>next-hop</i>—Either the specific next-hop address you want to assign to the access route or one of the following next-hop address predefined variables.</p> <ul style="list-style-type: none"><li>For IPv4 access routes, use the variable, <b>\$junos-framed-route-nexthop</b>. The route prefix variable is dynamically replaced with the value in Framed-Route RADIUS attribute [22].</li><li>For IPv6 access routes, use the variable, <b>\$junos-framed-route-ipv6-nexthop</b>. The variable is dynamically replaced with the value in Framed-IPv6-Route RADIUS attribute [99].</li></ul>
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Dynamic Access Routes for Subscriber Management on page 206</li></ul>

## no-accounting

---

<b>Syntax</b>	<code>no-accounting;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Disable the collection of IGMP join and leave event statistics on a per-interface basis.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Dynamic Profile for Client Access on page 395</li><li>For information about disabling IGMP accounting on an interface, see “Recording IGMP Join and Leave Events” in the <a href="#">Junos OS Multicast Protocols Configuration Guide</a></li></ul>

## no-allow-snooped-clients

<b>Syntax</b>	no-allow-snooped-clients;
<b>Hierarchy Level</b>	<p>[edit forwarding-options dhcp-relay overrides],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</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> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Explicitly disable DHCP snooping support on the router.
	<div>  <p><b>NOTE:</b> In Junos OS Release 10.0 and earlier, DHCP snooping is <i>enabled</i> by default. In Release 10.1 and later, DHCP snooping is <i>disabled</i> by default.</p> </div>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Extended DHCP Relay Agent Overview on page 154</li> <li>Overriding the Default DHCP Relay Configuration Settings on page 168</li> <li>DHCP Snooping Support on page 174</li> </ul>

## no-arp (DHCP Local Server)

---

<b>Syntax</b>	no-arp;
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides], [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], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server overrides], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides], [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], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> overrides], [edit system services dhcp-local-server overrides], [edit system services dhcp-local-server group <i>group-name</i> overrides] [edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i> overrides]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Turn off ARP table population in a distrusted environment.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.




## no-arp (DHCP Relay Agent)

<b>Syntax</b>	no-arp;
<b>Hierarchy Level</b>	[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], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Turn off ARP table population in a distrusted environment.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Extended DHCP Relay Agent Overview on page 154</li> <li>Overriding the Default DHCP Relay Configuration Settings on page 168</li> </ul>

## no-bind-on-request (DHCP Relay Agent)

---

<b>Syntax</b>	no-bind-on-request;
<b>Hierarchy Level</b>	<p>[edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-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> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-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 logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-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], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Explicitly disable automatic binding of received DHCP request messages that have no entry in the database ( <i>stray</i> requests).
<div> <b>NOTE:</b> Beginning with Junos OS Release 10.4, automatic binding of stray requests is enabled by default. In Junos OS Release 10.3 and earlier releases, automatic binding of stray requests is disabled by default.</div>	
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Extended DHCP Relay Agent Overview on page 154</li><li>• Overriding the Default DHCP Relay Configuration Settings on page 168</li><li>• Disabling Automatic Binding of Stray DHCP Requests on page 187</li></ul>

## no-keepalives (Dynamic Profiles)

<b>Syntax</b>	no-keepalives;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ], [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit"]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Support of the [edit dynamic-profiles <i>profile-name</i> ] hierarchy level introduced in Junos OS Release 9.5. Support of the [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit"] hierarchy level introduced in Junos OS Release 10.1.
<b>Description</b>	Disable the sending of keepalives.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Dynamic Profiles Overview on page 369</li> <li>Configuring Dynamic Authentication for PPP Subscribers on page 219</li> </ul>

## no-qos-adjust (Dynamic Routing Options)

<b>Syntax</b>	no-qos-adjust;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> routing-options multicast interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Disable hierarchical bandwidth adjustment for all dynamically created subscriber interfaces that are identified by their MLD or IGMP request from a specific multicast interface.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Example: Configuring Multicast with Subscriber VLANs</li> </ul>

## oif-map (Dynamic IGMP Interface)

---

<b>Syntax</b>	<code>oif-map <i>map-name</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Associates an OIF map to the IGMP interface using a dynamic profile. The OIF map is a routing policy statement that can contain multiple terms.
<b>Options</b>	<i>map-name</i> —Name of the OIF map.
<b>Required Privilege</b>	routing—To view this statement in the configuration.
<b>Level</b>	routing-control—To add this statement to the configuration.

## oif-map (Dynamic MLD Interface)

---

<b>Syntax</b>	<code>oif-map <i>map-name</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols mld interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Associate an outgoing interface (OIF) map to a dynamic MLD logical interface. The OIF map is a routing policy statement that can contain multiple terms.
<b>Required Privilege</b>	routing—To view this statement in the configuration.
<b>Level</b>	routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Example: Configuring Multicast with Subscriber VLANs</li></ul>

## on-link (Dynamic Router Advertisement)

---

<b>Syntax</b>	(on-link   no-on-link);
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols router-advertisement interface <i>interface-name</i> prefix <i>prefix</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	<p>Specify whether to enable prefixes to be used for onlink determination:</p> <ul style="list-style-type: none"><li>• <b>no-on-link</b>—Disable prefixes from being used for onlink determination.</li><li>• <b>on-link</b>—Enable prefixes to be used for onlink determination.</li></ul>
<b>Default</b>	The configured object is enabled unless explicitly disabled.
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring the Prefix Information Included in Neighbor Discovery Advertisements</li></ul>

## option

---

<b>Syntax</b>	<pre>option {     [ (id-number option-type option-value)       (id-number array option-type option-value) ]; }</pre>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family (inet   inet6) dhcp-attributes]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Specify user-defined options that are added to client packets.
<b>Options</b>	<p><b>array</b>—An option can include an array of option types.</p> <p><b>id-number</b>—Any whole number. The ID number is used to index the option and must be unique across a DHCP server.</p> <p><b>option-type</b>—Any of the following types: byte, flag, integer, ip-address, short, string, unsigned-integer, or unsigned-short.</p> <p><b>option-value</b>—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).</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Address-Assignment Pools on page 68</li></ul>

## option-60 (DHCP Local Server)

<b>Syntax</b>	option-60;
<b>Hierarchy Level</b>	<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>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Specify that the payload of Option 60 (Vendor Class Identifier) from the client PDU be concatenated with the username during the subscriber authentication process.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Using External AAA Authentication Services with DHCP on page 110</li> </ul>

## option-60 (DHCP Relay Agent)

---

<b>Syntax</b>	option-60;
<b>Hierarchy Level</b>	[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]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	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.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Using External AAA Authentication Services with DHCP on page 110</li></ul>



## option-82 (Address-Assignment Pools)

---

<b>Syntax</b>	<pre>option-82 {     circuit-id <i>value</i> range <i>named-range</i>;     remote-id <i>value</i> range <i>named-range</i>; }</pre>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes option-match]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	<p>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.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Address-Assignment Pools on page 68</li></ul>

## option-82 (DHCP Local Server Authentication)

---


<b>Syntax</b>	<code>option-82 &lt;circuit-id&gt; &lt;remote-id&gt;;</code>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication <b>username-include</b>],</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 <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication <b>username-include</b>],</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 <b>username-include</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication <b>username-include</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication <b>username-include</b>],</p> <p>[edit system services dhcp-local-server authentication <b>username-include</b>],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication <b>username-include</b>]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	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.
<b>Options</b>	<p><b>circuit-id</b>—(Optional) Agent Circuit ID suboption (suboption 1).</p> <p><b>remote-id</b>—(Optional) Agent Remote ID suboption (suboption 2).</p>
<b>Required Privilege Level</b>	<p><b>system</b>—To view this statement in the configuration.</p> <p><b>system-control</b>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Using External AAA Authentication Services with DHCP on page 110</li></ul>

## option-82 (DHCP Local Server Pool Matching)

<b>Syntax</b>	option-82;
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>pool-match-order</b> ], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server <b>pool-match-order</b> ], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>pool-match-order</b> ], [edit system services dhcp-local-server <b>pool-match-order</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	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 <b>ip-address-first</b> statement before configuring the <b>option-82</b> 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. This statement is supported for IPv4 address-assignment pools only.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 111</li> <li>Extended DHCP Local Server Overview on page 98</li> <li>Address-Assignment Pools Overview on page 67</li> </ul>

## option-82 (DHCP Relay Agent)

---

<b>Syntax</b>	<code>option-82 &lt;circuit-id&gt; &lt;remote-id&gt;;</code>
<b>Hierarchy Level</b>	<code>[edit forwarding-options dhcp-relay authentication username-include],</code> <code>[edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</code> <code>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include],</code> <code>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</code> <code>[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],</code> <code>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</code> <code>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Specify the option 82 that is concatenated with the username during the subscriber authentication process. You can specify either, both, or neither the Agent Circuit ID and 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 neither suboption is supplied, the raw payload of option 82 is concatenated to the username.
<div> <b>NOTE:</b> The option 82 value used in creating the username is based on the option 82 value that is encoded in the outgoing (relayed) PDU.</div>	
<b>Options</b>	<b>circuit-id</b> —(Optional) The string for the Agent Circuit ID suboption (suboption 1).  <b>remote-id</b> —(Optional) The string for the Agent Remote ID suboption (suboption 2).
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Using External AAA Authentication Services with DHCP on page 110</li></ul>

## option-match

<b>Syntax</b>	<pre> option-match {   option-82 {     circuit-id <i>value</i> range <i>named-range</i>;     remote-id <i>value</i> range <i>named-range</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	<p>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.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Address-Assignment Pools on page 68</li> </ul>

## options

---

**Syntax**    options {  
              accounting-session-id-format (decimal | description);  
              client-accounting-algorithm (direct | round-robin);  
              client-authentication-algorithm (direct | round-robin);  
              ethernet-port-type-virtual;  
              interface-description-format {  
                  exclude-adapter;  
                  exclude-sub-interface;  
              }  
              nas-identifier *identifier-value*;  
              nas-port-extended-format {  
                  adapter-width *width*;  
                  port-width *width*;  
                  slot-width *width*;  
                  stacked-vlan-width *width*;  
                  vlan-width *width*;  
              }  
              revert-interval *interval*;  
              vlan-nas-port-stacked-format;  
          }

**Hierarchy Level**    [edit access profile *profile-name* radius]

**Release Information**    Statement introduced in Junos OS Release 9.1.  
                              Statement introduced in Junos OS Release 9.1 for EX Series switches.

**Description**    Configure the options used by RADIUS authentication and accounting servers.  
  
                      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 Documentation**    • Configuring RADIUS Server Parameters for Subscriber Access on page 26  
                                  • RADIUS Server Options for Subscriber Access on page 28

## order

---

<b>Syntax</b>	<code>order [ <i>accounting-method</i> ];</code>
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> accounting]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
<b>Description</b>	Set the order in which the Junos OS tries different accounting methods for client activity. When a client logs in, the software tries the accounting methods in the specified order.
<b>Options</b>	<b><i>accounting-method</i></b> —One or more accounting methods. When a client logs in, the software tries the accounting methods in the following order, from first to last. The only valid value is <b>radius</b> for RADIUS accounting.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li></ul>

## order (Mobile IP)

---

<b>Syntax</b>	order (aaa   local);
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> services mobile-ip authenticate], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip authenticate], [edit routing-instances <i>routing-instances-name</i> services mobile-ip authenticate], [edit services mobile-ip authenticate]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.
<b>Description</b>	Define the authentication method performed for Mobile IP.
<b>Default</b>	AAA is the default authentication method.
<b>Options</b>	<b>aaa</b> —Authentication is performed by AAA. This option is available only in the default router and default routing instance, and therefore only in the [edit services mobile-ip] hierarchy level.  <b>local</b> —Authentication is performed using parameters defined in the local database.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Mobile IP on page 357</li><li>Configuring the Access Type for Mobile IP on page 361</li></ul>



## origin (Diameter Base Protocol)

<b>Syntax</b>	origin { host <i>hostname</i> ; realm <i>realm-name</i> ; }
<b>Hierarchy Level</b>	[edit diameter]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify values of Origin-Realm-AVP and Origin-Host-AVP used in all messages sent by the Diameter instance.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Diameter on page 259</li> <li>Configuring the Origin Attributes of the Diameter Instance on page 260</li> </ul>

## other-stateful-configuration (Dynamic Router Advertisement)

<b>Syntax</b>	(other-stateful-configuration   no-other-stateful-configuration);
<b>Hierarchy Level</b>	[edit dynamic-profiles protocols router-advertisement interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Specify whether to enable autoconfiguration of other nonaddress-related information: <ul style="list-style-type: none"> <li><b>no-other-stateful-configuration</b>—Disable autoconfiguration of other nonaddress-related information.</li> <li><b>other-stateful-configuration</b>—Enable autoconfiguration of other nonaddress-related information.</li> </ul>
<b>Default</b>	The configured object is disabled unless explicitly enabled.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Enabling Stateful Autoconfiguration with Neighbor Discovery</li> </ul>

## output (Dynamic Service Sets)

---

<b>Syntax</b>	<code>service-set service-set-name {     service-filter filter-name; }</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> service], [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i> service]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. Support of the [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i> service] hierarchy level introduced in Junos OS Release 10.1.
<b>Description</b>	Define the output service sets and filters to be applied to traffic by a dynamic profile. Only the Internet Protocol version 4 (IPv4) protocol family is currently supported for dynamic PPPoE logical interfaces.  The remaining statement is explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Dynamic Service Sets Overview on page 569</li><li>• Associating Service Sets with Interfaces in a Dynamic Profile on page 595</li></ul>

## output-traffic-control-profile (Dynamic CoS Definition)

---

<b>Syntax</b>	<code>output-traffic-control-profile profile-name;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Apply an output traffic scheduling and shaping profile to the logical interface.
<b>Options</b>	<i>profile-name</i> —Name of the traffic-control profile to be applied to this interface
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>• Applying Traffic Shaping and Scheduling to a Subscriber Interface in a Dynamic Profile on page 685</li><li>• traffic-control-profiles on page 1240</li></ul>

## output-vlan-map (Dynamic Interfaces)

<b>Syntax</b>	<pre>output-vlan-map {     inner-tag-protocol-id <i>tpid</i>;     inner-vlan-id <i>number</i>;     (pop   swap);     tag-protocol-id <i>tpid</i>;     vlan-id <i>number</i>; }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	<p>For dynamic interfaces, define the rewrite profile to be applied to outgoing frames on this logical interface.</p> <p>The statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution</li> </ul>

## overhead-accounting (Dynamic Traffic Shaping)

---

<b>Syntax</b>	<code>overhead-accounting (<i>shaping-mode</i>) &lt;bytes (<i>byte-value</i>)</code> ;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Configure the mode to shape downstream ATM traffic based on either frames or cells.
<b>Default</b>	The default is <b>frame-mode</b> .
<b>Options</b>	<p><i>shaping-mode</i>—One of the following shaping mode parameters:</p> <ul style="list-style-type: none"><li>• <b>frame-mode</b>—Shaping based on the number of bytes in the frame, without regard to cell encapsulation or padding overhead.</li><li>• <b>cell-mode</b>—Shaping based on the number of bytes in cells, and accounts for the ATM cell encapsulation and padding overhead. The resulting traffic stream conforms to the policing rates configured in downstream ATM switches, reducing the number of packet drops in the Ethernet network</li><li>• <b>\$junos-cos-shaping-mode</b>—Variable for the shaping mode that is replaced with a value obtained from the RADIUS server when a subscriber authenticates over the interface to which the dynamic profile is attached.</li></ul> <p><i>byte-value</i>—Byte adjustment value for the cell or shaping mode, or the Junos predefined variable:</p> <p><b>\$junos-cos-byte-adjust</b>—Variable for byte adjustment that is replaced with a value obtained from the RADIUS server when a subscriber authenticates over the interface to which the dynamic profile is attached.</p> <p><b>Range:</b> –120 through 124 bytes</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Dynamic Shaping Parameters to Account for Overhead in Downstream Traffic Rates on page 758</li><li>• Bandwidth Management for Downstream Traffic in Edge Networks Overview on page 747</li><li>• egress-shaping-overhead</li></ul>

## overrides (DHCP Local Server)

<b>Syntax</b>	<pre> overrides {     client-discover-match;     interface-client-limit <i>number</i>;     no-arp; } </pre>
<b>Hierarchy Level</b>	<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> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</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>],</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> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit system services dhcp-local-server],</p> <p>[edit system services dhcp-local-server dhcpv6],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i>],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit system services dhcp-local-server group <i>group-name</i>],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Override the default configuration settings for the extended DHCP local server. Specifying the <b>overrides</b> 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 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 override configuration options for a specific interface within a named group of interfaces, include the statements at the **[edit system services dhcp-local-server group *group-name* interface *interface-name*]** hierarchy level.
- Use the **[edit system services dhcp-local-server dhcpv6]** hierarchy level to override DHCPv6 configuration options.

The remaining statements are explained separately.

The **interface-client-limit** and **no-arp** statements are not supported in the **[edit system services dhcp-local-server dhcpv6]** hierarchy level.

<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
---------------------------------	---

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Extended DHCP Local Server Overview on page 98</li><li>• Overriding Default DHCP Local Server Configuration Settings on page 115</li><li>• Deleting DHCP Local Server and DHCP Relay Override Settings on page 122</li></ul>
------------------------------	--

## overrides (DHCP Relay Agent)

<b>Syntax</b>	<pre> overrides {     allow-snooped-clients;     always-write-giaddr;     always-write-option-82;     client-discover-match &lt;option60-and-option82&gt;;     disable-relay;     interface-client-limit <i>number</i>;     layer2-unicast-replies;     no-allow-snooped-clients;     no-arp;     no-bind-on-request;     proxy-mode;     replace-ip-source-with;     send-release-on-delete;     trust-option-82; } </pre>
<b>Hierarchy Level</b>	<pre> [edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay group <i>group-name</i>], [edit forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay], [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> forwarding-options dhcp-relay group <i>group-name</i>  interface <i>interface-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 logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>  forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-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>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group  <i>group-name</i> interface <i>interface-name</i>] </pre>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	<p>Override the default configuration settings for the extended DHCP relay agent. Specifying the <b>overrides</b> statement with no subordinate statements removes all DHCP relay agent overrides at that hierarchy level.</p> <ul style="list-style-type: none"> <li>To override global DHCP relay configuration options, include the <b>overrides</b> statement and its subordinate statements at the <b>[edit forwarding-options dhcp-relay]</b> hierarchy level.</li> <li>To override configuration options for a named group of interfaces, include the statements at the <b>[edit forwarding-options dhcp-relay group <i>group-name</i>]</b> hierarchy level.</li> </ul>

- To override configuration options for a specific interface within a named group of interfaces, include the statements at the **[edit forwarding-options dhcp-relay group *group-name* interface *interface-name*]** hierarchy level.

The remaining statements are explained separately.

<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Extended DHCP Relay Agent Overview on page 154</li><li>• Overriding the Default DHCP Relay Configuration Settings on page 168</li><li>• Deleting DHCP Local Server and DHCP Relay Override Settings on page 122</li></ul>

---

## packet-triggered-subscribers

---

**Syntax**

```
packet-triggered-subscribers {  
  partition partition-name {  
    destination-host hostname;  
    destination-realm realm;  
    diameter-instance instance-name;  
  }  
  traceoptions {  
    file filename <files number> <match regular-expression > <size maximum-file-size>  
      <world-readable | no-world-readable>;  
    flag flag <disable>;  
    no-remote-trace;  
  }  
}
```

**Hierarchy Level** [edit system services]

**Release Information** Statement introduced in Junos OS Release 10.2.

**Description** Configure PTSP to interact with an SAE in an SRC environment to provision packet-triggered subscribers.

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 Documentation**

- Configuring the PTSP Partition on page 312



## packet-triggered-subscribers-partition

---

<b>Syntax</b>	<code>packet-triggered-subscribers-partition <i>partition-name</i>;</code>
<b>Hierarchy Level</b>	[edit system]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify the PTSP partition to associate with the logical system and routing instance.
<b>Options</b>	<b><i>partition-name</i></b> —Name of the PTSP partition that you want PTSP to use. The name is defined with the <b>partition</b> statement at the [edit system services packet-triggered-subscribers] hierarchy level.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Assigning the PTSP Partition on page 312</li> </ul>

## padn (Domain Maps)

---

<b>Syntax</b>	<code>padn <i>destination-address</i> {     <i>mask destination-mask</i>;     <i>metric route-metric</i>; }</code>
<b>Hierarchy Level</b>	[edit access domain map <i>domain-map-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Configure PADN parameters for a domain map.
<b>Options</b>	<b><i>destination-address</i></b> —IP address of the destination.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring PADN Parameters for a Domain Map on page 89</li> </ul>

## pap (Dynamic PPP)

---

<b>Syntax</b>	pap;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" ppp-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Specify PAP authentication in a PPP dynamic profile.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Dynamic Profiles Overview on page 369</li><li>• Configuring Dynamic Authentication for PPP Subscribers on page 219</li><li>• Attaching Dynamic Profiles to Static PPP Subscriber Interfaces on page 223</li></ul>

## parse-direction (Domain Maps)

---

<b>Syntax</b>	parse-direction (left-to-right   right-to-left);
<b>Hierarchy Level</b>	[edit access domain]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the direction in which the router searches for the domain name in a username.
<b>Default</b>	right-to-left
<b>Options</b>	<p><b>left-to-right</b>—The router searches starting at the left-most character. When the router reaches a domain delimiter, it uses anything to the right of the delimiter as the domain name.</p> <p><b>right-to-left</b>—The router searches starting at the right-most character. When the router reaches a domain delimiter, it uses anything to the right of the delimiter as the domain name.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Specifying the Parsing Direction for Domain Names on page 87</li><li>• Configuring Domain Name Usage for Domain Maps on page 86</li></ul>

## partition

---

<b>Syntax</b>	<pre>partition <i>partition-name</i> {     diameter-instance <i>instance-name</i>;     destination-host <i>hostname</i>;     destination-realm <i>realm</i>; }</pre>
<b>Hierarchy Level</b>	[edit jsrsrc]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Configure a JSRC partition.
<b>Options</b>	<p><b><i>partition-name</i></b>—Name of the JSRC partition.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring JSRC on page 279</li> <li>Configuring the JSRC Partition on page 280</li> </ul>

## partition (Gx-Plus)

---


<b>Syntax</b>	<pre>partition <i>partition-name</i> {     diameter-instance <i>instance-name</i>;     destination-host <i>hostname</i>;     destination-realm <i>realm</i>; }</pre>
<b>Hierarchy Level</b>	[edit access gx-plus]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Configure a Gx-Plus partition.
<b>Options</b>	<p><b><i>partition-name</i></b>—Name of the Gx-Plus partition.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Gx-Plus on page 339</li> <li>Configuring the Gx-Plus Partition on page 340</li> </ul>

## partition (PTSP)

---


<b>Syntax</b>	<pre>partition <i>partition-name</i> {     destination-host <i>hostname</i>;     destination-realm <i>realm</i>;     diameter-instance <i>instance-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit system services packet-triggered-subscribers]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Configure a PTSP partition.
<b>Options</b>	<p><i>partition-name</i>—Name of the PTSP partition.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring the PTSP Partition on page 312</li></ul>

## passive (Dynamic IGMP Interface)

<b>Syntax</b>	<code>passive &lt;allow-receive&gt; &lt;send-general-query&gt; &lt;send-group-query&gt;;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6. <b>allow-receive</b> , <b>send-general-query</b> , and <b>send-group-query</b> options were introduced in Junos OS Release 10.0.
<b>Description</b>	Dynamically specify that IGMP run on the interface and either not send and receive control traffic or selectively send and receive control traffic such as IGMP reports, queries, and leaves.
<div>  <p><b>NOTE:</b> You can selectively activate up to two out of the three available options for the <b>passive</b> statement while keeping the other functions passive (inactive). Activating all three options would be equivalent to not using the <b>passive</b> statement.</p> </div>	
<b>Options</b>	<p><b>allow-receive</b>—Enables IGMP to receive control traffic on the interface.</p> <p><b>send-general-query</b>—Enables IGMP to send general queries on the interface.</p> <p><b>send-group-query</b>—Enables IGMP to send group-specific and group-source-specific queries on the interface.</p>
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Example: Configuring Multicast with Subscriber VLANs</li> <li>For general information about configuring IGMP, see the <a href="#">Junos OS Multicast Protocols Configuration Guide</a>.</li> </ul>

## passive (Dynamic MLD Interface)

---

<b>Syntax</b>	<code>passive;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols mld interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Specify that MLD run on the interface and either not send and receive control traffic or selectively send and receive control traffic such as MLD reports, queries, and leaves.
	<div><p><b>NOTE:</b> You can selectively activate up to two out of the three available options for the <code>passive</code> statement while keeping the other functions <code>passive</code> (inactive). Activating all three options would be equivalent to not using the <code>passive</code> statement.</p></div>
<b>Options</b>	<p><code>allow-receive</code>—Enables IGMP to receive control traffic on the interface.</p> <p><code>send-general-query</code>—Enables IGMP to send general queries on the interface.</p> <p><code>send-group-query</code>—Enables IGMP to send group-specific and group-source-specific queries on the interface.</p>
<b>Required Privilege Level</b>	<p><code>routing</code>—To view this statement in the configuration.</p> <p><code>routing-control</code>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Example: Configuring Multicast with Subscriber VLANs</li></ul>

## password (DHCP Local Server)

<b>Syntax</b>	<code>password password-string;</code>
<b>Hierarchy Level</b>	<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 dhcpv6 authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 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 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 dhcpv6 authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> 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 dhcpv6 authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 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 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 dhcpv6 authentication],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> 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 dhcpv6],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Configure the password that is sent to the external AAA authentication server for subscriber authentication.
<b>Options</b>	<i>password-string</i> —Authentication password.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Using External AAA Authentication Services with DHCP on page 110</li> </ul>

## password (DHCP Relay Agent)

---

<b>Syntax</b>	<code>password password-string;</code>
<b>Hierarchy Level</b>	<code>[edit forwarding-options dhcp-relay authentication],</code> <code>[edit forwarding-options dhcp-relay group group-name authentication],</code> <code>[edit logical-systems logical-system-name forwarding-options dhcp-relay authentication],</code> <code>[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name authentication],</code> <code>[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay authentication],</code> <code>[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication],</code> <code>[edit routing-instances routing-instance-name forwarding-options dhcp-relay authentication],</code> <code>[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Configure the password that is sent to the external AAA authentication server for subscriber authentication.
<b>Options</b>	<i>password-string</i> —Authentication password.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Using External AAA Authentication Services with DHCP on page 110</li></ul>



## password (Static Subscribers)

<b>Syntax</b>	<pre>password password-string;   username-include {     domain-name domain-name;     username-include;     logical-system-name;     routing-instance-name;     user-prefix user-prefix-string;   }</pre>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i> authentication],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers authentication],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication username-include], authentication],</p> <p>[edit system services static-subscribers authentication]</p> <p>[edit system services static-subscribers group <i>group-name</i> authentication]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify the password that is sent to AAA for user login for all static subscribers on interfaces configured at the [edit system services static-subscribers interface] hierarchy level, or for the subscribers in a specified group. The group version of the statement takes precedence over the global version.
<b>Options</b>	<p><b>password-string</b>—String that defines the password.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>system-level—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Subscribers over Static Interfaces on page 288</li> <li>Configuring the Static Subscriber Global Authentication Password on page 290</li> <li>Configuring the Static Subscriber Group Authentication Password on page 294</li> </ul>

## peer

---

<b>Syntax</b>	<pre>peer {   (ip-address <i>address</i>   nai <i>name@domain</i>) {     spi <i>hexadecimal-value</i> {       algorithm (hmac-md5   md5);       entity-type (host   mobility-agent);       key (hex   ascii) <i>string</i>;       replay-method (timestamp <i>seconds</i>   none);     }   } }</pre>
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> services <b>mobile-ip</b> ], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services <b>mobile-ip</b> ], [edit routing-instances <i>routing-instances-name</i> services <b>mobile-ip</b> ], [edit services <b>mobile-ip</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.
<b>Description</b>	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.
<b>Options</b>	<p><b>ip-address <i>address</i></b>—IP address of the peer.</p> <p><b>nai <i>name@domain</i></b>—Network address identifier (NAI) of the peer. The <i>name</i> can include only alphanumeric characters, dots, hyphens, or underscores. The <i>name</i> cannot end in @; @ must be used to separate <i>name</i> and <i>domain</i>. The <i>domain</i> can include only alphanumeric characters, dots, or hyphens. The <i>domain</i> must be in the format <i>domain.suffix</i>, where the <i>suffix</i> is com, org, net, and so on. The <i>suffix</i> must consist of at least two alphanumeric characters.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Mobile IP on page 357</li><li>Configuring the Mobile IP Home Agent on page 358</li></ul>

## peer (Diameter Base Protocol)

<b>Syntax</b>	<pre>peer <i>peer-name</i> {     address <i>ip-address</i>;     connect-actively {         port <i>port-number</i>;         transport <i>transport-name</i>;     }     logical-system <i>logical-system-name</i> &lt;routing-instance <i>routing-instance-name</i>&gt;;     routing-instance <i>routing-instance-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit diameter]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	<p>Configure a remote peer for the Diameter instance.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Diameter on page 259</li> <li>Configuring Diameter Peers on page 260</li> </ul>

## peer (Diameter Network Element)

<b>Syntax</b>	<pre>peer <i>peer-name</i> {     priority <i>priority-value</i>; }</pre>
<b>Hierarchy Level</b>	[edit diameter network-element <i>element-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Define and prioritize a peer associated with a Diameter network element.
<b>Options</b>	<p><i>peer-name</i>—Name of the peer.</p> <p>The remaining statement is explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Diameter on page 259</li> <li>Configuring Diameter Network Elements on page 261</li> </ul>

## pool (Address-Assignment Pools)

---

<b>Syntax</b>	<pre>pool <i>pool-name</i> {     family <i>family</i> {         dhcp-attributes {             [ <i>protocol-specific attributes</i> ]         }         host <i>hostname</i> {             hardware-address <i>mac-address</i>;             ip-address <i>ip-address</i>;         }         network <i>ip-prefix</i>/<i>&lt;prefix-length&gt;</i>;         prefix <i>ipv6-prefix</i>;         range <i>range-name</i> {             high <i>upper-limit</i>;             low <i>lower-limit</i>;             prefix-length <i>prefix-length</i>;         }     }     link <i>pool-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit access address-assignment]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Configure the name of an address-assignment pool.
<b>Options</b>	<p><i>pool-name</i>—Name assigned to the address-assignment pool.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Address-Assignment Pools Overview on page 67</li><li>• Configuring Address-Assignment Pools on page 68</li></ul>

## pool-match-order

<b>Syntax</b>	pool-match-order { external-authority; ip-address-first; option-82; }
<b>Hierarchy Level</b>	[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]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	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.  The remaining statements are explained separately.
<b>Default</b>	DHCP local server uses the <b>ip-address-first</b> method to determine which address pool to use.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 111</li> <li>Extended DHCP Local Server Overview on page 98</li> </ul>

## pop (Dynamic VLANs)

<b>Syntax</b>	pop;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	For dynamic VLAN interfaces, specify the VLAN rewrite operation to remove a VLAN tag from the top of the VLAN tag stack. The outer VLAN tag of the frame is removed.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Removing a VLAN Tag</li> <li>Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution</li> </ul>

## port

---

<b>Syntax</b>	<code>port <i>port-number</i>;</code>
<b>Hierarchy Level</b>	[edit access radius-server <i>server-address</i> ], [edit access profile <i>profile-name</i> radius-server <i>server-address</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure the port number on which to contact the RADIUS server.
<b>Options</b>	<i>port-number</i> —Port number on which to contact the RADIUS server. <b>Default:</b> 1812 (as specified in RFC 2865)
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Router or Switch Interaction with RADIUS Servers on page 20</li><li>Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li></ul>

## port (Diameter Peer)

---

<b>Syntax</b>	<code>port <i>port-number</i>;</code>
<b>Hierarchy Level</b>	[edit diameter peer <i>peer-name</i> connect-actively]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify the destination TCP port used by the active connection to peer.
<b>Options</b>	<i>port-number</i> —Number of the TCP port. <b>Default:</b> 3868
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Diameter on page 259</li><li>Configuring Diameter Peers on page 260</li></ul>

## post-service-filter (Dynamic Service Sets)

<b>Syntax</b>	<code>post-service-filter <i>filter-name</i>;</code>
<b>Hierarchy Level</b>	<p>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> service input],</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit “\$junos-interface-unit” family <i>family</i> service input]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.5.</p> <p>Support at the [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit “\$junos-interface-unit” family <i>family</i> service input] hierarchy level introduced in Junos OS Release 10.1.</p>
<b>Description</b>	<p>Define the filter to be applied to traffic after service processing. The filter is applied only if a service set is configured and selected. You can configure a postservice filter on the input side of the interface only. Only the Internet Protocol version 4 (IPv4) protocol family is currently supported for dynamic PPPoE logical interfaces.</p>
<b>Options</b>	<i>filter-name</i> —Identifier for the post-service filter.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Dynamic Service Sets Overview on page 569</li> <li>Associating Service Sets with Interfaces in a Dynamic Profile on page 595</li> </ul>

## pp0 (Dynamic PPPoE)

```
Syntax  pp0 {
        unit logical-unit-number {
            keepalives interval seconds;
            no-keepalives;
            pppoe-options {
                underlying-interface interface-name;
                server;
            }
            ppp-options {
                chap;
                pap;
            }
            family inet {
                unnumbered-address interface-name destination address;
                address address;
                service {
                    input {
                        service-set service-set-name {
                            service-filter filter-name;
                        }
                        post-service-filter filter-name;
                    }
                    output {
                        service-set service-set-name {
                            service-filter filter-name;
                        }
                    }
                }
            }
            filter {
                input filter-name {
                    precedence precedence;
                }
                output filter-name {
                    precedence precedence;
                }
            }
        }
    }
```

**Hierarchy Level** [edit dynamic-profiles *profile-name* interfaces]

**Release Information** Statement introduced in Junos OS Release 10.1.

**Description** Configure the dynamic PPPoE logical interface in a dynamic profile. When the router creates a dynamic PPPoE logical interface on an underlying Ethernet interface configured with PPPoE (**ppp-over-ether**) encapsulation, it uses the information in the dynamic profile to determine the properties of the dynamic PPPoE logical interface.

The remaining statements are explained separately.



<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring a Basic PPPoE Dynamic Profile on page 536</li><li>• Configuring a PPPoE Dynamic Profile with Additional Options on page 539</li><li>• For information about creating static PPPoE interfaces, see Configuring PPPoE</li></ul>

---

## pppoe-options (Dynamic PPPoE)

---

<b>Syntax</b>	<pre>pppoe-options {     underlying-interface <i>interface-name</i>;     server; }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit"]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	<p>Configure the underlying interface and PPPoE server mode for a dynamic PPPoE logical interface in a dynamic profile.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring a Basic PPPoE Dynamic Profile on page 536</li><li>• For information about creating static PPPoE interfaces, see the <a href="#">Junos OS Network Interfaces Configuration Guide</a></li></ul>

## pppoe-underlying-options (Static and Dynamic Subscribers)

---

<b>Syntax</b>	<pre>pppoe-underlying-options {     access-concentrator <i>name</i>;     dynamic-profile <i>profile-name</i>;     duplicate-protection;     max-sessions <i>number</i>;     service-name-table <i>table-name</i>; }</pre>
<b>Hierarchy Level</b>	[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> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	<p>Configure PPPoE-specific interface properties for the underlying interface on which the router creates a static or dynamic PPPoE logical interface. The underlying interface must be configured with PPPoE (<b>ppp-over-ether</b>) encapsulation.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring PPPoE (for static interfaces)</li><li>Configuring an Underlying Interface for Dynamic PPPoE Subscriber Interfaces on page 541</li><li>Assigning a Service Name Table to a PPPoE Underlying Interface</li></ul>


## ppp-options (Dynamic PPP)

---

<b>Syntax</b>	<pre>ppp-options {     chap;     pap; }</pre>
<b>Hierarchy Level</b>	[edit <b>dynamic-profiles</b> <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit"]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	<p>Configure PPP-specific interface properties in a dynamic profile.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Dynamic Profiles Overview on page 369</a></li><li>• <a href="#">Configuring Dynamic Authentication for PPP Subscribers on page 219</a></li><li>• <a href="#">Attaching Dynamic Profiles to Static PPP Subscriber Interfaces on page 223</a></li></ul>

## ppp-subscriber-services

---

<b>Syntax</b>	ppp-subscriber-services (disable   enable);
<b>Hierarchy Level</b>	[edit chassis]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Enable dynamic PPP subscriber services on non-PPPoE interfaces on certain PICs.
	<div><p><b>NOTE:</b> When you include this statement, the relevant PICs restart. This action disrupts subscribers already logged in through those PICs. You can confirm completion of the restart by issuing the <code>show chassis pic fpc-slot slot-number pic-slot slot-number</code> command.</p></div>
<b>Options</b>	<p><b>disable</b>—Disable subscriber services.</p> <p><b>enable</b>—Enable subscriber services.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• show chassis pic</li><li>• Attaching Dynamic Profiles to MLPPP Bundles on page 227</li><li>• For hardware requirements, see Hardware Requirements for PPP Subscriber Services on Non-Ethernet Interfaces on page 226</li></ul>

## precedence

<b>Syntax</b>	<code>precedence <i>precedence</i>;</code>
<b>Hierarchy Level</b>	<p>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> filter input <i>filter-name</i>],</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> filter output <i>filter-name</i>],</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family <i>family</i> filter input <i>filter-name</i>],</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family <i>family</i> filter output <i>filter-name</i>],</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i> filter input <i>filter-name</i>],</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i> filter output <i>filter-name</i>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3.</p> <p>The [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family inet filter input <i>filter-name</i>] hierarchy level and [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family inet filter output <i>filter-name</i>] hierarchy level introduced in Junos OS Release 10.1.</p>
<b>Description</b>	Apply a precedence to a dynamic filter. Only the Internet Protocol version 4 (IPv4) protocol family is currently supported for dynamic PPPoE logical interfaces.
<b>Options</b>	<p><b><i>precedence</i></b>—Precedence value for the filter. The lower the precedence value, the higher the precedence.</p> <p><b>Range:</b> 0 through 250</p> <p><b>Default:</b> 0</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>For general information about configuring firewall filters, see the <a href="#">Junos OS Routing Policy Configuration Guide</a></li> <li>Dynamic Firewall Filters Overview on page 555</li> <li>Classic Filters Overview on page 556</li> <li>Fast Update Filters Overview on page 564</li> <li>Basic Classic Filter Syntax on page 558</li> <li>Basic Fast Update Filter Syntax on page 567</li> </ul>

## predefined-variable-defaults (Dynamic Profiles)

---

<b>Syntax</b>	<code>predefined-variable-defaults predefined-variable &lt;variable-option&gt; default-value</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles profile-name]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Configure default values for the predefined variables that are configured in a dynamic profile. These default values are used when RADIUS does not supply a value.
<b>Options</b>	<p><b><i>predefined-variable</i></b>—Name of the predefined variable to which you want to assign a default value. Do not include the junos prefix.</p> <p><b><i>variable-option</i></b>—Name of the specific variable option to which you want to assign a default value. Only certain predefined variables support multiple default values.</p> <p><b><i>default-value</i></b>—Default value that you want to assign to the predefined variable.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Default Values for Predefined Variables in a Dynamic Profile on page 393</li></ul>

## preference

---

<b>Syntax</b>	<code>preference route-distance;</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles routing-options access route prefix]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Dynamically configure the distance for an access route.
<b>Options</b>	<p><b><i>route-distance</i></b>—Either the specific distance you want to assign to the access route or the distance variable (<code>\$junos-framed-route-distance</code>). The distance variable is dynamically replaced with the value in Framed-Route Attribute [22].</p>
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Dynamic Access Routes for Subscriber Management on page 206</li></ul>

## preference (Tunnel Profile)

<b>Syntax</b>	<code>preference <i>number</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	<p>Specify the preference for a tunnel. You can specify up to 8 levels of preference, and you can assign the same preference to a maximum of 31 tunnels. When you define multiple preferences for a destination, you increase the probability of a successful connection.</p> <p>This value can be overridden by RADIUS attribute Tunnel-Preference [83].</p>
<b>Options</b>	<p><b><i>number</i></b>—Number that indicates the order in which the router attempts to connect to the destination. Zero is the highest level of preference.</p> <p><b>Range:</b> 0 through 2000</p> <p><b>Default:</b> 2000</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring a Tunnel Profile for Subscriber Access on page 242</li> </ul>

## preferred-lifetime (Dynamic Router Advertisement)

<b>Syntax</b>	<code>preferred-lifetime <i>seconds</i>;</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> protocols router-advertisement interface <i>interface-name</i> prefix <i>prefix</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Specify how long the prefix generated by stateless autoconfiguration remains preferred.
<b>Options</b>	<p><b><i>seconds</i></b>—Preferred lifetime, in seconds. If you set the preferred lifetime to <code>0xffffffff</code>, the lifetime is infinite. The preferred lifetime is never greater than the valid lifetime.</p> <p><b>Default:</b> 604,800 seconds</p>
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>valid-lifetime</li> <li>Configuring the Prefix Information Included in Neighbor Discovery Advertisements</li> </ul>

## prefix (Address-Assignment Pools)

---

<b>Syntax</b>	<code>prefix <i>ipv6-prefix</i>;</code>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family inet6]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Specify the IPv6 prefix for the IPv6 address-assignment pool. This statement is mandatory for IPv6 address-assignment pools.
<b>Options</b>	<i>ipv6-prefix</i> —IPv6 prefix.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Address-Assignment Pools Overview on page 67</li><li>Configuring Address-Assignment Pools on page 68</li></ul>



## prefix (DHCP Relay Agent)

<b>Syntax</b>	<code>prefix <i>prefix</i>;</code>
<b>Hierarchy Level</b>	<p>[edit forwarding-options dhcp-relay relay-option-82 circuit-id],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-82 circuit-id],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay relay-option-82 circuit-id],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-82 circuit-id],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-82 circuit-id],</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-82 circuit-id],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-82 circuit-id],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-82 circuit-id]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	<p>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.</p> <p>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:</p> <pre> 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 </pre> <p>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:</p> <pre> logical-system-name;routing-instance-name:(fe   ge)-fpc/pic/port:svlan-id-vlan-id </pre> <p>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:</p> <pre> host-name/logical-system-name;routing-instance-name:(fe   ge)-fpc/pic/port:svlan-id-vlan-id </pre> <p>For Fast Ethernet or Gigabit Ethernet interfaces that use virtual LANs (VLANs) but not S-VLANs, only the <b>vlan-id</b> 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 <b>vlan-id</b> value nor the <b>svlan-id</b> value appears.</p>
<b>Options</b>	<i>prefix</i> —Any combination of the following:

- **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 Documentation**

- Enabling and Disabling Insertion of Option 82 Information on page 192
- Configuring an Option 82 Prefix on page 193

---

## prefix (Dynamic Router Advertisement)

---

**Syntax** `prefix prefix {  
    (autonomous | no-autonomous);  
    (on-link | no-on-link);  
    preferred-lifetime seconds;  
    valid-lifetime seconds;  
}`

**Hierarchy Level** [edit dynamic-profiles protocols router-advertisement interface *interface-name*]

**Release Information** Statement introduced in Junos OS Release 10.1.

**Description** Configure the prefix name in router advertisement messages.

**Options** *prefix*—Prefix name. For dynamic configuration, specify the *\$junos-ipv6-ndra-prefix* dynamic variable.

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 Documentation**

- Configuring the Prefix Information Included in Neighbor Discovery Advertisements

## pre-ietf-mode

---

<b>Syntax</b>	<code>pre-ietf-mode</code>
<b>Hierarchy Level</b>	<code>[edit protocols anc],</code> <code>[edit protocols anc neighbor]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
<b>Description</b>	Configure ANCP to run in a mode that is backward compatible with Internet draft draft-ietf-ancp-protocol-00.txt, <i>Protocol for Access Node Control Mechanism in Broadband Networks</i> for all neighbors or for a specific neighbor.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring ANCP on page 786</li><li>• Configuring ANCP for Backward Compatibility on page 789</li><li>• Configuring ANCP Neighbors on page 786</li></ul>

## priority (Diameter Peer)

---

<b>Syntax</b>	<code>priority <i>priority-value</i>;</code>
<b>Hierarchy Level</b>	<code>[edit diameter network-element <i>element-name</i> peer <i>peer-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Set the priority for a peer within a Diameter network element. A peer with a lower number has a higher priority.
<b>Options</b>	<b><i>priority-value</i></b> —Priority for the peer within the network element. <b>Range:</b> 1 through 65535
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Diameter on page 259</li><li>• Configuring Diameter Network Elements on page 261</li></ul>

## priority (Dynamic Schedulers)

---

<b>Syntax</b>	<code>priority (<i>priority-level</i>   <code>\$junos-cos-scheduler-priority</code>);</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. The <code>\$junos-cos-scheduler-bs</code> predefined variable introduced in Junos OS Release 9.4.
<b>Description</b>	Specify packet-scheduling priority value in a dynamic profile.
<b>Options</b>	<p><i>priority-level</i>—one of the following packet-scheduling priority values:</p> <ul style="list-style-type: none"><li>• <b>low</b>—Scheduler has low priority.</li><li>• <b>medium-low</b>—Scheduler has medium-low priority.</li><li>• <b>medium-high</b>—Scheduler has medium-high priority.</li><li>• <b>high</b>—Scheduler has high priority. Assigning high priority to a queue prevents the queue from being underserved.</li><li>• <b>strict-high</b>—Scheduler has strictly high priority. Configure a <b>high</b> priority queue with unlimited transmission bandwidth available to it. As long as it has traffic to send, the <b>strict-high</b> priority queue receives precedence over <b>low</b>, <b>medium-low</b>, and <b>medium-high</b> priority queues, but not <b>high</b> priority queues. You can configure <b>strict-high</b> priority on only one queue per interface.</li></ul> <p><code>\$junos-cos-scheduler-pri</code>—Junos predefined variable that is replaced with the packet-scheduling priority value obtained from the RADIUS server when a subscriber authenticates over the interface to which the dynamic profile is attached.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>• Configuring Schedulers in a Dynamic Profile for Subscriber Access on page 679</li><li>• Dynamic Variables Overview on page 371</li><li>• <b>scheduler (Dynamic Scheduler Maps) on page 1174</b></li></ul>

## profile

```
Syntax  profile profile-name {
        accounting {
            accounting-stop-on-access-deny;
            accounting-stop-on-failure;
            coa-immediate-update;
            immediate-update;
            order [ accounting-method ];
            statistics (time | volume-time);
            update-interval minutes;
        }
        authentication-order [ authentication-methods ];
        client client-name {
            chap-secret chap-secret;
            group-profile profile-name;
            ike {
                allowed-proxy-pair {
                    remote remote-proxy-address local local-proxy-address;
                }
                pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
                ike-policy policy-name;
                interface-id string-value;
            }
            l2tp {
                interface-id interface-id;
                lcp-renegotiation;
                local-chap;
                maximum-sessions-per-tunnel number;
                multilink {
                    drop-timeout milliseconds;
                    fragment-threshold bytes;
                }
                ppp-authentication (chap | pap);
                ppp-profile profile-name;
                shared-secret shared-secret;
            }
            pap-password pap-password;
            ppp {
                cell-overhead;
                encapsulation-overhead bytes;
                framed-ip-address ip-address;
                framed-pool framed-pool;
                idle-timeout seconds;
                interface-id interface-id;
                keepalive seconds;
                primary-dns primary-dns;
                primary-wins primary-wins;
                secondary-dns secondary-dns;
                secondary-wins secondary-wins;
            }
            user-group-profile profile-name;
        }
        radius {
```

```
accounting-server [ ip-address ];
authentication-server [ ip-address ];
options {
  accounting-session-id-format (decimal | description);
  client-accounting-algorithm (direct | round-robin);
  client-authentication-algorithm (direct | round-robin);
  ethernet-port-type-virtual;
  interface-description-format {
    exclude-adapter;
    exclude-sub-interface;
  }
  nas-identifier identifier-value;
  nas-port-extended-format {
    adapter-width width;
    port-width width;
    slot-width width;
    stacked-vlan-width width;
    vlan-width width;
  }
  revert-interval interval;
  vlan-nas-port-stacked-format;
}
attributes {
  exclude {
    accounting-authentic [ accounting-on | accounting-off ];
    accounting-delay-time [ accounting-on | accounting-off ];
    accounting-session-id [ access-request | accounting-on | accounting-off |
      accounting-stop ];
    accounting-terminate-cause [ accounting-off ];
    called-station-id [ access-request | accounting-start | accounting-stop ];
    calling-station-id [ access-request | accounting-start | accounting-stop ];
    class [ accounting-start | accounting-stop ];
    dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
    dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
    event-timestamp [ accounting-on | accounting-off | accounting-start |
      accounting-stop ];
    framed-ip-address [ accounting-start | accounting-stop ];
    framed-ip-netmask [ accounting-start | accounting-stop ];
    input-filter [ accounting-start | accounting-stop ];
    input-gigapackets [ accounting-stop ];
    input-gigawords [ accounting-stop ];
    interface-description [ access-request | accounting-start | accounting-stop ];
    nas-identifier [ access-request | accounting-on | accounting-off | accounting-start
      | accounting-stop ];
    nas-port [ access-request | accounting-start | accounting-stop ];
    nas-port-id [ access-request | accounting-start | accounting-stop ];
    nas-port-type [ access-request | accounting-start | accounting-stop ];
    output-filter [ accounting-start | accounting-stop ];
    output-gigapackets [ accounting-stop ];
    output-gigawords [ accounting-stop ];
  }
  ignore {
    framed-ip-netmask;
    input-filter;
    logical-system::routing-instance;
    output-filter;
```

```

    }
  }
}
radius-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]

**Release Information** Statement introduced before Junos OS Release 7.4.

**Description** Configure PPP CHAP, or a profile and its subscriber access, L2TP, or PPP properties.

**Options** *profile-name*—Name of the profile.

For CHAP, the name serves as the mapping between peer identifiers and CHAP secret keys. This entity is queried for the secret key whenever a CHAP challenge or response is received.

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 Documentation**

- Configuring the PPP Authentication Protocol
- Configuring Access Profiles for L2TP or PPP Parameters
- Configuring L2TP Properties for a Client-Specific Profile
- Configuring PPP Properties for a Client-Specific Profile
- AAA Service Framework Overview on page 18


## promiscuous-mode

---

<b>Syntax</b>	<code>promiscuous-mode;</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify that the interface accepts IGMP reports from hosts on any subnetwork.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Dynamic Profile for Client Access on page 395</li><li>For information about how to use IGMP promiscuous mode, see “Accepting IGMP Messages from Remote Subnetworks” in the <a href="#">Junos OS Multicast Protocols Configuration Guide</a></li></ul>

## protocol (Dynamic Schedulers)

---

<b>Syntax</b>	<code>protocol (any   non-tcp   tcp);</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i> drop-profile-map]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify the protocol type for the specified scheduler in a dynamic profile.
<b>Options</b>	<p><b>any</b>—Accept any protocol type.</p> <p><b>non-tcp</b>—Accept any protocol type other than TCP/IP.</p> <p><b>tcp</b>—Accept only TCP/IP protocol.</p>
<div> <b>NOTE:</b> Protocol types <b>non-tcp</b> and <b>tcp</b> are not supported on MX Series routers.</div>	
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>Configuring Schedulers in a Dynamic Profile for Subscriber Access on page 679</li></ul>



## protocols (Dynamic Profiles)

```
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;
        }
    }
    mld {
        interface interface-name {
            disable;
            (accounting | no-accounting);
            group-policy;
            immediate-leave;
            oif-map;
            passive;
            ssm-map ssm-map-name;
            static {
                group multicast-group-address {
                    exclude;
                    group-count number;
                    group-increment increment;
                    source ip-address {
                        source-count number;
                        source-increment increment;
                    }
                }
            }
            version version;
        }
    }
    router-advertisement {
        interface interface-name {
            current-hop-limit number;
            default-lifetime seconds;
            (managed-configuration | no-managed-configuration);
            max-advertisement-interval seconds;
            min-advertisement-interval seconds;
            (other-stateful-configuration | no-other-stateful-configuration);
            prefix prefix;
            reachable-time milliseconds;
            retransmit-timer milliseconds;
        }
    }
}
```

```
    }  
  }  
}
```

**Hierarchy Level** [edit dynamic-profiles *profile-name*]

**Release Information** Statement introduced in Junos OS Release 9.2.  
Support at the [edit dynamic-profiles *profile-name* protocols mld] and [edit dynamic-profiles *profile-name* protocols router-advertisement] hierarchy levels introduced in Junos OS Release 10.1.

**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).

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 Documentation**

- For general information about configuring IGMP or MLD, see the [Junos OS Multicast Protocols Configuration Guide](#).

## provisioning-order

<b>Syntax</b>	<code>provisioning-order (gx-plus   jsrc);</code>
<b>Hierarchy Level</b>	<code>[edit access profile <i>profile-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6. Support for Gx-Plus introduced in Junos OS Release 11.2.
<b>Description</b>	Configure AAA to use the specified application for subscriber service provisioning.
<b>Options</b>	<p><code>gx-plus</code>—Specify Gx-Plus as the application used to communicate with a PCRF for subscriber service provisioning.</p> <p><code>jsrc</code>—Specify JSRC as the application used to communicate with the SAE for subscriber service provisioning. JSRC is used in an SRC environment to request services from the SAE for an authenticated subscriber. JSRC attempts to activate these services. If successful, JSRC returns an ACK message. If unsuccessful, the subscriber is denied access.</p>
<b>Required Privilege Level</b>	<p><code>admin</code>—To view this statement in the configuration.</p> <p><code>admin-control</code>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring JSRC on page 279</li> <li>Provisioning Subscribers with JSRC on page 282</li> <li>Configuring Gx-Plus on page 339</li> <li>Provisioning Subscribers with Gx-Plus on page 341</li> </ul>

## proxy-arp

<b>Syntax</b>	<code>proxy-arp;</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	For Ethernet interfaces only, configure the router to respond to any ARP request, as long as the router has an active route to the target address of the ARP request.
<b>Required Privilege Level</b>	<p><code>interface</code>—To view this statement in the configuration.</p> <p><code>interface-control</code>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Unrestricted Proxy ARP</li> <li>Configuring Gratuitous ARP</li> </ul>

## proxy-mode

---

<b>Syntax</b>	proxy-mode;
<b>Hierarchy Level</b>	[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] [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	<p>Enable DHCP relay proxy mode on the extended DHCP relay. Proxy mode supports all extended DHCP relay functionality.</p> <p>The extended DHCP relay proxy is not supported for the J Series routers DHCP server. Also, you cannot configure both the DHCP relay proxy and the extended DHCP local server on the same interface.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• DHCP Relay Proxy Overview on page 156</li><li>• Extended DHCP Relay Agent Overview on page 154</li><li>• Enabling DHCP Relay Proxy Mode on page 196</li></ul>

## push (Dynamic VLANs)

<b>Syntax</b>	push;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	For dynamic VLAN interfaces, specify the VLAN rewrite operation to add a new VLAN tag to the top of the VLAN stack. An outer VLAN tag is pushed in front of the existing VLAN tag. If you include the <b>push</b> statement in the configuration, you must also include the pop statement at the [edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map] hierarchy level.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution</li> </ul>

## qos-adjust

<b>Syntax</b>	qos-adjust;
<b>Hierarchy Level</b>	[edit protocols ancp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
<b>Description</b>	Specify that CoS policy for interfaces and interface sets is adjusted according to ANCP protocol messages. Updates QoS adjustments for all subscribers.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring ANCP on page 786</li> <li>Configuring ANCP to Adjust CoS Traffic Shaping on page 790</li> </ul>

## qualified-next-hop

---

<b>Syntax</b>	<code>qualified-next-hop <i>interface-name</i> {     mac-address <i>address</i>; }</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles routing-options access-internal route <i>subscriber-ip-address</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Dynamically configure the qualified next-hop and the MAC address for an access-internal route for DHCP and PPP subscriber interfaces.
<b>Options</b>	<p><b><i>interface-name</i></b>—Either the specific interface you want to assign to the access route or the variable, or the <b>\$junos-interface-name</b> variable. The variable is dynamically replaced with the value supplied by DHCP or PPP when a subscriber logs in.</p> <p>The remaining statement is explained separately.</p>
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management on page 207</li></ul>

## radius (Access Profile)

```

Syntax  radius {
        accounting-server [ ip-address ];
        attributes {
            exclude
                accounting-authentic [ accounting-on | accounting-off ];
                accounting-delay-time [ accounting-on | accounting-off ];
                accounting-session-id [ access-request | accounting-on | accounting-off |
                    accounting-stop ];
                accounting-terminate-cause [ accounting-off ];
                called-station-id [ access-request | accounting-start | accounting-stop ];
                calling-station-id [ access-request | accounting-start | accounting-stop ];
                class [ accounting-start | accounting-stop ];
                dhcp-gi-address [ access-request | accounting-start | accounting-stop ];
                dhcp-mac-address [ access-request | accounting-start | accounting-stop ];
                event-timestamp [ accounting-on | accounting-off | accounting-start | accounting-stop
                ];
                framed-ip-address [ accounting-start | accounting-stop ];
                framed-ip-netmask [ accounting-start | accounting-stop ];
                input-filter [ accounting-start | accounting-stop ];
                input-gigapackets [ accounting-stop ];
                input-gigawords [ accounting-stop ];
                interface-description [ access-request | accounting-start | accounting-stop ];
                nas-identifier [ access-request | accounting-on | accounting-off | accounting-start |
                    accounting-stop ];
                nas-port [ access-request | accounting-start | accounting-stop ];
                nas-port-id [ access-request | accounting-start | accounting-stop ];
                nas-port-type [ access-request | accounting-start | accounting-stop ];
                output-filter [ accounting-start | accounting-stop ];
                output-gigapackets [ accounting-stop ];
                output-gigawords [ accounting-stop ];
        }
        ignore {
            framed-ip-netmask;
            input-filter;
            logical-system-routing-instance;
            output-filter;
        }
    }
    authentication-server [ ip-address ];
    options {
        accounting-session-id-format (decimal | description);
        client-accounting-algorithm (direct | round-robin);
        client-authentication-algorithm (direct | round-robin);
        ethernet-port-type-virtual;
        interface-description-format {
            exclude-adapter;
            exclude-sub-interface;
        }
        nas-identifier identifier-value;
        nas-port-extended-format {
            adapter-width width;
            port-width width;
    }

```

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

<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
<b>Description</b>	Configure the RADIUS parameters that the router uses for AAA authentication and accounting for subscribers.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring RADIUS Server Parameters for Subscriber Access on page 26</li><li>RADIUS Server Options for Subscriber Access on page 28</li></ul>

---

## radius (Dynamic Profiles)

---

```
Syntax  radius {  
        vendor-id id {  
            attribute attribute-number;  
            tag tag-number;  
        }  
    }  
}
```

<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> variables]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure RADIUS attribute variables in a dynamic profile.  The statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 698</li></ul>



## radius-disconnect (DHCP Local Server)

<b>Syntax</b>	radius-disconnect;
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure trigger],</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> reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure trigger],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure trigger],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure trigger],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure trigger],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure trigger],</p> <p>[edit system services dhcp-local-server reconfigure trigger],</p> <p>[edit system services dhcp-local-server dhcpv6 reconfigure trigger],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> reconfigure trigger],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure trigger]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
<b>Description</b>	Configure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces to be reconfigured when a RADIUS-initiated disconnect is received by the DHCP client or group of clients. A group configuration takes precedence over a DHCP local server configuration.
<b>Default</b>	The client is deleted when a RADIUS-initiated disconnect is received.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 133</li> <li>Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 136</li> </ul>

## radius-flow-tap

---

<b>Syntax</b>	<pre>radius-flow-tap {     forwarding-class <i>class-name</i>;     interfaces <i>interface-name</i>;     source-ipv4-address <i>ipv4-address</i>; }</pre>
<b>Hierarchy Level</b>	[edit services]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
<b>Description</b>	<p>Assign parameters that are used with subscriber secure policy mirroring.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>flow-tap—To view this statement in the configuration.</p> <p>flow-tap-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Subscriber Secure Policy Overview on page 625</li><li>Configuring RADIUS-Flow-Tap Service Support for Subscriber Secure Policy Mirroring on page 632</li></ul>

## radius-server

<b>Syntax</b>	<pre>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; }</pre>
<b>Hierarchy Level</b>	[edit access], [edit access profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	<p>Configure RADIUS for subscriber access management, L2TP, or PPP.</p> <p>To configure multiple RADIUS servers, include multiple <b>radius-server</b> 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.</p>
<b>Options</b>	<p><b>server-address</b>—Address of the RADIUS authentication server.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring RADIUS Authentication for L2TP</li> <li>Configuring the PPP Authentication Protocol</li> <li>Configuring RADIUS Authentication</li> <li>Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li> </ul>

## range (Address-Assignment Pools)

---

<b>Syntax</b>	<pre>range <i>range-name</i> {     high <i>upper-limit</i>;     low <i>lower-limit</i>;     prefix-length <i>prefix-length</i>; }</pre>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family (inet   inet6)]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0. IPv6 support introduced in Junos OS Release 10.0.
<b>Description</b>	Configure a named range of IPv4 addresses or IPv6 prefixes, used within an address-assignment pool.
<b>Options</b>	<p><b>high <i>upper-limit</i></b>—Upper limit of an address range or IPv6 prefix range.</p> <p><b>low <i>lower-limit</i></b>—Lower limit of an address range or IPv6 prefix range.</p> <p><b>prefix-length <i>prefix-length</i></b>—Assigned length of the IPv6 prefix.</p> <p><b><i>range-name</i></b>—Name assigned to the range of IPv4 addresses or IPv6 prefixes.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Address-Assignment Pools Overview on page 67</li><li>• Configuring Address-Assignment Pools on page 68</li></ul>

## reachable-time (Dynamic Router Advertisement)

<b>Syntax</b>	<code>reachable-time <i>milliseconds</i>;</code>
<b>Hierarchy Level</b>	[edit protocols router-advertisement interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Set the length of time that a node considers a neighbor reachable until another reachability confirmation is received from that neighbor.
<b>Options</b>	<p><i>milliseconds</i>—Reachability time limit.</p> <p><b>Range:</b> 0 through 3,600,000 milliseconds</p> <p><b>Default:</b> 0 milliseconds</p>
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring the Delay Before Neighbor-Discovery Neighbors Mark the Router as Down</li> </ul>

## rebalance-periodic (Aggregated Ethernet Subscriber Interfaces)

<b>Syntax</b>	<code>rebalance-periodic time <i>hour:minute</i> &lt;interval <i>hours</i>&gt;</code>
<b>Hierarchy Level</b>	[edit interfaces ae <i>number</i> aggregated-ether-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Configure periodic rebalancing of distribution of subscribers on an aggregated Ethernet bundle.
<b>Options</b>	<p><i>hour:minute</i>—Time at which the rebalancing occurs, in military time.</p> <p><i>hours</i>—Interval at which the rebalancing occurs, in hours. Default: 24 hours.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Periodic Rebalancing of Subscribers in an Aggregated Ethernet Interface on page 485</li> </ul>

## realm (Diameter Origin)

---

<b>Syntax</b>	<code>realm <i>realm-name</i>;</code>
<b>Hierarchy Level</b>	[edit diameter origin]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify the realm of the host that originates the Diameter message.
<b>Options</b>	<b><i>realm-name</i></b> —Name of the message origin realm. Supplied as the value of Origin-Realm AVP for all messages sent by the Diameter master instance.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Diameter on page 259</li><li>Configuring the Origin Attributes of the Diameter Instance on page 260</li></ul>

## reconfigure (DHCP Local Server)

<b>Syntax</b>	<pre> reconfigure {     attempts <i>attempt-count</i>;     clear-on-abort;     strict;     timeout <i>timeout-value</i>;     token <i>token-value</i>;     trigger {         radius-disconnect;     } } </pre>
<b>Hierarchy Level</b>	<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> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6],</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>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i>],</p> <p>[edit system services dhcp-local-server],</p> <p>[edit system services dhcp-local-server dhcpv6],</p> <p>[edit system services dhcp-local-server group <i>group-name</i>],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
<b>Description</b>	<p>Enable dynamic reconfiguration triggered by the DHCP local server of all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. A group configuration takes precedence over a DHCP local server configuration. The <b>strict</b> statement is available only for DHCPv6.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 133</li> </ul>

## registration-lifetime

---

<b>Syntax</b>	<code>registration-lifetime seconds;</code>
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i> ], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i> ], [edit routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i> ], [edit services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.
<b>Description</b>	Configure maximum period for registration lifetime that is accepted by the Mobile IP home agent.
<b>Options</b>	<b>registration-lifetime seconds</b> —Maximum lifetime that the home agent accepts in any registration request. The registration lifetime is not affected if you change the system clock. <b>Range:</b> 7 through 65535 seconds <b>Default:</b> 3600 seconds
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Mobile IP on page 357</li><li>Configuring the Mobile IP Home Agent on page 358</li></ul>



## relay-agent-interface-id

<b>Syntax</b>	relay-agent-interface-id;
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 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 dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 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 dhcpv6 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 dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify that the DHCPv6 Relay Agent Interface-ID option (option 18) in the client PDU name is concatenated with the username during the subscriber authentication process.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Creating Unique Usernames for DHCP Clients on page 128</li> </ul>

## relay-agent-remote-id

---

<b>Syntax</b>	relay-agent-remote-id;
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 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 dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 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 dhcpv6 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 dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify that the DHCPv6 Relay Agent Remote-ID option (option 37) in the client PDU name is concatenated with the username during the subscriber authentication process.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Creating Unique Usernames for DHCP Clients on page 128</li></ul>

## relay-agent-subscriber-id

<b>Syntax</b>	relay-agent-subscriber-id;
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication <b>username-include</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication <b>username-include</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication <b>username-include</b>],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication <b>username-include</b>],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication <b>username-include</b>]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify that the DHCPv6 Relay Agent Subscriber-ID option (option 38) in the client PDU name is concatenated with the username during the subscriber authentication process.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Creating Unique Usernames for DHCP Clients on page 128</li> </ul>

## relay-option-60

---

<b>Syntax</b>	<pre>relay-option-60 {   vendor-option {     (equals   starts-with) (ascii <i>match-string</i>   hexadecimal <i>match-hex</i>) {       (relay-server-group <i>server-group-name</i>           local-server-group <i>local-server-group-name</i>           drop);     }     (default-relay-server-group <i>server-group-name</i>         default-local-server-group <i>local-server-group-name</i>         drop);   } }</pre>
<b>Hierarchy Level</b>	<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 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], [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>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	<p>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.</p> <p>You can use the <b>relay-option-60</b> statement and its subordinate statements at the <b>[edit forwarding-options dhcp-relay]</b> hierarchy level to configure option 60 support globally, or at the <b>[edit forwarding-options dhcp-relay group <i>group-name</i>]</b> 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.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 189</li></ul>

## relay-option-82

<b>Syntax</b>	<pre> relay-option-82 {     circuit-id {         prefix <i>prefix</i>;         use-interface-description (logical   device);     } } </pre>
<b>Hierarchy Level</b>	<p>[edit forwarding-options <b>dhcp-relay</b>],  [edit forwarding-options <b>dhcp-relay group group-name</b>],  [edit logical-systems <i>logical-system-name</i> forwarding-options <b>dhcp-relay</b>],  [edit logical-systems <i>logical-system-name</i> forwarding-options <b>dhcp-relay group group-name</b>],  [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options <b>dhcp-relay</b>],  [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options <b>dhcp-relay group group-name</b>],  [edit routing-instances <i>routing-instance-name</i> forwarding-options <b>dhcp-relay</b>],  [edit routing-instances <i>routing-instance-name</i> forwarding-options <b>dhcp-relay group group-name</b>]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	<p>Enable or disable the insertion of the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server.</p> <p>If you enable insertion of option 82 information in DHCP packets, you must specify at least the <b>circuit-id</b> statement to include the Agent Circuit ID suboption (suboption 1) of the DHCP relay agent information option.</p> <p>You can use the <b>relay-option-82</b> statement and its subordinate statements at the <b>[edit forwarding-options dhcp-relay]</b> hierarchy level to control insertion of option 82 information globally, or at the <b>[edit forwarding-options dhcp-relay group group-name]</b> hierarchy level to control insertion of option 82 information for a named group of interfaces.</p> <p>To restore the default behavior (option 82 information is not inserted into DHCP packets), use the <b>delete relay-option-82</b> statement.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Enabling and Disabling Insertion of Option 82 Information on page 192</li> </ul>

## relay-server-group

<b>Syntax</b>	<code>relay-server-group server-group-name;</code>
<b>Hierarchy Level</b>	<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>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	<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 <b>server-group</b> 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>
<b>Options</b>	<b>server-group-name</b> —Name of the extended DHCP relay server group.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 189</li> </ul>

## remote-gateway (Tunnel Profile)

<b>Syntax</b>	remote-gateway { address <i>server-ip-address</i> ; gateway-name <i>server-name</i> ; }
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the IP address and hostname of the remote gateway at the L2TP tunnel endpoint, the LNS.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring a Tunnel Profile for Subscriber Access on page 242</li> </ul>

## remote-id

<b>Syntax</b>	remote-id <i>value</i> range <i>named-range</i> ;
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes option-match option-82]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Specify the address-assignment pool named range to use based on the particular option 82 Agent Remote ID value.
<b>Options</b>	<p><b>range <i>named-range</i></b>—Name of the address-assignment pool range to use.</p> <p><b><i>value</i></b>—String for Agent Remote ID suboption (suboption 2) of the DHCP relay agent information option (option 82) in DHCP packets.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Address-Assignment Pools on page 68</li> </ul>

## replace-ip-source-with

---

<b>Syntax</b>	replace-ip-source-with giaddr;
<b>Hierarchy Level</b>	[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] [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Extended DHCP Relay Agent Overview on page 154</li><li>Replacing the DHCP Relay Request and Release Packet Source Address on page 170</li></ul>



## replay-method

<b>Syntax</b>	<code>replay-method (none   timestamp <i>seconds</i>);</code>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>].</p> <p>[edit logical-systems <i>logical-system-name</i> services mobile-ip peer <i>nai@domain</i> spi <i>hexadecimal-value</i>].</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>].</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer <i>nai@domain</i> spi <i>hexadecimal-value</i>].</p> <p>[edit routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>].</p> <p>[edit routing-instances <i>routing-instances-name</i> services mobile-ip peer <i>nai@domain</i> spi <i>hexadecimal-value</i>],</p> <p>[edit services mobile-ip peer ip-address <i>address</i> spi <i>hexadecimal-value</i>],</p> <p>[edit services mobile-ip peer <i>nai@domain</i> spi <i>hexadecimal-value</i>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.</p>
<b>Description</b>	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.
<b>Default</b>	If you do not configure the replay protection method, then the timestamp tolerance is taken from the home agent by default.
<b>Options</b>	<p><b>none</b>—Timestamp tolerance is obtained from the setting configured for the home agent</p> <p><b>timestamp <i>seconds</i></b>—Tolerance time in which a registration request timestamp and the local time of the home agent can differ.</p> <p><b>Range:</b> 1 through 255 seconds</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Mobile IP on page 357</li> <li>Configuring the Mobile IP Home Agent on page 358</li> </ul>

## retransmit-timer (Dynamic Router Advertisement)

---

<b>Syntax</b>	<code>retransmit-timer <i>milliseconds</i>;</code>
<b>Hierarchy Level</b>	[edit protocols router-advertisement interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Set the retransmission frequency of neighbor solicitation messages.
<b>Options</b>	<i>milliseconds</i> —Retransmission frequency. <b>Default:</b> 0 milliseconds
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring the Frequency of Neighbor Solicitation Messages</li></ul>

## retry

---

<b>Syntax</b>	<code>retry <i>attempts</i>;</code>
<b>Hierarchy Level</b>	[edit access radius-server <i>server-address</i> ], [edit access profile <i>profile-name</i> radius-server <i>server-address</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Specify the number of times that the router or switch is allowed to attempt to contact a RADIUS authentication or accounting server.
<b>Options</b>	<i>attempts</i> —Number of times that the router is allowed to attempt to contact a RADIUS server. <b>Range:</b> 1 through 10 <b>Default:</b> 3
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li><li>Configuring Router or Switch Interaction with RADIUS Servers on page 20</li><li>Example: Configuring CHAP Authentication with RADIUS</li><li>Configuring RADIUS Authentication for L2TP</li><li><b>timeout on page 1208</b></li></ul>

## revert-interval

---

<b>Syntax</b>	<code>revert-interval <i>interval</i>;</code>
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> radius options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
<b>Description</b>	Configure the amount of time the router or switch waits after a server has become unreachable. The router or switch rechecks the connection to the server when the specified interval expires. If the server is then reachable, it is used in accordance with the order of the server list.
<b>Options</b>	<b><i>interval</i></b> —Amount of time to wait. <b>Range:</b> 0 through 4294967295 seconds <b>Default:</b> 60 seconds
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring RADIUS Server Options for Subscriber Access on page 29</li><li>Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li></ul>

## revocation-required

---

<b>Syntax</b>	revocation-required;
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i> ], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i> ], [edit routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i> ], [edit services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.
<b>Description</b>	Configure the Mobile IP home agent to accept registration revocation requests only when the request includes the revocation extension.
<b>Default</b>	The Mobile IP home agent supports registration revocation requests that include the revocation extension, but it does not require the extension.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Mobile IP on page 357</li><li>• Configuring the Mobile IP Home Agent on page 358</li></ul>

## rewrite-rules (Dynamic CoS Interfaces)

<b>Syntax</b>	<pre>rewrite-rules {   dscp (rewrite-name   default);   dscp-ipv6 (rewrite-name   default);   ieee-802.1 (rewrite-name   default) vlan-tag (outer   outer-and-inner);   inet-precedence (rewrite-name   default); }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Associate a rewrite-rules configuration or default mapping with a specific interface in a dynamic profile.
<b>Options</b>	<p><b>rewrite-name</b>—Name of a <b>rewrite-rules</b> mapping configured at the [edit class-of-service <b>rewrite-rules</b>] hierarchy level.</p> <p><b>default</b>—The default mapping.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li> <li>rewrite-rules</li> </ul>

## route (Access)

---

**Syntax**    `route prefix {  
              next-hop next-hop;  
              metric route-cost;  
              preference route-distance;  
              tag route-tag;  
          }`

**Hierarchy Level**    [edit dynamic-profiles routing-options access]

**Release Information**    Statement introduced in Junos OS Release 9.5.

**Description**    Dynamically configure the parameters for access routes.

**Options**    *prefix*—Either the specific route prefix that you want to assign to the access route or one of the following route prefix variables.

- For IPv4 access routes, use the variable, **\$junos-framed-route-ip-address-prefix**. The route prefix variable is dynamically replaced with the value in Framed-Route RADIUS attribute [22].
- For IPv6 access routes, use the variable, **\$junos-framed-route-ipv6-address-prefix**. The variable is dynamically replaced with the value in Framed-IPv6-Route RADIUS attribute [99].



**NOTE:** The **metric** and **preference** statements are not supported when you specify the IPv6 route prefix variable.

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 Documentation**    • Configuring Dynamic Access Routes for Subscriber Management on page 206

## route (Access Internal)

<b>Syntax</b>	<pre>route <i>subscriber-ip-address</i> {     <b>qualified-next-hop</b> <i>underlying-interface</i> {         <b>mac-address</b> <i>address</i>;     } }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles routing-options access-internal]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Dynamically configure parameters for an access-internal route.
<b>Options</b>	<p><i>subscriber-ip-address</i>—Either the specific IP address you want to assign to the access-internal route or the subscriber IP address variable (\$junos-subscriber-ip-address). The subscriber IP address variable is dynamically replaced with the value supplied by DHCP or PPP when a subscriber logs in.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management on page 207</li> <li>Configuring Dynamic Access-Internal Routes for PPP Subscriber Management on page 222</li> </ul>

## route (Diameter Network Element)

---

<b>Syntax</b>	<pre>route <i>dne-route-name</i> {     destination realm <i>realm-name</i> &lt;host <i>hostname</i>&gt;;     function <i>function-name</i> &lt;partition <i>partition-name</i>&gt;;     metric <i>route-metric</i>; }</pre>
<b>Hierarchy Level</b>	[edit diameter network-element <i>element-name</i> forwarding]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Define a route reachable through the Diameter network element by associating a metric with a combination of destination and function partition.
<b>Options</b>	<p><b><i>dne-route-name</i></b>—Route name defined for the Diameter network element.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Diameter on page 259</li><li>Configuring Diameter Network Elements on page 261</li></ul>

## router (Address-Assignment Pools)

---

<b>Syntax</b>	<pre>router [ <i>router-address</i> ];</pre>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Specify one or more routers located on the client's subnet. This statement is the equivalent of DHCP option 3.
<b>Options</b>	<b><i>router-address</i></b> —IP address of one or more routers.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Address-Assignment Pools on page 68</li></ul>



## router-advertisement (Dynamic Profiles)

---

<b>Syntax</b>	router-advertisement {...}
<b>Hierarchy Level</b>	[edit dynamic-profiles protocols]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Enable router advertisement.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring an Interface to Send Neighbor Discovery Advertisements</li> </ul>

## routing-instance

---

<b>Syntax</b>	routing-instance <i>routing-instance-name</i> ;
<b>Hierarchy Level</b>	[edit access radius-server <i>server-address</i> ], [edit access profile <i>profile-name</i> radius-server <i>server-address</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure the routing instance used to send RADIUS packets to the RADIUS server.
<b>Options</b>	<i>routing-instance-name</i> —Routing instance name.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring the PPP Authentication Protocol</li> <li>Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li> </ul>

## routing-instance (Diameter Peer)

---

<b>Syntax</b>	<code>routing-instance <i>routing-instance-name</i> ;</code>
<b>Hierarchy Level</b>	<code>[edit diameter peer <i>peer-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify a routing instance for a Diameter peer. Alternatively, you can include the <b>logical-system</b> statement at the <code>[edit diameter peer <i>peer-name</i>]</code> hierarchy level to configure a logical and routing instance.
<b>Options</b>	<b><i>routing-instance-name</i></b> —Name of the routing instance. <b>Default:</b> Master routing instance
<b>Required Privilege Level</b>	<b>admin</b> —To view this statement in the configuration. <b>admin-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Diameter on page 259</li><li>Configuring Diameter Peers on page 260</li></ul>

## routing-instance (Diameter Transport)

---

<b>Syntax</b>	<code>routing-instance <i>routing-instance-name</i> ;</code>
<b>Hierarchy Level</b>	<code>[edit diameter transport <i>transport-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Specify a routing instance for the Diameter transport layer connection.
<b>Options</b>	<b><i>routing-instance-name</i></b> —Name of the routing instance. <b>Default:</b> Master routing instance
<b>Required Privilege Level</b>	<b>admin</b> —To view this statement in the configuration. <b>admin-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring the Diameter Transport on page 262</li></ul>

## routing-instance (Tunnel Profile)

---

<b>Syntax</b>	<code>routing-instance <i>routing-instance-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify a routing instance for a tunnel.
<b>Options</b>	<b><i>routing-instance-name</i></b> —Name of the routing instance. <b>Default:</b> Routing instance <i>default</i>
<b>Required Privilege Level</b>	<b>admin</b> —To view this statement in the configuration. <b>admin-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Tunnel Profile for Subscriber Access on page 242</li></ul>

## routing-instance (PPPoE Service Name Tables)

---

<b>Syntax</b>	<code>routing-instance <i>routing-instance-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit protocols pppoe service-name-tables <i>table-name</i> service <i>service-name</i>],</code> <code>[edit protocols pppoe service-name-tables <i>table-name</i> service <i>service-name</i> agent-specifier</code> <code>aci <i>circuit-id-string</i> ari <i>remote-id-string</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	<p>Use in conjunction with the <b>dynamic-profile</b> statement at the same hierarchy levels to specify the routing instance in which to instantiate a dynamic PPPoE interface. You can associate a routing instance with a named service entry, <b>empty</b> service entry, or <b>any</b> service entry configured in a PPPoE service name table, or with an agent circuit identifier/agent remote identifier (ACI/ARI) pair defined for these services.</p> <p>The routing instance associated with a service entry in a PPPoE service name table overrides the routing instance associated with the PPPoE underlying interface on which the dynamic PPPoE interface is created.</p> <p>If you include the <b>routing-instance</b> statement at the <code>[edit protocols pppoe service-name-tables <i>table-name</i> service <i>service-name</i> agent-specifier aci <i>circuit-id-string</i> ari <i>remote-id-string</i>]</code> hierarchy level, you cannot also include the <b>static-interface</b> statement at this level. The <b>routing-instance</b> and <b>static-interface</b> statements are mutually exclusive for ACI/ARI pair configurations.</p>
<b>Options</b>	<b><i>routing-instance-name</i></b> —Name of the routing instance in which the router instantiates the dynamic PPPoE interface.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring PPPoE Service Name Tables</li><li>Assigning a Dynamic Profile and Routing Instance to a Service Name or ACI/ARI Pair for Dynamic PPPoE Interface Creation on page 543</li></ul>

## routing-instance-name (DHCP Local Server)

<b>Syntax</b>	routing-instance-name;
<b>Hierarchy Level</b>	<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 dhcpv6 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 dhcpv6 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 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 dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> 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 dhcpv6 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 dhcpv6 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 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 dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> 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 dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication username-include]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Specify that the routing instance name be concatenated with the username during the subscriber authentication process. No routing instance name is concatenated if the configuration is in the default routing instance.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Using External AAA Authentication Services with DHCP on page 110</li> </ul>

## routing-instance-name (DHCP Relay Agent)

---

<b>Syntax</b>	routing-instance-name;
<b>Hierarchy Level</b>	[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]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	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.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Using External AAA Authentication Services with DHCP on page 110</li></ul>

## routing-instance-name (Static Subscribers)

<b>Syntax</b>	routing-instance-name;
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers authentication <b>username-include</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i> authentication <b>username-include</b>],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers authentication <b>username-include</b>],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication <b>username-include</b>],</p> <p>[edit system services static-subscribers authentication <b>username-include</b>],</p> <p>[edit system services static-subscribers group <i>group-name</i> authentication <b>username-include</b>]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify that the name of the routing instance is included as part of the username created for all static subscribers or for the static subscribers in the specified group. The group version of the statement takes precedence over the global version. The username is also sent to RADIUS in the Access-Request message.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Subscribers over Static Interfaces on page 288</li> <li>Configuring the Static Subscriber Global Username on page 291</li> <li>Configuring the Static Subscriber Group Username on page 295</li> </ul>

## routing-instances

---

<b>Syntax</b>	<code>routing-instances <i>routing-instance-name</i> {     interface <i>interface-name</i>; }</code>
<b>Hierarchy Level</b>	[edit <b>dynamic-profiles</b> ],
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Dynamically configure an additional routing entity for a router.
<b>Options</b>	<b><i>routing-instance-name</i></b> —The routing instance variable (\$junos-routing-instance). The routing instance variable is dynamically replaced with the routing instance the accessing client uses when connecting to the router.

The remaining statement is explained separately.



**NOTE:** Though we do not recommend it, you can also enter a specific name for the routing instance, a maximum of 31 characters.

The **interface** statement is described separately.

<b>Required Privilege Level</b>	<code>routing</code> —To view this statement in the configuration. <code>routing-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Dynamic Profile for use by a Retailer in the DHCPv4 Solution</li></ul>



## routing-options (Dynamic Profiles)

```
Syntax  routing-options {
        access {
            route prefix {
                next-hop next-hop;
                metric route-cost;
                preference route-distance;
                tag route-tag;
            }
        }
        access-internal {
            route subscriber-ip-address {
                qualified-next-hop underlying-interface {
                    mac-address address;
                }
            }
        }
        multicast {
            interface interface-name {
                no-qos-adjust;
            }
        }
    }
```

**Hierarchy Level** [edit *dynamic-profiles profile-name*]

**Release Information** Statement introduced in Junos OS Release 9.6.

**Description** Configure protocol-independent routing properties in a 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 Documentation**

- Configuring Dynamic Access Routes for Subscriber Management on page 206
- Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management on page 207

## rpf-check (Dynamic Profiles)

---

<b>Syntax</b>	<code>rpf-check {     mode loose; }</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> ],
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	<p>Check whether traffic is arriving on an expected path. You can include this statement with the <b>inet</b> protocol family only.</p> <p>The <b>mode</b> statement is explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Unicast RPF</li></ul>

## rule

```
Syntax  rule rule-name {
        match-direction (input | output | input-output);
        term term-name {
            from {
                application [junos-http, junos-https, junos-httpproxy];
                destination-address address <except>;
                destination-prefix-list list-name <except>;
            }
            then {
                accept;
                rewrite {
                    destination-address address;
                    destination-port port;
                }
                syslog;
            }
        }
    }
```

**Hierarchy Level** [edit services captive-portal-content-delivery]

**Release Information** Statement introduced in Junos OS Release 10.4.

**Description** Specify the rule the router uses when applying this service.

**Options** *rule-name*—Identifier for the collection of terms that constitute this rule.  
The remaining statements are explained separately.

**Required Privilege Level** services—To view this statement in the configuration.  
services—control—To add this statement to the configuration.

**Related Documentation**

- Redirecting HTTP Requests on page 613

## rule-set

---

<b>Syntax</b>	<code>rule-set <i>rule-set-name</i> {     [rule <i>rule-name</i> ]; }</code>
<b>Hierarchy Level</b>	<code>[edit services captive-portal-content-delivery]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the rule set the router uses when applying this service.
<b>Options</b>	<b><i>rule-set-name</i></b> —Identifier for the collection of rules that constitute this rule set.  The remaining statement is explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Redirecting HTTP Requests on page 613</li></ul>

## scheduler (Dynamic Scheduler Maps)

---

<b>Syntax</b>	<code>scheduler <i>scheduler-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service scheduler-maps <i>map-name</i>     forwarding-class <i>class-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Associate a scheduler with a scheduler map in a dynamic profile.
<b>Options</b>	<b><i>scheduler-name</i></b> —Either the specific name of the scheduler configuration block or the scheduler variable ( <code>\$junos-cos-scheduler</code> ).
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>• Configuring Schedulers in a Dynamic Profile for Subscriber Access on page 679</li><li>• Dynamic Variables Overview on page 371</li></ul>

## scheduler-map (Dynamic Traffic Shaping)

<b>Syntax</b>	<code>scheduler-map (map-name);</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles profile-name class-of-service traffic-control-profiles profile-name]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. The <code>\$junos-cos-scheduler-map</code> variable introduced in Junos OS Release 9.4.
<b>Description</b>	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 profile-name class-of-service scheduler-maps]</code> hierarchy level) or statically (at the <code>[edit class-of-service scheduler-maps]</code> hierarchy level).
<b>Options</b>	<b>map-name</b> —Name of the scheduler map or the Junos predefined variable ( <code>\$junos-cos-scheduler-map</code> ). When you specify the variable, the scheduler-map name is obtained from the RADIUS server when a subscriber authenticates over the interface to which the dynamic profile is attached.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li> <li>Configuring Traffic Scheduling and Shaping for Subscriber Access on page 677</li> <li><b>output-traffic-control-profile on page 1092</b></li> </ul>

## scheduler-maps (Dynamic CoS Definition)

---

<b>Syntax</b>	<pre>scheduler-maps {   map-name {     forwarding-class class-name scheduler scheduler-name;   } }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. Support at the [edit dynamic-profiles <i>profile-name</i> ] hierarchy level introduced in Junos OS Release 9.3.
<b>Description</b>	Specify a scheduler map name in a dynamic profile and associate it with the scheduler configuration and forwarding class.
<b>Options</b>	<i>map-name</i> —Name of the scheduler map.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>Configuring Schedulers in a Dynamic Profile for Subscriber Access on page 679</li></ul>

## schedulers (Dynamic CoS Definition)

<b>Syntax</b>	<pre> schedulers {   (<i>scheduler-name</i>) {     buffer-size (percent <i>percentage</i>   remainder   temporal <i>microseconds</i>         \$junos-cos-scheduler-bs);     drop-profile-map loss-priority (any   low   medium-low   medium-high   high) protocol       (any   non-tcp   tcp) drop-profile (<i>profile-name</i>   <i>predefined-variable</i>);     excess-priority (low   high   \$junos-cos-scheduler-excess-priority);     excess-rate (percent <i>percentage</i>   percent \$junos-cos-scheduler-excess-rate);     overhead-accounting (<i>shaping-mode</i>) &lt;bytes (<i>byte-value</i>)&gt;;     priority (<i>priority-level</i>   \$junos-cos-scheduler-priority);     shaping-rate (<i>rate</i>   <i>predefined-variable</i>);     transmit-rate (<i>rate</i>   percent <i>percentage</i>   remainder   percent <i>percentage</i>       \$junos-cos-scheduler-tx) &lt;exact   rate-limit&gt;;   } } </pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. The <b>\$junos-cos-scheduler</b> predefined variable introduced in Junos OS Release 9.4.
<b>Description</b>	Specify scheduler name and parameter values in a dynamic profile.
<b>Options</b>	<p><b><i>scheduler-name</i></b>—Name of the scheduler to be configured or the Junos predefined variable (<b>\$junos-cos-scheduler</b>). The predefined variable is replaced with the scheduler name obtained from the RADIUS server when a subscriber authenticates over the interface to which the dynamic profile is attached.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li> <li>Configuring Schedulers in a Dynamic Profile for Subscriber Access on page 679</li> <li><b>scheduler</b> on page 1174</li> </ul>

## secret

---

<b>Syntax</b>	<code>secret password;</code>
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> radius-server <i>server-address</i> ], [edit access radius-disconnect <i>client-address</i> ], [edit access radius-server <i>server-address</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure the password to use with the RADIUS server. The secret password used by the local router or switch must match that used by the server.
<b>Options</b>	<i>password</i> —Password to use; it can include spaces if the character string is enclosed in quotation marks.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li><li>• Configuring Router or Switch Interaction with RADIUS Servers on page 20</li><li>• Example: Configuring CHAP Authentication with RADIUS</li><li>• Configuring RADIUS Authentication for L2TP</li><li>• Configuring the RADIUS Disconnect Server for L2TP</li></ul>

## secret (Tunnel Profile)

---

<b>Syntax</b>	<code>secret password;</code>
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the tunnel password sent to the LNS for authentication.
<b>Options</b>	<i>password</i> —Cleartext password.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring a Tunnel Profile for Subscriber Access on page 242</li></ul>



## send-release-on-delete (DHCP Relay Agent)

<b>Syntax</b>	send-release-on-delete;
<b>Hierarchy Level</b>	[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], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Send a release message to the DHCP server whenever DHCP relay or relay proxy deletes a client.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Extended DHCP Relay Agent Overview on page 154</li> <li>Overriding the Default DHCP Relay Configuration Settings on page 168</li> <li>Sending Release Messages When Clients Are Deleted on page 184</li> </ul>

## server (Dynamic PPPoE)

<b>Syntax</b>	server;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" pppoe-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	In a dynamic profile, configure the router to act as a PPPoE server, also known as a remote access concentrator, when a PPPoE logical interface is dynamically created.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring a Basic PPPoE Dynamic Profile on page 536</li> <li>For information about creating static PPPoE interfaces, see the <a href="#">Junos OS Network Interfaces Configuration Guide</a></li> </ul>

## server-group

---

<b>Syntax</b>	<pre>server-group {     server-group-name {         server-ip-address;     } }</pre>
<b>Hierarchy Level</b>	[edit forwarding-options <b>dhcp-relay</b> ], [edit logical-systems <i>logical-system-name</i> forwarding-options <b>dhcp-relay</b> ], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options <b>dhcp-relay</b> ], [edit routing-instances <i>routing-instance-name</i> forwarding-options <b>dhcp-relay</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	Specify the name of a group of DHCP server addresses for use by the extended DHCP relay agent.
<b>Options</b>	<b>server-group-name</b> —Name of the group of DHCP server addresses.  <b>server-ip-address</b> —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.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Extended DHCP Relay Agent Overview on page 154</li></ul>

## server-identifier (Address-Assignment Pools)

---

<b>Syntax</b>	<pre>server-identifier <i>ipv4-address</i>;</pre>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family inet <b>dhcp-attributes</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Specify the IP address that is used as the source address the DHCP server includes in IP packets when communicating with clients. The address is included in the DHCP packet in option 54.
<b>Options</b>	<b>ipv4-address</b> —IP address.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Address-Assignment Pools on page 68</li></ul>

## service (Dynamic Service Sets)

<b>Syntax</b>	<pre> service {   input {     service-set <i>service-set-name</i> {       service-filter <i>filter-name</i>;     }     post-service-filter <i>filter-name</i>;   }   output {     service-set <i>service-set-name</i> {       service-filter <i>filter-name</i>;     }   } } </pre>
<b>Hierarchy Level</b>	<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 pp0 unit "\$junos-interface-unit" family <i>family</i>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.5.</p> <p>Support at the [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i>] hierarchy level introduced in Junos OS Release 10.1.</p>
<b>Description</b>	<p>Define the service sets and filters to be applied to an interface. This statement is not supported for <b>family inet6</b>.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Dynamic Service Sets Overview on page 569</li> <li>Associating Service Sets with Interfaces in a Dynamic Profile on page 595</li> </ul>

## service-filter (Dynamic Service Sets)

---

<b>Syntax</b>	<code>service-filter <i>filter-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> service input service-set <i>service-set-name</i>],</code> <code>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i> service output service-set <i>service-set-name</i>],</code> <code>[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i> service input service-set <i>service-set-name</i>],</code> <code>[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i> service output service-set <i>service-set-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. Support at the <code>[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i> service input service-set <i>service-set-name</i>]</code> and <code>[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i> service output service-set <i>service-set-name</i>]</code> hierarchy levels introduced in Junos OS Release 10.1.
<b>Description</b>	Define the filter to be applied to traffic before it is accepted for service processing. Configuration of a service filter is optional; if you include the <b>service-set</b> statement without a <b>service-filter</b> definition, the router software assumes that the match condition is true and selects the service set for processing automatically. Only the Internet Protocol version 4 (IPv4) protocol family is currently supported for dynamic PPPoE logical interfaces.
<b>Options</b>	<i>filter-name</i> —Identifies the filter to be applied in service processing.
<b>Required Privilege Level</b>	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Dynamic Service Sets Overview on page 569</li><li>Associating Service Sets with Interfaces in a Dynamic Profile on page 595</li></ul>

## service-name-table

<b>Syntax</b>	<code>service-name-table <i>table-name</i>;</code>
<b>Hierarchy Level</b>	<p>[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> pppoe-underlying-options],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> pppoe-underlying-options]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 10.0.</p> <p>(MX Series routers with Trio MPCs only) The [edit ... family pppoe] hierarchies introduced in Junos OS Release 11.2.</p>
<b>Description</b>	Specify the PPPoE service name table assigned to a PPPoE underlying interface. This underlying interface is configured with either the <b>encapsulation ppp-over-ether</b> statement or the <b>family pppoe</b> statement; the two statements are mutually exclusive.
<b>Options</b>	<b><i>table-name</i></b> —Name of the PPPoE service name table, a string of up to 32 alphanumeric characters.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring PPPoE Service Name Tables</li> <li>Assigning a Service Name Table to a PPPoE Underlying Interface</li> <li>Configuring the PPPoE Family for an Underlying Interface on page 486</li> </ul>

## service-set (Dynamic Service Sets)

---

<b>Syntax</b>	<pre>service-set <i>service-set-name</i> {     service-filter <i>filter-name</i>; }</pre>
<b>Hierarchy Level</b>	<pre>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family   <i>family</i> service input], [edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family   <i>family</i> service output], [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i>   service input], [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i>   service output]</pre>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. Support at the [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i> service input] and [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family <i>family</i> service output] hierarchy levels introduced in Junos OS Release 10.1.
<b>Description</b>	Define one or more service sets in a dynamic profile. Service sets are applied to an interface. If you define multiple service sets, the router software evaluates the filters in the order in which they appear in the configuration. Only the Internet Protocol version 4 (IPv4) protocol family is currently supported for dynamic PPPoE logical interfaces.
<b>Options</b>	<p><b><i>service-set-name</i></b>—Name of the service set.</p> <p>The remaining statement is explained separately.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Dynamic Service Sets Overview on page 569</li><li>Associating Service Sets with Interfaces in a Dynamic Profile on page 595</li></ul>

## services

---

<b>Syntax</b>	<code>services captive-portal-content-delivery { ... }</code>
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Define the captive portal and content delivery set of the rules statements to be applied to traffic.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Redirecting HTTP Requests on page 613</li> </ul>

## session-options

---

<b>Syntax</b>	<pre>session-options {   client-group [ <i>group-names</i> ];   client-idle-timeout <i>minutes</i>;   client-session-timeout <i>minutes</i>; }</pre>
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5. Support for MX Series routers introduced in Junos OS Release 11.1.
<b>Description</b>	<p>Define options that control a user's session after successful authentication. This statement is supported on J Series, MX Series, and SRX Series devices. The subordinate <code>client-group [ <i>group-names</i> ]</code> statement is not supported on MX Series routers.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Understanding Session Options for Subscriber Access on page 54</li> <li>• Configuring Subscriber Session Options on page 55</li> </ul>

## shaping-rate (Dynamic Traffic Shaping and Scheduling)

---

<b>Syntax</b>	<code>shaping-rate (<i>rate</i>   <i>predefined-variable</i>);</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>]</code> <code>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2. The <b>\$junos-cos-shaping-rate</b> variable for traffic-control profiles introduced in Junos OS Release 9.4. The <b>\$junos-cos-scheduler-shaping-rate</b> variable for schedulers introduced in Junos OS Release 10.2.
<b>Description</b>	Configure a shaping rate for a logical interface or a scheduler. 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).
<b>Options</b>	<p><b>rate</b>—Peak rate in bits per second (bps). You can specify the value as a complete decimal number or as a decimal number followed by the abbreviation <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).</p> <p><b>Range:</b> 1000 through 160,000,000,000 bps</p> <p><b>predefined-variable</b>—One of the following Junos predefined variables. The variable is replaced with a value obtained from the RADIUS server when a subscriber authenticates over the interface to which the dynamic profile is attached.</p> <ul style="list-style-type: none"><li>• <b>\$junos-cos-shaping-rate</b>—Variable for the shaping rate that is specified for the logical interface. Use this variable at the <code>[edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>]</code> hierarchy level.</li><li>• <b>\$junos-cos-scheduler-shaping-rate</b>—Variable for the shaping rate that is specified for a scheduler. Use this variable at the <code>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>]</code> hierarchy level.</li></ul>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>• Configuring Traffic Scheduling and Shaping for Subscriber Access on page 677</li><li>• <b>output-traffic-control-profile</b> on page 1092</li></ul>



## sip-server-address

---

<b>Syntax</b>	<code>sip-server-address <i>ipv6-address</i>;</code>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family <i>family</i> dhcp-attributes]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Specify a SIP outbound proxy server that DHCPv6 local server clients can use. This is equivalent to DHCPv6 option 22. To specify multiple servers, add multiple <b>sip-server-address</b> statements in order of preference.
<b>Options</b>	<i>ipv6-address</i> —IPv6 address of a SIP outbound proxy server.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Address-Assignment Pools Overview on page 67</li> <li>Configuring Address-Assignment Pools on page 68</li> </ul>

## sip-server-domain-name

---

<b>Syntax</b>	<code>sip-server-domain-name <i>domain-name</i>;</code>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family <i>family</i> dhcp-attributes]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.0.
<b>Description</b>	Configure the domain name of the SIP outbound proxy server that DHCPv6 local server clients can use. This is equivalent to DHCPv6 option 21.
<b>Options</b>	<i>domain-name</i> —Name of the domain.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Address-Assignment Pools Overview on page 67</li> <li>Configuring Address-Assignment Pools on page 68</li> </ul>

## source (Dynamic IGMP Interface)

---

<b>Syntax</b>	<code>source <i>source</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i> static]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the IP version 4 (IPv4) unicast address to send data on an interface.
<b>Options</b>	<i>source</i> —IPv4 unicast address.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Dynamic Profile for Client Access on page 395</li><li>For information about defining an IGMP source, see “Enabling IGMP Static Group Membership” in the <a href="#">Junos OS Multicast Protocols Configuration Guide</a></li></ul>

## source (Dynamic MLD Interface)

---

<b>Syntax</b>	<code>source <i>ip-address</i> {     source-count <i>number</i>;     source-increment <i>increment</i>; }</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols mld interface <i>interface-name</i> static group <i>multicast-group-address</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	IP version 6 (IPv6) unicast source address for the multicast group being configured on a dynamic interface.
<b>Options</b>	<i>ip-address</i> —One or more IPv6 unicast addresses.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Enabling MLD Static Group Membership</li></ul>

## source-address

<b>Syntax</b>	<code>source-address <i>source-address</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access radius-server <i>server-address</i>],</code> <code>[edit access profile <i>profile-name</i> radius-server <i>server-address</i>]</code>
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure a source address for each configured RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address.
<b>Options</b>	<b><i>source-address</i></b> —Valid IPv4 address configured on one of the router or switch interfaces. On M Series routers only, the source address can be an IPv6 address and the UDP source port is 514.
<b>Required Privilege Level</b>	<code>admin</code> —To view this statement in the configuration. <code>admin-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Router or Switch Interaction with RADIUS Servers on page 20</li> <li>Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li> <li>Example: Configuring CHAP Authentication with RADIUS</li> <li>Configuring RADIUS Authentication for L2TP</li> </ul>

## source-count (Dynamic MLD Interface)

<b>Syntax</b>	<code>source-count <i>number</i>;</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> protocols mld interface <i>interface-name</i> static group <i>multicast-group-address</i> source]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Configure the number of multicast source addresses that should be accepted for each static group created on dynamic interfaces.
<b>Options</b>	<b><i>number</i></b> —Number of source addresses. <b>Default:</b> 1 <b>Range:</b> 1 through 1024
<b>Required Privilege Level</b>	<code>routing</code> —To view this statement in the configuration. <code>routing-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Enabling MLD Static Group Membership</li> </ul>

## source-gateway (Tunnel Profile)

---

<b>Syntax</b>	<pre>source-gateway {     address <i>client-ip-address</i>;     gateway-name <i>client-name</i>; }</pre>
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	<p>Specify the IP address and hostname of the source gateway at the local L2TP tunnel endpoint, the LAC.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Tunnel Profile for Subscriber Access on page 242</li></ul>

## source-increment (Dynamic MLD Interface)

---

<b>Syntax</b>	<pre>source-increment <i>number</i>;</pre>
<b>Hierarchy Level</b>	[edit dynamic-profile <i>profile-name</i> protocols mld interface <i>interface-name</i> static group <i>multicast-group-address</i> source]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	<p>Configure the number of times the address should be incremented for each static group created on the dynamic interface. The increment is specified in a format similar to an IPv6 address.</p>
<b>Options</b>	<p><b><i>increment</i></b>—Number of times the source address should be incremented.</p> <p><b>Default:</b> ::1</p> <p><b>Range:</b> ::1 through ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:</p>
<b>Required Privilege Level</b>	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Enabling MLD Static Group Membership</li></ul>

## source-ipv4-address

---

<b>Syntax</b>	<code>source-ipv4-address <i>ipv4-address</i>;</code>
<b>Hierarchy Level</b>	<code>[edit services radius-flow-tap]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
<b>Description</b>	Specify the source IP address used in the IP header that is prepended to mirrored packets sent to a mediation device.
<b>Options</b>	<i>ipv4-address</i> —IPv4 address.
<b>Required Privilege Level</b>	flow-tap—To view this statement in the configuration. flow-tap-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Subscriber Secure Policy Overview on page 625</li><li>Configuring RADIUS-Initiated Subscriber Secure Policy Mirroring Overview on page 635</li></ul>

## spi

---

<b>Syntax</b>	<pre>spi <i>hexadecimal-value</i> {     algorithm (hmac-md5   md5);     entity-type (host   mobility-agent);     key (hex   ascii) <i>string</i>;     replay-method (none   timestamp <i>seconds</i>); }</pre>
<b>Hierarchy Level</b>	<pre>[edit logical-systems <i>logical-system-name</i> services mobile-ip peer ip-address <i>address</i>], [edit logical-systems <i>logical-system-name</i> services mobile-ip peer nai <i>user@domain</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services   mobile-ip peer ip-address <i>address</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services   mobile-ip peer nai <i>user@domain</i>], [edit routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i>], [edit routing-instances <i>routing-instances-name</i> services mobile-ip peer nai <i>user@domain</i>], [edit services mobile-ip peer ip-address <i>address</i>], [edit services mobile-ip peer nai <i>user@domain</i>]</pre>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit logical-systems <i>logical-system-name</i> services mobile-ip peer ip-address <i>address</i>], [edit logical-systems <i>logical-system-name</i> services mobile-ip peer nai <i>user@domain</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip peer nai <i>user@domain</i>], [edit routing-instances <i>routing-instances-name</i> services mobile-ip peer ip-address <i>address</i>], and [edit routing-instances <i>routing-instances-name</i> services mobile-ip peer nai <i>user@domain</i>] hierarchy levels introduced in Junos OS Release 9.5.</p>
<b>Description</b>	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.
<b>Options</b>	<p><i>hexadecimal-value</i>—Security parameter index identifier.</p> <p><b>Range:</b> 100 to FFFFFFFF</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Mobile IP on page 357</li><li>Configuring the Mobile IP Home Agent on page 358</li></ul>

## ssm-map (Dynamic IGMP Interface)

---

<b>Syntax</b>	<code>ssm-map <i>ssm-map-name</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Apply an SSM map to an IGMP interface.
<b>Options</b>	<i>ssm-map-name</i> —Name of SSM map.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring a Dynamic Profile for Client Access on page 395</li> <li>For information about configuring SSM maps, see “Source-Specific Multicast Groups Overview” in the <i>Junos OS Multicast Protocols Configuration Guide</i></li> </ul>

## ssm-map (Dynamic MLD Interface)

---

<b>Syntax</b>	<code>ssm-map <i>ssm-map-name</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols mld interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Apply an SSM map to a dynamic MLD interface.
<b>Options</b>	<i>ssm-map-name</i> —Name of SSM map.
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Example: Configuring SSM Mapping</li> </ul>

## static (Dynamic IGMP Interface)

---

<b>Syntax</b>	<pre>static {     group <i>group</i>;     group <i>group</i> {         source <i>source</i>;     } }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols igmp interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Test multicast forwarding on an interface without a receiver host.
<b>Options</b>	The remaining statements are explained separately.
<b>Required Privilege Level</b>	routing and trace—To view this statement in the configuration. routing-control and trace-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Dynamic Profile for Client Access on page 395</li><li>For information about testing multicast forwarding without a receiver host, see “Enabling IGMP Static Group Membership” in the <a href="#">Junos OS Multicast Protocols Configuration Guide</a></li></ul>



## static (Dynamic MLD Interface)

<b>Syntax</b>	<pre>static {   group <i>multicast-group-address</i> {     exclude;     group-count <i>number</i>;     group-increment <i>increment</i>;     source <i>ip-address</i> {       source-count <i>number</i>;       source-increment <i>increment</i>;     }   } }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols mld interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	<p>Test multicast forwarding on an interface.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>routing and trace—To view this statement in the configuration.</p> <p>routing-control and trace-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Enabling MLD Static Group Membership</li> </ul>

## static-subscribers

---

<b>Syntax</b>	<pre>static-subscribers {   access-profile <i>profile-name</i>;   authentication {     password <i>password-string</i>;     username-include {       domain-name <i>domain-name</i>;       interface;       logical-system-name;       routing-instance-name;       user-prefix <i>user-prefix-string</i>;     }   }   dynamic-profile <i>profile-name</i> {     aggregate-clients (merge   replace);   }   group <i>group-name</i> {     access-profile <i>profile-name</i>;     authentication {       password <i>password-string</i>;       username-include {         domain-name <i>domain-name</i>;         interface;         logical-system-name;         routing-instance-name;         user-prefix <i>user-prefix-string</i>;       }     }     dynamic-profile <i>profile-name</i> {       aggregate-clients (merge   replace);     }     interface <i>interface-name</i> &lt;exclude&gt; &lt;upto <i>upto-interface-name</i>&gt;;   } }</pre>
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> system services], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services], [edit routing-instances <i>routing-instances-name</i> system services], [edit system services]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	<p>Configure and associate subscribers with statically configured interfaces for dynamic service provisioning.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.

- Related Documentation**
- Configuring Subscribers over Static Interfaces on page 288

---

## statistics

---

<b>Syntax</b>	statistics (time   volume-time);
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> accounting]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches. Option <b>volume-time</b> introduced in Junos OS Release 9.4.
<b>Description</b>	Configure the router or switch to collect time statistics, or both volume and time statistics, for the sessions being managed by AAA.
<b>Options</b>	<b>time</b> —Collect uptime statistics only.  <b>volume-time</b> —Collect both volume and uptime statistics. This option is not available for Mobile IP.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Mobile IP Home Agent Elements and Behavior on page 345</li><li>• Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li></ul>

## strict (DHCP Local Server)

---

<b>Syntax</b>	strict;
<b>Hierarchy Level</b>	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure], [edit system services dhcp-local-server dhcpv6 reconfigure], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify whether the server denies a client to bind when the client does not indicate that it accepts reconfigure messages. This feature is available only for DHCPv6.
<b>Default</b>	Accept solicit messages from clients that do not support reconfiguration and permit them to bind.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 133</li><li>Preventing Binding of Clients That Do Not Support Reconfigure Messages</li></ul>

## strip-domain (Domain Maps)

---

<b>Syntax</b>	strip-domain;
<b>Hierarchy Level</b>	[edit access domain map <i>domain-map-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Remove the domain name from the username before continuing with any AAA services specified in a domain map.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Enabling Domain Name Stripping on page 88</li><li>Configuring Domain Name Usage for Domain Maps on page 86</li></ul>

## subscriber-management (Subscriber Management)

<b>Syntax</b>	<pre>subscriber-management {   maintain-subscriber {     interface-delete;   }   traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i>&gt; &lt;size <i>maximum-file-size</i>&gt;       &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>;   } }</pre>
<b>Hierarchy Level</b>	[edit system services]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1.
<b>Description</b>	Configure global services for subscriber management, such as maintaining subscribers and tracing operations.
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 124</li> <li>Tracing Subscriber Management Database Operations for Subscriber Access on page 58</li> </ul>

## swap (Dynamic VLANs)

<b>Syntax</b>	swap;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	For dynamic VLAN interfaces, specify the VLAN rewrite operation to replace a VLAN tag. The outer VLAN tag of the frame is overwritten with the user-specified VLAN tag information.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Rewriting the VLAN Tag on Tagged Frames</li> <li>Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution</li> </ul>

## tag (Access)

---

<b>Syntax</b>	<code>tag route-tag;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles routing-options access route <i>prefix</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Dynamically configure the tag for an access route.
<b>Options</b>	<b>route-tag</b> —Either the specific tag you want to assign to the access route or the tag variable ( <b>\$junos-framed-route-tag</b> ). The tag variable is dynamically replaced with the value in Framed-Route Attribute [22].
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Dynamic Access Routes for Subscriber Management on page 206</li></ul>

## tag (Dynamic Profiles)

---

<b>Syntax</b>	<code>tag tag-number;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> variables radius vendor-id]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure a tag for a RADIUS attribute as a variable in a dynamic profile.
<b>Options</b>	<b>tag-number</b> —Tag number for the RADIUS attribute.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 698</li></ul>

## tag-protocol-id (Dynamic VLANs)

<b>Syntax</b>	tag-protocol-id <i>tpid</i> ;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	For dynamic VLAN interfaces, configure the outer TPID value. All TPIDs you include in input and output VLAN maps must be among those you specify at the <b>[edit interfaces <i>interface-name</i> gigether-options ethernet-switch-profile tag-protocol-id [ <i>tpids</i> ]]</b> hierarchy level.
<b>Default</b>	If the <b>tag-protocol-id</b> statement is not configured, the TPID value is 0x8100.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Inner and Outer TPIDs and VLAN IDs</li> </ul>

## target-logical-system (Domain Maps)

---

<b>Syntax</b>	<code>target-logical-system <i>logical-system-name</i> {     target-routing-instance <i>routing-instance-name</i>; }</code>
<b>Hierarchy Level</b>	[edit access domain map <i>domain-map-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	<p>Configure a non-default logical system and optionally a non-default routing instance for the subscriber's interface in a domain map.</p> <p>You use the <b>target-routing-instance</b> statement at the [edit access domain map <b><i>domain-map-name</i></b>] hierarchy level to configure a non-default routing instance for the default logical system.</p>
<b>Default</b>	Default logical system for the subscriber..
<b>Options</b>	<p><b><i>logical-system-name</i></b>—Name of the logical system.</p> <p>The remaining statement is explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Specifying a Target Logical System/Routing Instance in a Domain Map on page 85</li></ul>



## target-routing-instance (Domain Maps)

<b>Syntax</b>	<code>target-routing-instance <i>routing-instance-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access domain map <i>domain-map-name</i>],</code> <code>[edit access domain map <i>domain-map-name</i> target-logical-system <i>logical-system-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	<p>Configure a non-default routing instance for the target logical system for the subscriber's interface in a domain map.</p> <ul style="list-style-type: none"> <li>When configured at the <code>[edit access domain map <i>domain-map-name</i>]</code> hierarchy level, this statement configures the routing instance used with the default target logical system.</li> <li>When configured at the <code>[edit access domain map <i>domain-map-name</i> target-logical-system <i>logical-system-name</i>]</code> hierarchy level, this statement configures the routing instance used with the specified non-default target logical system.</li> </ul>
<b>Default</b>	Default routing instance for the subscriber.
<b>Options</b>	<i>routing-instance-name</i> —Name of the routing instance.
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Specifying a Target Logical System/Routing Instance in a Domain Map on page 85</li> </ul>

## targeted-distribution (Demux Interfaces over Aggregated Ethernet)

<b>Syntax</b>	<code>targeted-distribution;</code>
<b>Hierarchy Level</b>	<code>[edit interfaces demux0unit <i>logical-unit-number</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	<p>Configure egress data for a logical interface to be sent across a single member link in an aggregated Ethernet bundle. A backup link is provisioned with CoS scheduling resources in the event that the primary assigned link goes down. The aggregated Ethernet interface must be configured without link protection.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring the Distribution Type for Demux Subscribers on Aggregated Ethernet Interfaces on page 484</li> </ul>

## term

---

<b>Syntax</b>	<pre>term <i>term-name</i> {     from {         <i>match-conditions</i>;     }     then {         <i>action</i>;         <i>action-modifiers</i>;     }     only-at-create; }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> firewall family <i>family</i> fast-update-filter <i>filter-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Define terms for fast update filters.
<b>Options</b>	<p><b>action</b>—(Optional) An action to take if conditions match. If you do not specify an action, the packets that match the conditions in the <b>from</b> statement are accepted.</p> <p><b>action-modifiers</b>—(Optional) One or more actions to perform on a packet.</p> <p><b>from</b>—(Optional) Match packet fields to values. If not included, all packets are considered to match and the actions and action modifiers in the <b>then</b> statement are taken.</p> <p><b>match-conditions</b>—One or more conditions to make a match.</p> <p><b>only-at-create</b>—(Optional) Specify that the term is added only when the fast update filter is first created. No subsequent changes can be made to the term in the filter. Use this option only for terms that do not include subscriber-specific data in their match conditions, such as common or default terms (for example, counting the default drop packets).</p> <p><b>term-name</b>—Name that identifies the term. The name can contain letters, numbers, and hyphens (-), and can be up to 64 characters long. To include spaces in the name, enclose it in quotation marks (" ").</p> <p><b>then</b>—(Optional) Actions to take on matching packets. If not included and a packet matches all the conditions in the <b>from</b> statement, the packet is accepted.</p>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Fast Update Filters on page 581</li><li>• Configuring Terms for Fast Update Filters on page 583</li><li>• Fast Update Filter Match Conditions on page 584</li><li>• Fast Update Filter Actions and Action Modifiers on page 585</li></ul>

## term (Captive Portal Content Delivery)

<b>Syntax</b>	<pre>term <i>term-name</i> {   from {     application [ <i>application-name</i>];     destination-address <i>address</i> &lt;except&gt;;     destination-prefix-list <i>list-name</i> &lt;except&gt;;   }   then {     action;     action-modifiers;   } }</pre>
<b>Hierarchy Level</b>	[edit services captive-portal-content-delivery rule <i>rule-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Define the captive-portal-content-delivery term properties.
<b>Options</b>	<p><i>term-name</i>—Identifier for the term.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Redirecting HTTP Requests on page 613</li> </ul>

## tftp-server

<b>Syntax</b>	tftp-server <i>ip-address</i> ;
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	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.
<b>Options</b>	<i>ip-address</i> —IP address of the TFTP server.
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Address-Assignment Pools on page 68</li> </ul>

## then

---

<b>Syntax</b>	<pre>then {     action;     action-modifiers; }</pre>
<b>Hierarchy Level</b>	[edit services captive-portal-content-delivery rule <i>rule-name</i> term <i>term-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Define the captive-portal-content-delivery term actions. The action modifiers are optional.
<b>Options</b>	<p>You can configure one of the following actions:</p> <ul style="list-style-type: none"><li>• <b>accept</b>—Accept the packets and all subsequent packets in flows that match the rules.</li><li>• <b>rewrite</b>—Rewrite the packet and all subsequent packets in flows that match the rules.</li><li>• <b>redirect</b>—Redirect the packet and all subsequent packets in flows that match the rules.</li><li>• <b>insert</b>—Insert the packet and all subsequent packets in flows that match the rules.</li></ul> <p>When you select <b>rewrite</b> as the action, you can optionally configure one of the following action modifiers:</p> <ul style="list-style-type: none"><li>• <b>destination-address <i>address</i></b>—Destination address of the packet.</li><li>• <b>destination-address <i>address</i> destination-port <i>port</i></b>—Destination address and destination port of the packet.</li></ul> <p>When you select <b>redirect</b> as the action, you can optionally configure the following action modifier:</p> <ul style="list-style-type: none"><li>• <b>redirect-url</b>—Redirect URL of the packet.</li></ul> <p>When you select <b>insert</b> as the action, you can optionally configure the following action modifier:</p> <ul style="list-style-type: none"><li>• <b>subscriber-tag</b>—Subscriber tag of the packet.</li></ul>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Redirecting HTTP Requests on page 613</li><li>• <a href="#">Junos OS Routing Policy Configuration Guide</a></li></ul>

## timeout (DHCP Local Server)

<b>Syntax</b>	<code>timeout <i>timeout-value</i>;</code>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 <b>reconfigure</b>],</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> <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>reconfigure</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 <b>reconfigure</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit system services dhcp-local-server <b>reconfigure</b>],</p> <p>[edit system services dhcp-local-server dhcpv6 <b>reconfigure</b>],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> <b>reconfigure</b>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
<b>Description</b>	<p>Configure the initial value in seconds between attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. Each successive attempt doubles the interval between attempts. For example, if the first value is 2, the first retry is attempted 2 seconds after the first attempt fails. The second retry is attempted 4 seconds after the first retry fails. The third retry is attempted 8 seconds after the second retry fails, and so on. A group configuration takes precedence over a DHCP local server configuration.</p>
<b>Options</b>	<p><b><i>timeout-value</i></b>—Initial retry timeout value.</p> <p><b>Range:</b> 1 through 10 seconds</p> <p><b>Default:</b> 2 seconds</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 133</li> <li>Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 134</li> </ul>

## timeout (RADIUS)

---

<b>Syntax</b>	<code>timeout seconds;</code>
<b>Hierarchy Level</b>	[edit access <b>radius-server</b> <i>server-address</i> ], [edit access profile <i>profile-name</i> <b>radius-server</b> <i>server-address</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	Configure the amount of time that the local router or switch waits to receive a response from a RADIUS server.
<b>Options</b>	<b>seconds</b> —Amount of time to wait. <b>Range:</b> 1 through 90 seconds <b>Default:</b> 3 seconds
<b>Required Privilege Level</b>	<b>system</b> —To view this statement in the configuration. <b>system-control</b> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Router or Switch Interaction with RADIUS Servers on page 20</li><li>• Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li><li>• Example: Configuring CHAP Authentication with RADIUS</li><li>• Configuring RADIUS Authentication for L2TP</li></ul>

## timestamp-tolerance

<b>Syntax</b>	<code>timestamp-tolerance <i>seconds</i>;</code>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i>],</p> <p>[edit services mobile-ip home-agent virtual-network home-agent-address <i>ip-address</i>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.</p>
<b>Description</b>	Configure the acceptable difference between a registration request timestamp and the local time of the home agent.
<b>Options</b>	<p><b>timestamp-tolerance <i>seconds</i></b>—Acceptable difference in time between a registration request timestamp and the local time of the home agent.</p> <p><b>Range:</b> 1 through 255 seconds</p> <p><b>Default:</b> 7 seconds</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Mobile IP on page 357</li> <li>Configuring the Mobile IP Home Agent on page 358</li> </ul>

## token (DHCP Local Server)

<b>Syntax</b>	<code>token <i>token-value</i>;</code>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 <b>reconfigure</b>],</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> <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>reconfigure</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 <b>reconfigure</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit system services dhcp-local-server <b>reconfigure</b>],</p> <p>[edit system services dhcp-local-server dhcpv6 <b>reconfigure</b>],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> <b>reconfigure</b>],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> <b>reconfigure</b>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
<b>Description</b>	<p>Configure a plain-text token for all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. The token enables rudimentary entity authentication to protect against inadvertently instantiated DHCP servers. A null token (empty string) indicates that the configuration token functionality is not enabled. A group configuration takes precedence over a DHCP local server configuration. For more information about tokens, see RFC 3118, <i>Authentication for DHCP Messages</i>, section 4.</p>
<b>Options</b>	<p><b><i>token-value</i></b>—Plain-text alphanumeric string.</p> <p><b>Default:</b> null (empty string)</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 133</li> <li>Configuring a Token for DHCP Local Server Authentication on page 136</li> </ul>



## trace (DHCP Local Server)

<b>Syntax</b>	trace;
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</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> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</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> interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Enable trace operations for a group of interfaces or for a specific interface within a group.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Tracing Extended DHCP Operations on page 139</li> <li>Tracing Extended DHCP Operations for Specific Interfaces on page 144</li> </ul>

## trace (DHCP Relay Agent)

---

<b>Syntax</b>	trace;
<b>Hierarchy Level</b>	[edit forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> ], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-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> interface <i>interface-name</i> ], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Enable trace operations for a group of interfaces or for a specific interface within a group.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Tracing Extended DHCP Operations on page 139</li><li>• Tracing Extended DHCP Operations for Specific Interfaces on page 144</li></ul>

## tracoptions (General Authentication Service)

<b>Syntax</b>	<pre>tracoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;     &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>;     no-remote-trace; }</pre>
<b>Hierarchy Level</b>	[edit system processes general-authentication-service]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Configure tracing options for the general authentication service.
<b>Options</b>	<p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. All files are placed in the directory <code>/var/log</code>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. For example, when a trace file named <b>authd</b> reaches its maximum size, it is renamed <b>authd.0</b>, then <b>authd.1</b>, and finally <b>authd.2</b>, 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 <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can include the following flags:</p> <ul style="list-style-type: none"> <li>• <b>address-assignment</b>—Trace address-assignment pool events</li> <li>• <b>all</b>—Trace all tracing operations</li> <li>• <b>configuration</b>—Trace configuration events</li> <li>• <b>framework</b>—Trace authentication framework events</li> <li>• <b>gx-plus</b>—Trace Gx-Plus events</li> <li>• <b>jsrc</b>—Trace JSRC events</li> <li>• <b>ldap</b>—Trace LDAP authentication events</li> <li>• <b>local-authentication</b>—Trace local authentication events</li> <li>• <b>radius</b>—Trace RADIUS authentication events</li> </ul> <p><b>match <i>regular-expression</i></b>—(Optional) Refine the output to include lines that contain the regular expression.</p> <p><b>no-remote-trace</b>—Disable remote tracing.</p> <p><b>no-world-readable</b>—(Optional) Disable unrestricted file access.</p>

**size** *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate 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.

**Syntax:** *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

**Range:** 10240 through 1073741824

**Default:** 128 KB

**world-readable**—(Optional) Enable unrestricted file access.

<b>Required Privilege Level</b>	trace—To view this statement in the configuration. trace-control—To add this statement to the configuration.
---------------------------------	---

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Tracing General Authentication Service Processes on page 74</li></ul>
------------------------------	---

## traceoptions (ANCP)

<b>Syntax</b>	<pre> traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;         &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i> &lt;disable&gt;;     level (all   error   info   notice   verbose   warning);     no-remote-trace; } </pre>
<b>Hierarchy Level</b>	[edit protocols ancp]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.4.
<b>Description</b>	Define tracing operations for ANCP processes.
<b>Options</b>	<p><b>file <i>filename</i></b>— 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><b>files <i>number</i></b>— (Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, and finally <b>trace-file.2</b>, 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 <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can include the following flags:</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Trace all operations.</li> <li>• <b>config</b>—Trace configuration events.</li> <li>• <b>general</b>—Trace general flow.</li> <li>• <b>packet</b>—Trace ANCP packet transmit and receive operations.</li> <li>• <b>process</b>—Trace process internals.</li> <li>• <b>protocol</b>—Trace protocol events.</li> <li>• <b>restart</b>—Trace process restart flow</li> <li>• <b>routing-socket</b>—Trace routing socket events.</li> <li>• <b>session</b>—Trace connection events and flow.</li> <li>• <b>startup</b>—Trace ANCP startup events and flow.</li> <li>• <b>subscriber</b>—Trace subscriber events.</li> <li>• <b>timer</b>—Trace timer processing.</li> </ul> <p><b>level</b>—Level of tracing to perform. You can specify any of the following levels:</p>

- **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**—(Optional) Disable this trace flag.

**match *regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

**no-remote-trace**—Disable remote tracing.

**no-world-readable**—(Optional) Disable unrestricted file access.

**size *maximum-file-size***—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate 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.

**Syntax:** *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

**Range:** 10240 through 1073741824

**Default:** 128 KB

**world-readable**—(Optional) Enable unrestricted file access.

<b>Required Privilege Level</b>	trace—To view this statement in the configuration. trace-control—To add this statement to the configuration.
---------------------------------	---

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring ANCP on page 786</li><li>• Tracing ANCP Operations for Subscriber Access on page 792</li></ul>
------------------------------	--

## traceoptions (Captive Portal Content Delivery)

<b>Syntax</b>	<pre> traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i>&gt; &lt;size <i>size</i>&gt; &lt;world-readable           no-world-readable&gt;;     flag configuration;     flag general;     flag gres;     flag rtsock;     flag statistics;     flag "all";     no-remote-trace; } </pre>
<b>Hierarchy Level</b>	[edit servicescaptive-portal-content-delivery]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4. Support at the [edit services captive-portal-content-delivery] hierarchy level introduced in Junos OS Release 10.4.
<b>Description</b>	Define tracing operations for captive-portal-content-delivery processes.
<b>Options</b>	<b>file <i>filename</i></b> —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 <b>/var/log</b> . Ensure that filenames are unique for each logical system or routing instance in which Mobile IP is configured.



**NOTE:** Global messages (common to all logical systems and routing instances) are always saved in **/var/log/mipd**. Messages that are specific to a logical system or routing instance are never saved in **/var/log/mipd**. If you do not configure a trace filename for a logical system or routing instance, then nothing is traced for that entity.

**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.

**Syntax:** **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

**Range:** 10 KB through 1 GB

**Default:** 128 KB

**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.

**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 operations.
- **configuration**—Trace home agent state machine operations.
- **general**—Trace general operations.
- **gres**—Trace graceful routing switchover operations.
- **rtsock**—Trace routing socket operations.
- **statistics**—Trace statistics operations.

<b>Required Privilege</b>	trace—To view this statement in the configuration.
<b>Level</b>	trace-control—To add this statement to the configuration.

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Redirecting HTTP Requests on page 613</a></li></ul>
------------------------------	---



## traceoptions (DHCP Local Server)

<b>Syntax</b>	<pre> traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;     &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>;     no-remote-trace; } </pre>
<b>Hierarchy Level</b>	<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>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Define global tracing operations for DHCP local server processes. You use the <b>trace</b> statement to configure interface-specific tracing.
<b>Options</b>	<p><b>file <i>filename</i></b>—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><b>files <i>number</i></b>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. See “Configuring the Extended DHCP Tracing Flags” on page 142 for a list of the flags that you can include.</p> <p><b>match <i>regular-expression</i></b>—(Optional) Refine the output to include lines that contain the regular expression.</p> <p><b>no-remote-trace</b>—Disable remote tracing.</p> <p><b>no-world-readable</b>—(Optional) Allow only the user <b>root</b> and users who have the Junos <b>maintenance</b> permission to access the trace files.</p> <p><b>size <i>maximum-file-size</i></b>—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate 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 <b>files</b> option.</p> <p><b>Syntax:</b> <b>sizek</b> to specify KB, <b>sizem</b> to specify MB, or <b>sizeg</b> to specify GB</p> <p><b>Range:</b> 10240 through 1073741824</p> <p><b>Default:</b> 128 KB</p> <p><b>world-readable</b>—(Optional) Enable all users to access the trace files.</p>

<b>Required Privilege</b>	trace—To view this statement in the configuration.
<b>Level</b>	trace-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Tracing Extended DHCP Operations on page 139</li><li>• Configuring the Extended DHCP Log Filename on page 140</li><li>• Configuring the Number and Size of Extended DHCP Log Files on page 141</li><li>• Configuring Access to the Extended DHCP Log File on page 141</li><li>• Configuring a Regular Expression for Extended DHCP Lines to Be Logged on page 142</li><li>• Configuring the Extended DHCP Tracing Flags on page 142</li></ul>

## traceoptions (DHCP Relay Agent)

<b>Syntax</b>	<pre> traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;     &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>;     no-remote-trace; } </pre>
<b>Hierarchy Level</b>	<pre> [edit forwarding-options dhcp-relay], [edit logical-systems <i>logical-system-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], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay] </pre>
<b>Release Information</b>	Statement introduced in Junos OS Release 8.5.
<b>Description</b>	Configure global tracing operations for extended DHCP relay agent processes. You use the <b>trace</b> statement to configure interface-specific tracing.
<b>Default</b>	If you do not include this statement, no global tracing operations are performed.
<b>Options</b>	<p><b>file <i>filename</i></b>—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 <b>/var/log</b>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. See “Configuring the Extended DHCP Tracing Flags” on page 142 for a list of the flags that you can include.</p> <p><b>match <i>regular-expression</i></b>—(Optional) Refine the output to include lines that contain the regular expression.</p> <p><b>no-remote-trace</b>—Disable remote tracing.</p> <p><b>no-world-readable</b>—(Optional) Disable unrestricted file access.</p> <p><b>size <i>maximum-file-size</i></b>—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate 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 <b>files</b> option.</p> <p><b>Syntax:</b> <b>sizek</b> to specify KB, <b>sizem</b> to specify MB, or <b>sizeg</b> to specify GB</p> <p><b>Range:</b> 10240 through 1073741824</p> <p><b>Default:</b> 128 KB</p>

**world-readable**—(Optional) Enable all users to access the trace files.

**Required Privilege Level**    trace—To view this statement in the configuration.  
                                     trace-control—To add this statement to the configuration.

**Related Documentation**

- Tracing Extended DHCP Operations on page 139
- Configuring the Extended DHCP Log Filename on page 140
- Configuring the Number and Size of Extended DHCP Log Files on page 141
- Configuring Access to the Extended DHCP Log File on page 141
- Configuring a Regular Expression for Extended DHCP Lines to Be Logged on page 142
- Configuring the Extended DHCP Tracing Flags on page 142

## traceoptions (Diameter Base Protocol)

<b>Syntax</b>	<pre> traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;         &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>;     level (all   error   info   notice   verbose   warning);     no-remote-trace; } </pre>
<b>Hierarchy Level</b>	[edit system processes diameter-service]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Define tracing options for Diameter processes.
<b>Options</b>	<p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. Enclose the filename within quotation marks. All files are placed in the directory <code>/var/log</code>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, and finally <b>trace-file.2</b>, 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 <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can include the following flags:</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Trace all operations</li> <li>• <b>application</b>—Trace Diameter application interface events</li> <li>• <b>configuration</b>—Trace configuration events</li> <li>• <b>daemon</b>—Trace Diameter daemon level events</li> <li>• <b>diameter-instance</b>—Trace Diameter instance events</li> <li>• <b>dne</b>—Trace Diameter network element events</li> <li>• <b>framework</b>—Trace Diameter framework events</li> <li>• <b>memory-management</b>—Trace memory management events</li> <li>• <b>messages</b>—Trace Diameter messages</li> <li>• <b>node</b>—Trace Diameter node events</li> <li>• <b>peer</b>—Trace Diameter peer events</li> </ul> <p><b>level</b>—Level of tracing to perform. You can specify any of the following levels:</p> <ul style="list-style-type: none"> <li>• <b>all</b>—Match all levels.</li> </ul>

- **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.

**match *regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

**no-remote-trace**—Disable remote tracing.

**no-world-readable**—(Optional) Disable unrestricted file access.

**size *maximum-file-size***—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate 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.

**Syntax:** *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

**Range:** 10240 through 1073741824

**Default:** 128 KB

**world-readable**—(Optional) Enable unrestricted file access.

<b>Required Privilege</b>	trace—To view this statement in the configuration.
<b>Level</b>	trace-control—To add this statement to the configuration.

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Tracing Diameter Base Protocol Processes for Subscriber Access on page 262</li></ul>
------------------------------	--

## traceoptions (L2TP)

<b>Syntax</b>	<pre> traceoptions {   debug-level <i>level</i>;   file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;     &lt;world-readable   no-world-readable&gt;;   filter {     protocol <i>name</i>;     user-name <i>username</i>;   }   flag <i>flag</i>;   interfaces <i>interface-name</i> {     debug-level <i>level</i>;     flag <i>flag</i>;   }   level (all   error   info   notice   verbose   warning);   no-remote-trace; } </pre>
<b>Hierarchy Level</b>	[edit services l2tp]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4. Support for L2TP LAC introduced in Junos OS Release 10.4.
<b>Description</b>	Define tracing operations for L2TP processes.
<b>Options</b>	<p><b>debug-level <i>level</i></b>—Trace level for PPP, L2TP, RADIUS, and UDP; this option does not apply to L2TP LAC on MX Series routers:</p> <ul style="list-style-type: none"> <li>• <b>detail</b>—Trace detailed debug information.</li> <li>• <b>error</b>—Trace error information.</li> <li>• <b>packet-dump</b>—Trace packet decoding information.</li> </ul> <p><b>file <i>filename</i></b>—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 <b>/var/log</b>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, and finally <b>trace-file.2</b>, 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 <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>filter protocol <i>name</i></b>—Additional filter for the specified protocol; this option does not apply to L2TP LAC on MX Series routers:</p> <ul style="list-style-type: none"> <li>• <b>l2tp</b></li> <li>• <b>ppp</b></li> </ul>

- **radius**
- **udp**

**filter user-name** *username*—Additional filter for the specified username; this option does not apply to L2TP LAC on MX Series routers.

**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.
- **configuration**—Trace configuration events.
- **events**—Trace interface events.
- **general**—Trace general events.
- **gres**—Trace GRES events.
- **init**—Trace daemon initialization.
- **ipc-rx**—Trace IPC receive events.
- **ipc-tx**—Trace IPC transmit events.
- **memory**—Trace memory management code.
- **message**—Trace message processing code.
- **packet-error**—Trace packet error events.
- **parse**—Trace parsing events.
- **protocol**—Trace L2TP events.
- **receive-packets**—Trace received L2TP packets.
- **routing-process**—Trace routing process interactions.
- **routing-socket**—Trace routing socket events.
- **session-db**—Trace session database interactions.
- **states**—Trace state machine events.
- **timer**—Trace timer events.
- **transmit-packets**—Trace transmitted L2TP packets.
- **tunnel**—Trace tunnel events.

**interfaces** *interface-name*—Apply L2TP traceoptions to a specific services interface. This option does not apply to L2TP LAC on MX Series routers.



- **debug-level *level***—Trace level for the interface; this option does not apply to L2TP LAC on MX Series routers:
  - **detail**—Trace detailed debug information.
  - **error**—Trace error information.
  - **extensive**—Trace all PIC debug information.
- **flag *flag***—Tracing operation to perform for the interface. This option does not apply to L2TP LAC on MX Series routers. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:
  - **all**—Trace everything.
  - **ipc**—Trace L2TP Inter-Process Communication (IPC) messages between the PIC and the Routing Engine.
  - **packet-dump**—Dump each packet content based on debug level.
  - **protocol**—Trace L2TP, PPP, and multilink handling.
  - **system**—Trace packet processing on the PIC.

**level**—Specify 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.

**match *regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

**no-remote-trace**—Disable remote tracing.

**no-world-readable**—(Optional) Disable unrestricted file access.

**size *maximum-file-size***—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate 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.

**Syntax:** *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

**Range:** 10240 through 1073741824

**world-readable**—(Optional) Enable unrestricted file access.

<b>Required Privilege Level</b>	trace—To view this statement in the configuration. trace-control—To add this statement to the configuration.
---------------------------------	---

- Related Documentation**
- For information about configuration for L2TP LAC on MX Series routers, see [Configuring an L2TP LAC on page 241](#)
  - For information about L2TP LAC tracing on MX Series routers, see [Tracing L2TP Operations for Subscriber Access on page 247](#)
  - For information about L2TP tracing on M Series routers, see [Tracing L2TP Operations](#)

## traceoptions (Mobile IP)

<b>Syntax</b>	<pre> traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;         &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>;     level (all   error   info   notice   verbose   warning);     no-remote-trace; } </pre>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip],  [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip],  [edit routing-instances <i>routing-instances-name</i> services mobile-ip],  [edit services mobile-ip]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.</p>
<b>Description</b>	Define tracing operations for Mobile IP processes.
<b>Options</b>	<p><b>file <i>filename</i></b>— 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 <b>/var/log</b>. Ensure that filenames are unique for each logical system or routing instance in which Mobile IP is configured.</p>



**NOTE:** Global messages (common to all logical systems and routing instances) are always saved in **/var/log/mipd**. Messages that are specific to a logical system or routing instance are never saved in **/var/log/mipd**. If you do not configure a trace filename for a logical system or routing instance, then nothing is traced for that entity.

**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 finally **trace-file.2**, 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.

**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 operations.

- **authentication**—Trace authentication operations.
- **binding**—Trace bindings.
- **event**—Trace events.
- **ha-fsm**—Trace home agent state machine operations.
- **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.
- **timer**—Trace timer events.
- **trace**—Trace changes in tracing.
- **tunnel**—Trace tunneling operations.
- **user-interface**—Trace user interface events.

**level**—Specify 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.

**match *regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

**no-world-readable**—(Optional) Disable unrestricted file access.

**size *maximum-file-size***—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate 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.

**Syntax:** *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

**Range:** 10240 through 1073741824

**Default:** 128 KB

**world-readable**—(Optional) Enable unrestricted file access.

**Required Privilege** trace—To view this statement in the configuration.  
**Level** trace-control—To add this statement to the configuration.

**Related Documentation**

- Configuring Mobile IP on page 357
- Tracing Mobile IP Operations for Subscriber Access on page 361

## traceoptions (PTSP)

---

<b>Syntax</b>	<pre>traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;     &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i> &lt;disable&gt;;     no-remote-trace; }</pre>
<b>Hierarchy Level</b>	[edit system services packet-triggered-subscribers]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.2.
<b>Description</b>	Define tracing operations for PTSP.
<b>Options</b>	<p><b>file <i>filename</i></b>—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 <b>/var/log</b>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, and finally <b>trace-file.2</b>, 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 <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can include the following flags:</p> <ul style="list-style-type: none"><li>• <b>all</b>—Trace all operations.</li><li>• <b>configuration</b>—Trace configuration events.</li><li>• <b>general</b>—Trace general flow.</li><li>• <b>peer</b>—Trace SRC peer events.</li><li>• <b>pic</b>—Trace PIC events.</li><li>• <b>rtsock</b>—Trace routing socket events.</li><li>• <b>session</b>—Trace session events.</li></ul> <p><b>disable</b>—Disable this trace flag.</p> <p><b>match <i>regular-expression</i></b>—(Optional) Refine the output to include lines that contain the regular expression.</p> <p><b>no-remote-trace</b>—Disable remote tracing.</p> <p><b>no-world-readable</b>—(Optional) Disable unrestricted file access.</p> <p><b>size <i>maximum-file-size</i></b>—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to</p>

indicate 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.

**Syntax:** *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

**Range:** 10240 through 1073741824

**Default:** 128 KB

**world-readable**—(Optional) Enable unrestricted file access.

<b>Required Privilege</b>	trace—To view this statement in the configuration.
<b>Level</b>	trace-control—To add this statement to the configuration.

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Tracing Packet-Triggered Subscriber Operations on page 313</li></ul>
------------------------------	--

## traceoptions (Static Subscribers)

---

Syntax	<pre>traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i>&gt; &lt;size <i>maximum-file-size</i>&gt;     &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>;     level (all   error   info   notice   verbose   warning);     no-remote-trace; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> system processes static-subscribers],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system processes static-subscribers],</p> <p>[edit routing-instances <i>routing-instances-name</i> system processes static-subscribers],</p> <p>[edit system processes static-subscribers]</p>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Define tracing operations for static subscriber processes.
Options	<p><b>file <i>filename</i></b>— 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 <b>/var/log</b>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, and finally <b>trace-file.2</b>, 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 <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can include the following flags:</p> <ul style="list-style-type: none"><li>• <b>all</b>—Trace all operations.</li><li>• <b>authentication</b>—Trace authentication events.</li><li>• <b>configuration</b>—Trace configuration events.</li><li>• <b>database</b>—Trace database events.</li><li>• <b>general</b>—Trace general events.</li><li>• <b>gres</b>—Trace GRES events.</li><li>• <b>profile</b>—Trace dynamic profile events.</li><li>• <b>rtsock</b>—Trace routing socket events.</li><li>• <b>statistics</b>—Trace statistics events.</li><li>• <b>subscriber</b>—Trace subscriber events.</li></ul> <p><b>level</b>—Level of tracing to perform. You can specify any of the following levels:</p>



- **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.

**match *regular-expression***—(Optional) Refine the output to include lines that contain the regular expression.

**no-remote-trace**—(Optional) Disable remote tracing.

**no-world-readable**—(Optional) Disable unrestricted file access.

**size *maximum-file-size***—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate 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.

**Syntax:** *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

**Range:** 10240 through 1073741824

**Default:** 128 KB

**world-readable**—(Optional) Enable unrestricted file access.

<b>Required Privilege</b>	trace—To view this statement in the configuration.
<b>Level</b>	trace-control—To add this statement to the configuration.

<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Subscribers over Static Interfaces on page 288</li><li>• Tracing Static Subscriber Operations on page 297</li></ul>
------------------------------	---

## traceoptions (Subscriber Management)

---

<b>Syntax</b>	<pre>traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;     &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>; }</pre>
<b>Hierarchy Level</b>	[edit system services subscriber-management]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.1.
<b>Description</b>	Define tracing operations for subscriber management interface processes.
<b>Options</b>	<p><b>file <i>filename</i></b>—Name of the file to receive the output of the tracing operation. Enclose the filename within quotation marks. All files are placed in the directory <b>/var/log</b>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, and finally <b>trace-file.2</b>, 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 <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can include the following flags:</p> <ul style="list-style-type: none"><li>• <b>all</b>—Trace all operations.</li><li>• <b>database</b>—Trace database events.</li><li>• <b>general</b>—Trace general events.</li><li>• <b>issu</b>—Trace unified ISSU events.</li><li>• <b>server</b>—Trace server events.</li><li>• <b>session-db</b>—Trace session database interactions.</li><li>• <b>ui</b>—Trace user interface events.</li></ul> <p><b>match <i>regular-expression</i></b>—(Optional) Refine the output to include lines that contain the regular expression.</p> <p><b>no-world-readable</b>—(Optional) Disable unrestricted file access.</p> <p><b>size <i>maximum-file-size</i></b>—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate 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 <b>files</b> option.</p> <p><b>Syntax:</b> <b>sizek</b> to specify KB, <b>sizem</b> to specify MB, or <b>sizeg</b> to specify GB</p> <p><b>Range:</b> 10240 through 1073741824</p>

**Default:** 128 KB

**world-readable**—(Optional) Enable unrestricted file access.

**Required Privilege** trace—To view this statement in the configuration.  
**Level** trace-control—To add this statement to the configuration.

**Related Documentation**

- [Tracing Subscriber Management Database Operations for Subscriber Access on page 58](#)
- [Configuring the Subscriber Management Database Trace Log Filename on page 59](#)
- [Configuring the Number and Size of Subscriber Management Database Log Files on page 59](#)
- [Configuring Access to the Subscriber Management Database Log File on page 59](#)
- [Configuring a Regular Expression for Subscriber Management Database to Be Logged on page 60](#)
- [Configuring the Subscriber Management Database Tracing Flags on page 60](#)

## traceoptions (Subscriber Session Database Replication)

---

<b>Syntax</b>	<pre>traceoptions {     file <i>filename</i> &lt;files <i>number</i>&gt; &lt;match <i>regular-expression</i> &gt; &lt;size <i>maximum-file-size</i>&gt;     &lt;world-readable   no-world-readable&gt;;     flag <i>flag</i>;     no-remote-trace; }</pre>
<b>Hierarchy Level</b>	[edit system services <b>database-replication</b> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Define tracing operations for subscriber management session database replication processes.
<b>Options</b>	<p><b>file <i>filename</i></b>—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 <b>/var/log</b>.</p> <p><b>files <i>number</i></b>—(Optional) Maximum number of trace files. When a trace file named <b>trace-file</b> reaches its maximum size, it is renamed <b>trace-file.0</b>, then <b>trace-file.1</b>, and finally <b>trace-file.2</b>, 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 <b>size</b> option.</p> <p><b>Range:</b> 2 through 1000</p> <p><b>Default:</b> 3 files</p> <p><b>flag <i>flag</i></b>—Tracing operation to perform. To specify more than one tracing operation, include multiple <b>flag</b> statements. You can include the following flags:</p> <ul style="list-style-type: none"><li>• <b>all</b>—Trace all operations.</li><li>• <b>database</b>—Trace database events.</li><li>• <b>general</b>—Trace general flow.</li><li>• <b>mirror</b>—Trace mirroring events.</li><li>• <b>replication</b>—Trace database replication events.</li><li>• <b>server</b>—Trace server events.</li><li>• <b>session-db</b>—Trace session database interactions.</li><li>• <b>ui</b>—Trace user interface events.</li></ul> <p><b>match <i>regular-expression</i></b>—(Optional) Refine the output to include lines that contain the regular expression.</p> <p><b>no-remote-trace</b>—Disable remote tracing.</p> <p><b>no-world-readable</b>—(Optional) Disable unrestricted file access.</p>

**size maximum-file-size**—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate 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.

**Syntax:** **sizek** to specify KB, **sizem** to specify MB, or **sizeg** to specify GB

**Range:** 10240 through 1073741824

**Default:** 128 KB

**world-readable**—(Optional) Enable unrestricted file access.

<b>Required Privilege</b>	trace—To view this statement in the configuration.
<b>Level</b>	trace-control—To add this statement to the configuration.

- |                              |   |
|------------------------------|---|
| <b>Related Documentation</b> | <ul style="list-style-type: none"><li>• Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 61</li><li>• Configuring the Subscriber Management Session Database Replication Trace Log Filename on page 64</li><li>• Configuring the Number and Size of Subscriber Management Session Database Replication Log Files on page 62</li><li>• Configuring Access to the Subscriber Management Session Database Replication Log File on page 63</li><li>• Configuring a Regular Expression for Subscriber Management Session Database Replication to Be Logged on page 63</li><li>• Configuring the Subscriber Management Session Database Replication Tracing Flags on page 64</li></ul> |
|------------------------------|---|

## traffic-control-profiles (Dynamic CoS Definition)

---

<b>Syntax</b>	<pre>traffic-control-profiles <i>profile-name</i> {     delay-buffer-rate (percent <i>percentage</i>   <i>rate</i>);     excess-rate (percent <i>percentage</i>   proportion <i>value</i>   percent \$junos-cos-excess-rate);     guaranteed-rate (percent <i>percentage</i>   <i>rate</i>);     overhead-accounting (<i>shaping-mode</i>) &lt;bytes (<i>byte-value</i>&gt;;     scheduler-map <i>map-name</i>;     shaping-rate (percent <i>percentage</i>   <i>rate</i>   <i>predefined-variable</i>); }</pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Configure traffic shaping and scheduling profiles.
<b>Options</b>	<p><i>profile-name</i>—Name of the traffic-control profile.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>Configuring Traffic Scheduling and Shaping for Subscriber Access on page 677</li><li>output-traffic-control-profile on page 1092</li></ul>

## transmit-rate (Dynamic Schedulers)

<b>Syntax</b>	<code>transmit-rate (rate   percent <i>percentage</i>   remainder   percent <i>percentage</i> \$junos-cos-scheduler-tx) &lt;exact   rate-limit&gt;;</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. The <code>\$junos-cos-scheduler-tx</code> predefined variable introduced in Junos OS Release 9.4.
<b>Description</b>	Specify the transmit rate or percentage for a scheduler in a dynamic profile.
<b>Default</b>	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.
<b>Options</b>	<p><b>rate</b>—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 <b>k</b> (1000), <b>m</b> (1,000,000), or <b>g</b> (1,000,000,000).  <b>Range:</b> 3200 through 160,000,000,000 bps</p> <p><b>percent <i>percentage</i></b>—Percentage of transmission capacity. A percentage of zero drops all packets in the queue.  <b>Range:</b> 0 through 100 percent</p> <p><b>remainder</b>—Use remaining rate available.</p> <p><b>\$junos-cos-scheduler-tx</b>—Junos predefined variable that is replaced with the transmission rate obtained from the RADIUS server when a subscriber authenticates over the interface to which the dynamic profile is attached.</p> <p><b>exact</b>—(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><b>rate-limit</b>—(Optional) Limit the transmission rate to the rate-controlled amount during congestion. In contrast to the <b>exact</b> option, when there is no congestion, the scheduler with the <b>rate-limit</b> option shares unused bandwidth above the rate-controlled amount.</p>
<b>Required Privilege Level</b>	<p><b>interface</b>—To view this statement in the configuration.</p> <p><b>interface-control</b>—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li> <li>Configuring Schedulers in a Dynamic Profile for Subscriber Access on page 679</li> <li><b>scheduler</b> on page 1174</li> </ul>

## transport (Diameter Base Protocol)

---

<b>Syntax</b>	<pre>transport <i>transport-name</i> {     address;     logical-system <i>logical-system-name</i> &lt;routing-instance <i>routing-instance-name</i> &gt;;     routing-instance <i>routing-instance-name</i> }</pre>
<b>Hierarchy Level</b>	[edit diameter]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Configure the Diameter instance and the local IP address for the Diameter local transport connection.
<b>Options</b>	<p><i>transport-name</i>—Name of the transport.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Diameter on page 259</li><li>Configuring the Diameter Transport on page 262</li></ul>

## transport (Diameter Peer)

---

<b>Syntax</b>	<pre>transport <i>transport-name</i>;</pre>
<b>Hierarchy Level</b>	[edit diameter peer <i>peer-name</i> connect-actively]
<b>Release Information</b>	Statement introduced in Junos OS Release 11.2.
<b>Description</b>	Specify the transport layer connection to be used for establishing active connections to the peer.
<b>Default</b>	The transport is defined in the default logical system and master routing instance.
<b>Options</b>	<p><i>transport-name</i>—Name of the transport.</p>
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Diameter on page 259</li><li>Configuring Diameter Peers on page 260</li></ul>



## trigger (DHCP Local Server)

<b>Syntax</b>	<pre>trigger {     radius-disconnect; }</pre>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</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> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
<b>Description</b>	<p>Configure behavior in response to a trigger for all DHCP clients or only the DHCP clients serviced by the specified group of interfaces.</p> <p>The remaining statement is explained separately.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 133</li> <li>Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 136</li> <li>radius-disconnect (DHCP Local Server) on page 1139</li> </ul>

## trust-option-82

---

<b>Syntax</b>	trust-option-82;
<b>Hierarchy Level</b>	[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], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]
<b>Release Information</b>	Statement introduced in Junos OS Release 8.3.
<b>Description</b>	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.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Extended DHCP Relay Agent Overview on page 154</li></ul>

## tunnel (Tunnel Profile)

<b>Syntax</b>	<pre> tunnel <i>tunnel-id</i> {     identification <i>name</i>;     logical-system <i>logical-system-name</i>;     max-sessions <i>number</i>;     medium <i>type</i>;     preference <i>number</i>;     remote-gateway {         address <i>server-ip-address</i>;         gateway-name <i>server-name</i>;     }     routing-instance <i>routing-instance-name</i>;     secret <i>password</i>;     source-gateway {         address <i>client-ip-address</i>;         gateway-name <i>client-name</i>;     }     type <i>tunnel-type</i>; } </pre>
<b>Hierarchy Level</b>	[edit access tunnel-profile <i>profile-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Define the attributes of a tunnel for the tunnel profile. You can define up to 31 tunnels for each tunnel profile.
<b>Options</b>	<p><b><i>tunnel-id</i></b>—Unique integer that identifies a tunnel defined within a profile. For a subscriber, RADIUS attributes and VSAs can supply or override the attributes defined here for the tunnel.</p> <p><b>Range:</b> 1 through 31</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring a Tunnel Profile for Subscriber Access on page 242</li> </ul>

## tunnel-profile (Domain Maps)

---

<b>Syntax</b>	<code>tunnel-profile <i>profile-name</i>;</code>
<b>Hierarchy Level</b>	[edit access domain map <i>domain-map-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Tunnel profile that provides definitions for tunnels associated with the domain map.
<b>Options</b>	<i>profile-name</i> —Name of tunnel profile.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Specifying a Tunnel Profile in a Domain Map on page 88</li></ul>

## tunnel-profile (Tunnel Profile)


<b>Syntax</b>	<pre> tunnel-profile <i>profile-name</i> {     tunnel <i>tunnel-id</i> {         identification <i>name</i>;         logical-system <i>logical-system-name</i>;         max-sessions <i>number</i>;         medium <i>type</i>;         preference <i>number</i>;         remote-gateway {             address <i>server-ip-address</i>;             gateway-name <i>server-name</i>;         }         routing-instance <i>routing-instance-name</i>;         secret <i>password</i>;         source-gateway {             address <i>client-ip-address</i>;             gateway-name <i>client-name</i>;         }         type <i>tunnel-type</i>;     } } </pre>
<b>Hierarchy Level</b>	[edit access]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Define a tunnel profile for subscriber access.
<b>Options</b>	<p><b><i>profile-name</i></b>—Unique name that identifies the tunnel profile. The profile can be referenced from within a domain map or by the RADIUS Tunnel-Group VSA [26-64].</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring a Tunnel Profile for Subscriber Access on page 242</li> </ul>

## type (Tunnel Profile)

---

<b>Syntax</b>	<code>type <i>tunnel-type</i>;</code>
<b>Hierarchy Level</b>	<code>[edit access tunnel-profile <i>profile-name</i> tunnel <i>tunnel-id</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify the tunnel type (protocol).
<b>Default</b>	<code>l2tp</code>
<b>Options</b>	<i>tunnel-type</i> —Tunnel protocol type. The only value currently available is <code>l2tp</code> .
<b>Required Privilege Level</b>	<code>admin</code> —To view this statement in the configuration. <code>admin-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Tunnel Profile for Subscriber Access on page 242</li></ul>

## underlying-interface (demux0)

<b>Syntax</b>	<code>underlying-interface <i>underlying-interface-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> interfaces demux0 <i>interface-name</i> unit unit <i>logical-unit-number</i> demux-options]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3. Support for aggregated Ethernet introduced in Junos OS Release 9.4.
<b>Description</b>	Configure the underlying interface on which the demultiplexing (demux) interface is running.
<b>Options</b>	<p><b><i>underlying-interface-name</i></b>—Either the specific name of the interface on which the DHCP discover packet arrives or one of the following interface variables:</p> <ul style="list-style-type: none"> <li>• <b><i>\$junos-underlying-interface</i></b> when configuring dynamic IP demux interfaces.</li> <li>• <b><i>\$junos-interface-ifd-name</i></b> when configuring dynamic VLAN demux interfaces.</li> </ul> <p>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.</p>
<div>  <p><b>NOTE:</b> Logical demux interfaces are currently supported on Gigabit Ethernet, Fast Ethernet, 10-Gigabit Ethernet, or aggregated Ethernet interfaces.</p> </div>	
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Configuring Static Subscriber Interfaces Using IP Demux Interfaces on page 440</li> <li>• Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 445</li> <li>• Configuring Static Subscriber Interfaces Using VLAN Demux Interfaces on page 441</li> <li>• Configuring Dynamic Subscriber Interfaces Using VLAN Demux Interfaces in Dynamic Profiles on page 446</li> <li>• For information about static underlying interfaces, see the <a href="#">Junos OS Network Interfaces Configuration Guide</a></li> </ul>

## underlying-interface (Dynamic PPPoE)

---

<b>Syntax</b>	<code>underlying-interface <i>interface-name</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" ppoe-options]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	In a dynamic profile, configure the underlying interface on which the router creates the dynamic PPPoE logical interface.
<b>Options</b>	<b><i>interface-name</i></b> —Variable used to specify the name of the underlying interface on which the PPPoE logical interface is dynamically created. In the <b>underlying-interface <i>interface-name</i></b> statement for dynamic PPPoE logical interfaces, you must use the predefined variable <b>\$junos-underlying-interface</b> in place of <b><i>interface-name</i></b> . When the router creates the dynamic PPPoE interface, the <b>\$junos-underlying-interface</b> predefined variable is dynamically replaced with the name of the underlying interface supplied by the network when the subscriber logs in.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Basic PPPoE Dynamic Profile on page 536</li><li>For information about creating static PPPoE interfaces, see the <a href="#">Junos OS Network Interfaces Configuration Guide</a></li></ul>



## unit (Dynamic Demux Interface)

```
Syntax  unit logical-unit-number {
        demux-options {
            underlying-interface interface-name
        }
        family family {
            access-concentrator name;
            address address;
            demux-source {
                source-address;
            }
            duplicate-protection;
            dynamic-profile profile-name;
            filter {
                input filter-name;
                output filter-name;
            }
            mac-validate (loose | strict);
            max-sessions number;
            service-name-table table-name
            unnumbered-address interface-name <preferred-source-address address>;
        }
        filter {
            input filter-name;
            output filter-name;
        }
    }
    vlan-id number;
```

**Hierarchy Level** [edit dynamic-profiles *profile-name* interfaces demux0]

**Release Information** Statement introduced in Junos OS 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 Documentation**

- Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles on page 445

- For information about static IP demux interfaces, see the *[Junos OS Network Interfaces Configuration Guide](#)*

## unit (Dynamic PPPoE)

<b>Syntax</b>	<pre> unit <i>logical-unit-number</i> {     keepalives interval <i>seconds</i>;     no-keepalives;     pppoe-options {         underlying-interface <i>interface-name</i>;         server;     }     ppp-options {         chap;         pap;     }     family inet {         unnumbered-address <i>interface-name</i> <i>destination address</i>;         address <i>address</i>;         service {             input {                 service-set <i>service-set-name</i> {                     service-filter <i>filter-name</i>;                 }                 post-service-filter <i>filter-name</i>;             }             output {                 service-set <i>service-set-name</i> {                     service-filter <i>filter-name</i>;                 }             }         }         filter {             input <i>filter-name</i> {                 precedence <i>precedence</i>;             }             output <i>filter-name</i> {                 precedence <i>precedence</i>;             }         }     }     filter {         input <i>filter-name</i>;         output <i>filter-name</i>;     } } </pre>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces pp0]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	In a dynamic profile, configure a logical unit number for the dynamic PPPoE logical interface. You must configure a logical interface to be able to use the router.
<b>Options</b>	<b><i>logical-unit-number</i></b> —Variable used to specify the unit number when the PPPoE logical interface is dynamically created. In the <b>unit <i>logical-unit-number</i></b> statement for dynamic

PPPoE logical interfaces, you must use the predefined variable **\$junos-interface-unit** in place of **logical-unit-number**. The **\$junos-interface-unit** predefined variable is dynamically replaced with the unit number supplied by the router when the subscriber logs in.

The remaining statements are explained separately.

<b>Required Privilege Level</b>	interface—To view this statement in the configuration.
	interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	• Configuring a Basic PPPoE Dynamic Profile on page 536
	• For information about creating static PPPoE interfaces, see the <a href="#">Junos OS Network Interfaces Configuration Guide</a>

## unit (Dynamic Traffic Shaping)

<b>Syntax</b>	<pre> unit <i>logical-unit-number</i> {     classifiers {         type (<i>classifier-name</i>   default);     }     output-traffic-control-profile <i>profile-name</i>;     rewrite-rules {         dscp (<i>rewrite-name</i>   default);         dscp-ipv6 (<i>rewrite-name</i>   default);         ieee-802.1 (<i>rewrite-name</i>   default) vlan-tag (outer   outer-and-inner);         inet-precedence (<i>rewrite-name</i>   default);     } } </pre>
<b>Hierarchy Level</b>	<p>[edit dynamic-profiles <i>profile-name</i> class-of-service interfaces <i>interface-name</i>]</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces interface-set <i>interface-set-name</i> interface <i>interface-name</i>]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.2.</p> <p>Support at the [edit dynamic-profiles <i>profile-name</i> class-of-service interfaces interface-set <i>interface-set-name</i>] hierarchy level introduced in Junos OS Release 10.4.</p>
<b>Description</b>	<p>Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.</p>
<b>Options</b>	<p><b><i>logical-unit-number</i></b>—One of the following options:</p> <ul style="list-style-type: none"> <li>• <b><i>\$junos-underlying-interface-unit</i></b>—For static VLANs, the unit number variable. 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 when it accesses the subscriber network.</li> <li>• <b><i>\$junos-interface-unit</i></b>—For dynamic demux and dynamic PPPoE interfaces, the unit number variable. 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 or PPP when it accesses the subscriber network.</li> <li>• <b><i>value</i></b>—Specific unit number of the interface you want to assign to the dynamic-profile</li> </ul> <p><b>Range:</b> 0 through 16385. For demux and PPPoE interfaces, the unit numbers can range from 0 through 1,073,741,823.</p> <p>The remaining statements are explained separately. The <b>classifiers</b>, <b>output-traffic-control-profile</b>, and <b>rewrite-rules</b> statements are not supported for interface sets.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

**Related  
Documentation**

- Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660
- Applying Traffic Shaping and Scheduling to a Subscriber Interface in a Dynamic Profile on page 685
- Configuring an Interface Set of Subscribers in a Dynamic Profile on page 712

## unit (Dynamic Profiles Standard Interface)

```

Syntax  unit logical-unit-number {
    encapsulation (atm-ccc-cell-relay | atm-ccc-vc-mux | atm-cisco-nlpid | atm-tcc-vc-mux
    | atm-mlppp-llc | atm-nlpid | atm-ppp-llc | atm-ppp-vc-mux | atm-snap | atm-tcc-snap
    | atm-vc-mux | ether-over-atm-llc | ether-vpls-over-atm-llc | ether-vpls-over-fr |
    ether-vpls-over-ppp | ethernet | frame-relay-ccc | frame-relay-ppp | frame-relay-tcc |
    frame-relay-ether-type | frame-relay-ether-type-tcc | multilink-frame-relay-end-to-end
    | multilink-ppp | ppp-over-ether | ppp-over-ether-over-atm-llc | vlan-bridge | vlan-ccc |
    vlan-vci-ccc | vlan-tcc | vlan-vpls);
    family family {
        access-concentrator name;
        address address;
        duplicate-protection;
        dynamic-profile profile-name;
        filter {
            adf {
                counter;
                input-precedence precedence;
                output-precedence precedence;
                rule rule-value;
            }
            input filter-name (
                precedence precedence;
            )
            output filter-name {
                precedence precedence;
            }
        }
        max-sessions number;
        service {
            input {
                service-set service-set-name {
                    service-filter filter-name;
                }
                post-service-filter filter-name;
            }
            input-vlan-map {
                inner-tag-protocol-id tpid;
                inner-vlan-id number;
                (push | swap);
                tag-protocol-id tpid;
                vlan-id number;
            }
            output {
                service-set service-set-name {
                    service-filter filter-name;
                }
            }
            output-vlan-map {
                inner-tag-protocol-id tpid;
                inner-vlan-id number;
                (pop | swap);
                tag-protocol-id tpid;
            }
        }
    }
}

```

```
        vlan-id number;  
    }  
}  
service-name-table table-name  
unnumbered-address interface-name <preferred-source-address address>;  
filter {  
    input filter-name;  
    output filter-name;  
}  
keepalives {  
    interval seconds;  
}  
ppp-options {  
    chap;  
    pap;  
}  
vlan-id number;  
vlan-tags outer [tpid].vlan-id [inner [tpid].vlan-id];  
}  
}
```

**Hierarchy Level** [edit *dynamic-profiles profile-name interfaces interface-name*]

**Release Information** Statement introduced in Junos OS 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.

The remaining statements are explained separately.

**Required Privilege** interface—To view this statement in the configuration.  
**Level** interface-control—To add this statement to the configuration.



## unnumbered-address (Dynamic Profiles)

<b>Syntax</b>	<code>unnumbered-address interface-name &lt;preferred-source-address address&gt;;</code>
<b>Hierarchy Level</b>	<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>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.2.</p> <p><b>\$junos-preferred-source-address</b> variable support added in JUNOS Release 9.6.</p> <p>Support for the <b>\$junos-loopback-interface</b> predefined variable introduced in Junos OS Release 9.6.</p>
<b>Description</b>	<p>For Ethernet interfaces, enable the local address to be derived from the specified interface. Configuring unnumbered Ethernet interfaces enables IP processing on the interface without assigning an explicit IP address to the interface. To configure unnumbered address dynamically, include the <b>\$junos-loopback-interface-address</b> predefined variable.</p> <p>You can configure unnumbered address support on Ethernet interfaces for IPv4 and IPv6 address families.</p>
<b>Options</b>	<p><b>interface-name</b>—Name of the interface from which the local address is derived. Use the <b>\$junos-loopback-interface</b> dynamic variable to dynamically apply a loopback interface. The loopback interface used is based on the routing instance of the subscriber. The specified interface must have a logical unit number and a configured IP address, and must not be an unnumbered interface.</p> <p><b>preferred-source-address address</b>—Secondary IP address of the donor loopback interface. Use the <b>\$junos-preferred-source-address</b> dynamic variable to dynamically apply a preferred source address to the unnumbered Ethernet interface. When you use the dynamic variable, the address that is selected resides in the same network as the IP address of the subscriber. 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>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring an Unnumbered Interface in <a href="#">Junos OS Network Interfaces Configuration Guide</a>.</li> <li><a href="#">Junos OS Network Interfaces Configuration Guide</a></li> </ul>

## unnumbered-address (Dynamic PPPoE)

---


<b>Syntax</b>	<code>unnumbered-address interface-name destination address;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family inet]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	For dynamic PPPoE interfaces, enable the local address to be derived from the specified interface. Configuring unnumbered Ethernet interfaces enables IP processing on the interface without assigning an explicit IP address to the interface.
<b>Options</b>	<b>interface-name</b> —Interface from which the local address is derived. The interface name must include a logical unit number and must have a configured address.  The <b>destination</b> statement is explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring a Basic PPPoE Dynamic Profile on page 536</li><li>For information about creating static PPPoE interfaces, see the <a href="#">Junos OS Network Interfaces Configuration Guide</a></li></ul>

## update-interval

---

<b>Syntax</b>	<code>update-interval minutes;</code>
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> accounting]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
<b>Description</b>	Configure the amount of time that the router or switch waits before sending a new accounting update.
<b>Default</b>	No updates
<b>Options</b>	<b>minutes</b> —Amount of time between updates, in minutes. <b>Range:</b> 10 through 1440 minutes
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li></ul>

## use-interface-description

<b>Syntax</b>	use-interface-description (logical   device);
<b>Hierarchy Level</b>	<p>[edit forwarding-options dhcp-relay relay-option-82 circuit-id],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-82 circuit-id],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay relay-option-82 circuit-id],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-82 circuit-id],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-82 circuit-id],</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-82 circuit-id],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-82 circuit-id],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-82 circuit-id]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	<p>Use the textual interface description instead of the interface identifier when creating the agent-circuit-id suboption of the DHCP relay agent option 82.</p> <p>If you specify that the textual description is used and no description is configured for the interface, DHCP relay defaults to using the interface identifier. The textual description is configured using the <b>description</b> statement at the <b>[edit interfaces <i>interface-name</i>]</b> hierarchy level.</p> <div style="display: flex; align-items: flex-start; margin-top: 10px;"> <div style="flex: 1;">  </div> <div style="flex: 3; padding-left: 10px;"> <p><b>NOTE:</b> By default, DHCP relay accepts a maximum of 253 ASCII characters. If the textual interface description is longer than 253 characters, DHCP relay drops the packet, which results in the DHCP client failing to bind.</p> </div> </div>
<b>Options</b>	<p><b>logical</b>—Use the textual description that is configured for the logical interface.</p> <p><b>device</b>—Use the textual description that is configured for the device interface.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Enabling and Disabling Insertion of Option 82 Information on page 192</li> <li>Using a Textual Description in Option 82 on page 195</li> </ul>

## use-primary (DHCP Local Server)

---

<b>Syntax</b>	<code>use-primary <i>primary-profile-name</i>;</code>
<b>Hierarchy Level</b>	<code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>dynamic-profile</b> <i>profile-name</i>],</code> <code>[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> <b>dynamic-profile</b> <i>profile-name</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server <b>dynamic-profile</b> <i>profile-name</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> <b>dynamic-profile</b> <i>profile-name</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server <b>dynamic-profile</b> <i>profile-name</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> <b>dynamic-profile</b> <i>profile-name</i>],</code> <code>[edit system services dhcp-local-server <b>dynamic-profile</b> <i>profile-name</i>]</code> <code>[edit system services dhcp-local-server group <i>group-name</i> <b>dynamic-profile</b> <i>profile-name</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify 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.
<b>Options</b>	<b><i>primary-profile-name</i></b> —Name of the dynamic profile to configure as the primary dynamic profile
<b>Required Privilege Level</b>	<code>system</code> —To view this statement in the configuration. <code>system-control</code> —To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125</li></ul>

## use-primary (DHCP Relay Agent)

<b>Syntax</b>	<code>use-primary <i>primary-profile-name</i>;</code>
<b>Hierarchy Level</b>	<p>[edit forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</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> dynamic-profile <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Specify 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.
<b>Options</b>	<b><i>primary-profile-name</i></b> —Name of the dynamic profile to configure as the primary dynamic profile
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Attaching Dynamic Profiles to DHCP Subscriber Interfaces on page 125</li> </ul>

## user-prefix (DHCP Local Server)

<b>Syntax</b>	<code>user-prefix <i>user-prefix-string</i>;</code>
<b>Hierarchy Level</b>	<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 dhcpv6 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 dhcpv6 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 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 dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> 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 dhcpv6 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 dhcpv6 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 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 dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> 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 dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication username-include]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Specify the user prefix that is concatenated with the username during the subscriber authentication process.
<b>Options</b>	<i>user-prefix-string</i> —User prefix string.
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- Using External AAA Authentication Services with DHCP on page 110

## user-prefix (DHCP Relay Agent)

<b>Syntax</b>	<code>user-prefix <i>user-prefix-string</i>;</code>
<b>Hierarchy Level</b>	<p>[edit forwarding-options dhcp-relay authentication <b>username-include</b>],          [edit forwarding-options dhcp-relay group <i>group-name</i> authentication <b>username-include</b>],          [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication <b>username-include</b>],          [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication <b>username-include</b>],          [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication <b>username-include</b>],          [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 <b>username-include</b>],          [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication <b>username-include</b>],          [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication <b>username-include</b>]</p>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	Specify the user prefix that is concatenated with the username during the subscriber authentication process.
<b>Options</b>	<i>user-prefix-string</i> —User prefix string.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.          interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• Using External AAA Authentication Services with DHCP on page 110</li> </ul>

## user-prefix (Static Subscribers)

---

<b>Syntax</b>	<code>user-prefix <i>user-prefix-string</i>;</code>
<b>Hierarchy Level</b>	<code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers authentication <b>username-include</b>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication <b>username-include</b>],</code> <code>[edit logical-systems <i>logical-system-name</i> system services static-subscribers authentication <b>username-include</b>],</code> <code>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i> authentication <b>username-include</b>],</code> <code>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers authentication <b>username-include</b>],</code> <code>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication <b>username-include</b>],</code> <code>[edit system services static-subscribers authentication <b>username-include</b>],</code> <code>[edit system services static-subscribers group <i>group-name</i> authentication <b>username-include</b>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	Specify that a string is included as the beginning of the username created for all static subscribers or for the static subscribers in a specified group. The group version of the statement takes precedence over the global version. The username is also sent to RADIUS in the Access-Request message.
<b>Options</b>	<b><i>user-prefix-string</i></b> —String that begins the username. The string can include the following characters: a through z, A through Z, 0 through 9, "-", or ".".
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Subscribers over Static Interfaces on page 288</li><li>• Configuring the Static Subscriber Global Username on page 291</li><li>• Configuring the Static Subscriber Group Username on page 295</li></ul>



## username-include (DHCP Local Server)

**Syntax**    username-include {  
               circuit-type;  
               client-id;  
               delimiter *delimiter-character*;  
               domain-name *domain-name-string*;  
               logical-system-name;  
               mac-address;  
               option-60;  
               option-82 <circuit-id> <remote-id>;  
               relay-agent-interface-id;  
               relay-agent-remote-id;  
               relay-agent-subscriber-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 dhcpv6 authentication],  
                           [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* 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 dhcpv6 authentication],  
                           [edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* 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 dhcpv6 authentication],  
                           [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* 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 dhcpv6 authentication],  
                           [edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* 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 dhcpv6 authentication],  
                           [edit system services dhcp-local-server dhcpv6 group *group-name* authentication],  
                           [edit system services dhcp-local-server group *group-name* authentication]

**Release Information** Statement introduced in Junos OS 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. The **option-60** and **option-82** statements are not supported in the DHCPv6 hierarchy levels. The **client-id**, **relay-agent-interface-id**, **relay-agent-remote-id** and **relay-agent-subscriber-id** statements are supported in the DHCPv6 hierarchy levels only.

**Required Privilege Level** system—To view this statement in the configuration.  
system-control—To add this statement to the configuration.

**Related Documentation**

- Using External AAA Authentication Services with DHCP on page 110
- Creating Unique Usernames for DHCP Clients on page 128

## username-include (DHCP Relay Agent)

<b>Syntax</b>	<pre>username-include {     circuit-type;     delimiter <i>delimiter-character</i>;     domain-name <i>domain-name-string</i>;     logical-system-name;     mac-address;     option-60;     option-82 &lt;circuit-id&gt; &lt;remote-id&gt;;     routing-instance-name;     user-prefix <i>user-prefix-string</i>; }</pre>
<b>Hierarchy Level</b>	<pre>[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]</pre>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1.
<b>Description</b>	<p>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.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Using External AAA Authentication Services with DHCP on page 110</li> </ul>

## username-include (Static Subscribers)

---

<b>Syntax</b>	<pre>username-include {     domain-name <i>domain-name</i>;     interface;     logical-system-name;     routing-instance-name;     user-prefix <i>user-prefix-string</i>; }</pre>
<b>Hierarchy Level</b>	<pre>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system   services static-subscribers authentication], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system   services static-subscribers group <i>group-name</i> authentication], [edit logical-systems <i>logical-system-name</i> system services static-subscribers authentication], [edit logical-systems <i>logical-system-name</i> system services static-subscribers group   <i>group-name</i> authentication], [edit routing-instances <i>routing-instances-name</i> system services static-subscribers   authentication], [edit routing-instances <i>routing-instances-name</i> system services static-subscribers group   <i>group-name</i> authentication], [edit system services static-subscribers authentication], [edit system services static-subscribers group <i>group-name</i> authentication]</pre>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.6.
<b>Description</b>	<p>Specify the information included in the username created for all static subscribers or for static subscribers in a specified group. The group version of the statement takes precedence over the global version. The username is also sent to RADIUS in the Access-Request message.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Subscribers over Static Interfaces on page 288</li><li>Configuring the Static Subscriber Global Username on page 291</li><li>Configuring the Static Subscriber Group Username on page 295</li></ul>

## valid-lifetime (Dynamic Router Advertisement)

---

<b>Syntax</b>	<code>valid-lifetime <i>seconds</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols router-advertisement interface <i>interface-name</i> prefix <i>prefix</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Specify how long the prefix remains valid for onlink determination.
<b>Options</b>	<b><i>seconds</i></b> —Valid lifetime, in seconds. If you set the valid lifetime to <b>0xffffffff</b> , the lifetime is infinite. <b>Default:</b> 2,592,000 seconds
<b>Required Privilege Level</b>	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• preferred-lifetime</li><li>• Configuring the Prefix Information Included in Neighbor Discovery Advertisements</li></ul>

## variables

---

**Syntax**

```
variables {  
  variable-name {  
    mandatory;  
    default-value default-value;  
    radius {  
      vendor-id id {  
        attribute attribute-number;  
        tag tag-number;  
      }  
    }  
  }  
}
```

**Hierarchy Level** [edit dynamic-profiles *profile-name*]

**Release Information** Statement introduced in Junos OS 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** *variable-name*—Name of the variable.

The remaining statements are explained separately.

**Required Privilege** interface—To view this statement in the configuration.

**Level** interface-control—To add this statement to the configuration.

**Related Documentation**

- [Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 698](#)

## vendor-id

---

<b>Syntax</b>	<code>vendor-id <i>id</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> variables radius]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.3.
<b>Description</b>	Configure the vendor ID as a variable in a dynamic profile.
<b>Options</b>	<i>id</i> —Vendor ID for the RADIUS attribute.  The remaining statements are explained separately.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring User-Defined CoS Variables in a Dynamic Service Profile on page 698</li></ul>

## vendor-option

---

<b>Syntax</b>	<pre>vendor-option {     (equals   starts-with) (ascii <i>match-string</i>   hexadecimal <i>match-hex</i>) {         (relay-server-group <i>server-group-name</i>           local-server-group <i>local-server-group-name</i>           drop);     }     (default-relay-server-group <i>server-group-name</i>       default-local-server-group <i>local-server-group-name</i>       drop); }</pre>
<b>Hierarchy Level</b>	<pre>[edit forwarding-options dhcp-relay relay-option-60], [edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-60], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay relay-option-60], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i>     relay-option-60], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>     forwarding-options dhcp-relay relay-option-60], [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], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay     relay-option-60], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group     <i>group-name</i> relay-option-60]</pre>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	<p>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.</p> <p>The <b>vendor-option</b> statement enables you to specify either an exact, left-to-right match (with the <b>equals</b> statement) or a partial match (with the <b>starts-with</b> statement), and configure either an ASCII match string (with the <b>ascii</b> statement) or a hexadecimal match string (with the <b>hexadecimal</b> statement).</p> <p>You can configure an unlimited number of match strings. Match strings do not support the use of wildcard attributes.</p>
<b>Options</b>	<p><b>equals</b>—Use exact, left-to-right match of the ASCII or hexadecimal match string with the option 60 string.</p> <p><b>starts-with</b>—Use 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 <b>starts-with</b> statement, the longest match rule applies; that is, the router matches the string "test123" before it matches the string "test".</p>



**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.

<b>Required Privilege Level</b>	interface—To view this statement in the configuration.
	interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Using Option 60 Information to Forward Client Traffic to Specific DHCP Servers on page 189</li> </ul>

## version (Dynamic IGMP Interface)

<b>Syntax</b>	<code>version <i>version</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols igmpinterface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	Specify the version of IGMP.
<b>Options</b>	<b>version</b> —IGMP version number.
	<b>Range:</b> 1, 2, or 3
	<b>Default:</b> 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.

<b>Required Privilege Level</b>	routing—To view this statement in the configuration.
	routing-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring a Dynamic Profile for Client Access on page 395</li> </ul>
	<ul style="list-style-type: none"> <li>For information about specifying a different IGMP version, see “Changing the IGMP Version” in the <i>Junos OS Multicast Protocols Configuration Guide</i></li> </ul>

## version (Dynamic MLD Interface)

---

<b>Syntax</b>	<code>version <i>version</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> protocols mld interface <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Configure the MLD version explicitly on the dynamic interface. MLD version 2 (MLDv2) is used only to support source-specific multicast (SSM).
<b>Options</b>	<b>version</b> —MLD version to run on the interface. <b>Range:</b> 1 or 2 <b>Default:</b> 1 (MLDv1)
<b>Required Privilege Level</b>	routing and trace—To view this statement in the configuration. routing-control and trace-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Modifying the MLD Version</li></ul>

## virtual-network

<b>Syntax</b>	<pre>virtual-network {   home-agent-address <i>ip-address</i> {     registration-lifetime <i>seconds</i>;     revocation-required;     timestamp-tolerance <i>seconds</i>;   } }</pre>
<b>Hierarchy Level</b>	<p>[edit logical-systems <i>logical-system-name</i> services mobile-ip home-agent],          [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> services mobile-ip home-agent],          [edit routing-instances <i>routing-instances-name</i> services mobile-ip home-agent],          [edit services mobile-ip home-agent]</p>
<b>Release Information</b>	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> ...], and [edit routing-instances <i>routing-instances-name</i> ...] hierarchy levels introduced in Junos OS Release 9.5.</p>
<b>Description</b>	<p>Define the virtual network for the Mobile IP home agent. Only one virtual network is supported.</p> <p>The remaining statements are explained separately.</p>
<b>Required Privilege Level</b>	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Mobile IP on page 357</li> <li>Configuring the Mobile IP Home Agent on page 358</li> </ul>

## vlan-id (Dynamic Profiles)

---

<b>Syntax</b>	vlan-id ( <i>number</i>   none);
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ],
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. VLAN demux interface support introduced in Junos OS Release 10.2.
<b>Description</b>	For VLAN demux, Fast Ethernet, Gigabit Ethernet, and Aggregated Ethernet interfaces only, bind a 802.1Q VLAN tag ID to a logical interface.
<b>Options</b>	<p><b>number</b>—A valid VLAN identifier. When used in the <b>dynamic-profiles</b> hierarchy, specify the <code>\$junos-vlan-id</code> predefined variable to dynamically obtain the VLAN identifier.</p> <p><b>none</b>—Enable the use of untagged pseudo-wire frames on dynamic interfaces.</p> <p><b>Range:</b></p> <ul style="list-style-type: none"><li>• For aggregated Ethernet, 4-port, 8-port, and 12-port Fast Ethernet PICs, and for management and internal Ethernet interfaces, 1 through 1023.</li><li>• For 48-port Fast Ethernet and Gigabit Ethernet PICs, 1 through 4094.</li><li>• VLAN ID 0 is reserved for tagging the priority of frames.</li></ul>
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• Configuring Static Subscriber Interfaces Using VLAN Demux Interfaces on page 441</li><li>• Configuring Dynamic Subscriber Interfaces Using VLAN Demux Interfaces in Dynamic Profiles on page 446</li></ul>

## vlan-id (Dynamic VLANs)

<b>Syntax</b>	<code>vlan-id <i>number</i>;</code>
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	For dynamic VLAN interfaces, specify the line VLAN identifiers to be rewritten at the input or output interface.  You cannot include the <b>vlan-id</b> statement with the <b>swap</b> statement, <b>swap-push</b> statement, <b>push-push</b> statement, or <b>push-swap</b> statement at the [edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map] hierarchy level. If you include any of those statements in the output VLAN map, the VLAN ID in the outgoing frame is rewritten to the <b>vlan-id</b> statement that you include at the [edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> ] hierarchy level.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Rewriting the VLAN Tag on Tagged Frames</li> <li>Binding VLAN IDs to Logical Interfaces</li> </ul>

## vlan-nas-port-stacked-format

<b>Syntax</b>	<code>vlan-nas-port-stacked-format;</code>
<b>Hierarchy Level</b>	[edit access profile <i>profile-name</i> radius options]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
<b>Description</b>	Configure RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring RADIUS Server Options for Subscriber Access on page 29</li> <li>Configuring Authentication and Accounting Parameters for Subscriber Access on page 21</li> </ul>

## vlan-tag (Dynamic Classifiers)

---

<b>Syntax</b>	vlan-tag (inner   outer);
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> classifiers ieee-802.1]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Apply this IEEE-802.1 classifier to the inner or outer VLAN tags in a dynamic profile.
<b>Default</b>	If you do not include this statement, the classifier applies to the outer VLAN tag only.
<b>Options</b>	<b>inner</b> —Apply the classifier to the inner VLAN tag only. <b>outer</b> —Apply the classifier to the outer VLAN tag only.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li><li>Applying a Classifier to a Subscriber Interface in a Dynamic Profile on page 687</li><li>classifiers (Definition)</li></ul>

## vlan-tag (Dynamic Rewrite Rules)

<b>Syntax</b>	vlan-tag (outer   outer-and-inner);
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> class-of-service interfaces <i>interface-name</i> unit <i>logical-unit-number</i> rewrite-rules ieee-802.1]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.1.
<b>Description</b>	Apply this IEEE-802.1 rewrite rule to the outer or outer and inner VLAN tags in a dynamic profile.
<b>Default</b>	If you do not include this statement, the rewrite rule applies to the outer VLAN tag only.
<b>Options</b>	<p><b>outer</b>—Apply the rewrite rule to the outer VLAN tag only.</p> <p><b>outer-and-inner</b>—Apply the rewrite rule to both the outer and inner VLAN tags.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Guidelines for Configuring Dynamic CoS for Subscriber Access on page 660</li> <li>Applying a Rewrite Rule Definition to a Subscriber Interface in a Dynamic Profile on page 686</li> <li>rewrite-rules</li> </ul>

## vlan-tagging

---

<b>Syntax</b>	vlan-tagging;
<b>Hierarchy Level</b>	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> ], [edit interfaces <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.2.
<b>Description</b>	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 OS 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.

.....

<b>Required Privilege</b>	interface—To view this statement in the configuration.
<b>Level</b>	interface-control—To add this statement to the configuration.



## vlan-tags

<b>Syntax</b>	<code>vlan-tags outer [<i>tpid</i>].<i>vlan-id</i> [inner [<i>tpid</i>].<i>vlan-id</i>];</code>
<b>Hierarchy Level</b>	<code>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</code>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5. VLAN demux interface support introduced in Junos OS Release 10.2.
<b>Description</b>	For Gigabit Ethernet IQ and IQE interfaces only, binds TPIDs and 802.1Q VLAN tag IDs to a logical interface. You must include the <b>stacked-vlan-tagging</b> statement at the <code>[edit interfaces <i>interface-name</i>]</code> hierarchy level.



**NOTE:** The inner-range *vid1–vid2* option is supported on MX Series routers with IQE PICs only.

<b>Options</b>	<p><b>inner [<i>tpid</i>].<i>vlan-id</i></b>—A TPID (optional) and a valid VLAN identifier in the format <i>tpid.vlan-id</i>. When used in the <b>dynamic-profiles</b> hierarchy, specify the <b>\$junos-vlan-id</b> predefined variable to dynamically obtain the VLAN ID.</p> <p><b>Range:</b> For VLAN ID, 1 through 4094. VLAN ID 0 is reserved for tagging the priority of frames.</p> <p><b>outer [<i>tpid</i>].<i>vlan-id</i></b>—A TPID (optional) and a valid VLAN identifier in the format <i>tpid.vlan-id</i>. When used in the <b>dynamic-profiles</b> hierarchy, specify the <b>\$junos-stacked-vlan-id</b> predefined variable.</p> <p><b>Range:</b> For VLAN ID, 1 through 511 for normal interfaces, and 512 through 4094 for VLAN CCC interfaces. VLAN ID 0 is reserved for tagging the priority of frames.</p>
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>Configuring Dual VLAN Tags</li> <li>stacked-vlan-tagging</li> </ul>


## weighted-load-balancing (L2TP LAC)

---

<b>Syntax</b>	weighted-load-balancing;
<b>Hierarchy Level</b>	[edit services l2tp]
<b>Release Information</b>	Statement introduced in Junos OS Release 10.4.
<b>Description</b>	Specify that the router chooses among multiple tunnels that share the same preference level by considering the maximum sessions configured per tunnel. The tunnel configured with the highest maximum number of sessions in the preference level has the highest weight. This tunnel is selected until the maximum number of sessions for the tunnel is reached. Then the router selects the tunnel with the next higher weight to establish connections until that tunnel's maximum session limit is reached, and so on.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Weighted Load Balancing for LAC Tunnel Sessions on page 245</li><li>Configuring the L2TP LAC Tunnel Selection Parameters on page 244</li></ul>

## wimax

---

<b>Syntax</b>	wimax;
<b>Hierarchy Level</b>	[edit services <b>mobile-ip</b> access-type], [edit logical-systems <i>logical-system-name</i> services <b>mobile-ip</b> access-type], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> services <b>mobile-ip</b> access-type], [edit routing-instances <i>routing-instance-name</i> services <b>mobile-ip</b> access-type]
	<div> <b>NOTE:</b> Although this statement is available in the CLI for both default and nondefault router contexts, the commit operation is disallowed when you configure the statement in a nondefault router context.</div>
<b>Release Information</b>	Statement introduced in Junos OS Release 9.5.
<b>Description</b>	Enable WiMAX features for Mobile IP home agent, including the ability to process, send, and receive WiMAX Vendor Specific Attributes (VSAs).
<b>Required Privilege Level</b>	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Mobile IP on page 357</li><li>Configuring the Access Type for Mobile IP on page 361</li></ul>

## wins-server

---

<b>Syntax</b>	<pre>wins-server {     <i>ipv4-address</i>; }</pre>
<b>Hierarchy Level</b>	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
<b>Release Information</b>	Statement introduced in Junos OS Release 9.0.
<b>Description</b>	Specify one or more NetBIOS name servers (NBNS) that the client uses to resolve NetBIOS names. This is equivalent to DHCP option 44.
<b>Options</b>	<i>ipv4-address</i> —IP address of each NetBIOS name server; add them to the configuration in order of preference.
<b>Required Privilege Level</b>	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>Configuring Address-Assignment Pools on page 68</li></ul>



## PART 18

# Index

- Index on page 1289
- Index of Statements and Commands on page 1319



# Index

## Symbols

#, comments in configuration statements.....	lvi
\$junos-cos-delay-buffer-rate predefined variable.....	894
\$junos-cos-excess-priority predefined variable.....	952
\$junos-cos-excess-rate predefined variable.....	953
\$junos-cos-guaranteed-rate predefined variable.....	986
\$junos-cos-overhead-accounting predefined variable.....	1094
\$junos-cos-scheduler predefined variable.....	689, 1177
\$junos-cos-scheduler-bs predefined variable.....	689, 875
\$junos-cos-scheduler-dropfile-any predefined variable.....	689, 929
\$junos-cos-scheduler-dropfile-high predefined variable.....	689, 929
\$junos-cos-scheduler-dropfile-low predefined variable.....	689, 929
\$junos-cos-scheduler-dropfile-medium-high predefined variable.....	689, 929
\$junos-cos-scheduler-dropfile-medium-low predefined variable.....	689, 929
\$junos-cos-scheduler-excess-rate predefined variable.....	952
\$junos-cos-scheduler-map predefined variable.....	1175
\$junos-cos-scheduler-pri predefined variable.....	689, 1126
\$junos-cos-scheduler-shaping-rate predefined variable.....	1186
\$junos-cos-scheduler-tx predefined variable.....	689, 1241
\$junos-cos-shaping-rate predefined variable.....	1186
( ), in syntax descriptions.....	lvi
3GPP Gx	
Gx-Plus and.....	329

802.1Q VLANs	
VLAN tagging.....	1282
< >, in syntax descriptions.....	lv
[ ], in configuration statements.....	lvi
{ }, in configuration statements.....	lvi
(pipe), in syntax descriptions.....	lvi

## A

AAA	
configuration testing.....	56
Mobile IP home agent and .....with Diameter base protocol.....	348
with Diameter base protocol.....	255
AAA directed logout	
DHCP authentication services.....	110, 164
AAA logical system/routing instance	
domain map.....	84
AAA Service Framework.....	18
dynamic service activation	
during login.....	35
aaa-logical-system statement	
domain maps.....	835
aaa-routing-instance statement	
domain maps.....	836
abatedUtilization statement	
address-assignment pools.....	836
abatedUtilization-v6 statement	
address-assignment pools.....	837
access identifier	
configuring ANCP .....	787
access profile	
configuring global static subscriber.....	289
configuring static subscriber group.....	293
domain map.....	82
session options.....	54
access profile statements	
session-options.....	1185
access profiles	
attaching.....	53
configuring.....	53
access statement	
dynamic profiles.....	837

access type		configuring.....68
configuring Mobile IP.....361		
access-concentrator statement.....838		
access-identifier statement		
ANCP.....839		
access-internal statement		
dynamic profiles.....839		
access-profile statement		
domain maps.....840		
static subscribers.....841		
access-type statement		
Mobile IP.....842		
accounting		
configuring RADIUS.....21		
Mobile IP time-based.....351		
accounting method		
configuring Mobile IP.....360		
accounting methods.....21		
accounting statement		
access profile.....843		
dynamic IGMP		
interface.....843		
dynamic MLD interface.....844		
accounting statistics.....23		
per-service accounting.....23		
subscriber service session.....25, 576		
subscriber session.....24		
accounting-port statement.....844		
accounting-server statement.....845		
accounting-session-id-format statement.....845		
accounting-stop-on-access-deny statement.....846		
accounting-stop-on-failure statement.....846		
Acct-Off messages.....22		
Acct-On messages.....22		
active server groups		
DHCP relay.....196		
active-server-group statement.....847		
address pool		
domain map.....83		
address statement.....849		
Diameter base protocol.....848		
interface.....848		
tunnels		
LAC.....850		
LNS.....849		
address-assignment pools		
abatedUtilization.....836		
abatedUtilization-v6.....837		
client attributes.....72		
DHCP attributes.....73		
mapping option 82.....73		
setting the grace period.....73		
setting the maximum lease time.....73		
setting the name server address.....73		
specifying NetBIOS node type.....73		
specifying router addresses.....73		
specifying the boot file .....73		
specifying the boot server .....73		
specifying the DNS server IPv6		
address.....73		
specifying the domain name to search.....73		
specifying the SIP server domain		
name.....73		
specifying the SIP server IPv6 address.....73		
specifying the source address.....73		
specifying the TFTP server.....73		
specifying the WINS server.....73		
specifying user-defined options.....73		
DHCP local server.....100		
DHCPv6 attributes.....73		
highUtilization.....988		
highUtilization-v6.....988		
license requirements.....74		
linking.....70		
name.....69		
named range.....69		
network address.....69		
router advertisement.....1069		
static address.....71		
threshold traps.....71		
tracing operations.....74		
address-assignment statement		
address-assignment pools.....851		
address-pool statement		
domain maps.....852		
adf statement		
dynamic firewalls.....853		
adjacency timer		
ANCP global configuration.....788		
ANCP neighbor configuration.....786, 788		
adjacency-timer statement		
ANCP.....854		
Agent Circuit ID suboption		
DHCP relay.....193		



- 
- aggregate-clients statement
    - DHCP local server.....855
    - DHCP relay agent.....856
    - static subscribers.....857
  - aggregated Ethernet
    - targeted distribution of subscribers.....1039, 1143, 1203
  - aggregated Ethernet interfaces without link protection
    - manually rebalancing subscribers .....485
    - periodically rebalancing subscribers .....485
    - rebalancing subscribers.....485
    - targeting subscribers.....485
  - aggregated Ethernet logical interfaces See subscriber interfaces, IP demux over aggregated Ethernet See subscriber interfaces, VLAN demux over aggregated Ethernet See subscriber interfaces, VLAN over aggregated Ethernet
  - algorithm statement
    - Mobile IP.....858
  - allow-snooped-clients statement
    - DHCP relay agent.....859
  - always-write-giaddr statement
    - DHCP relay agent.....860
  - always-write-option-82 statement
    - DHCP relay agent.....861
  - ANCP
    - access identifier configuration.....787
    - adjacency timer global configuration.....788
    - adjacency timer neighbor configuration.....788
    - adjusting subscriber traffic with.....781
    - associating subscriber VLANs with access nodes.....787
    - backwards compatibility global configuration.....789
    - backwards compatibility neighbor configuration.....786, 789
    - configuration overview.....786
    - CoS information verifying.....791
    - CoS shaping rate adjustment for subscriber local loops.....781
    - CoS traffic shaping configuration.....790
    - discovery table global configuration.....788
    - discovery table neighbor configuration.....786, 788
    - event logging.....792
    - flags for tracing operations.....794
    - log file access for tracing operations.....793
    - log file size and number.....793
    - log filenames for tracing operations.....792
    - monitoring subscriber traffic with.....781
    - neighbor configuration
      - adjacency timer.....786
      - discovery table entries.....786
      - ietf mode.....786
      - IP address.....786
      - pre-ietf mode.....786
    - neighbor information verifying.....790
    - overview.....781
    - pre-ietf mode global configuration.....789
    - pre-ietf mode neighbor configuration.....786, 789
    - regular expressions for tracing operations.....794
    - restart time global configuration.....789
    - shaping-rate adjustments for subscriber local loops.....753
    - subscriber information verifying.....791
    - tracing operations.....792
  - ancc statement
    - ANCP.....862
  - ANCP statements
    - access-identifier.....839
    - adjacency-timer.....854
    - ancc.....862
    - ietf-mode.....995
    - interface-set.....1030
    - interfaces.....1025
    - maximum-discovery-table-entries.....1053
    - maximum-helper-restart-time.....1054
    - neighbor
      - for all neighbors.....1068
      - for unique access identifier.....1068
    - pre-ietf-mode.....1125
    - qos-adjust.....1135
    - traceoptions.....1215
  - application statement.....863
  - Ascend-Data-Filter
    - example of dynamic configuration.....600
    - example of static configuration.....603
    - field descriptions.....561
    - multiple filters.....560
    - naming convention.....560
    - verifying configuration.....578
  - Ascend-Data-Filters.....559

Ascent-Data-Filter.....	577
attempts statement	
DHCP local server.....	864
attribute statement	
dynamic profile variables.....	865
attributes statement.....	866
authenticate statement	
Mobile IP.....	867
authentication	
configuring RADIUS.....	21
dynamic VLAN.....	424
Mobile IP home agent.....	348
authentication attributes	
local Mobile IP.....	359
authentication method	
configuring Mobile IP.....	358
authentication methods.....	21
authentication password <i>See</i> password	
configuring global static subscriber.....	290
configuring group static subscriber.....	294
authentication services	
with DHCP.....	110, 164
authentication statement	
DHCP local server.....	868
DHCP relay agent.....	869
static subscribers.....	870
authentication-order statement	
access.....	871
authentication-server statement.....	872
authorization, subscriber	
JSRC.....	281
authorization-order statement	
JSRC.....	872
auto logout	
DHCP.....	120, 180
DHCP relay agent option 82.....	182
autonomous statement	
dynamic router advertisement.....	873
AVPs	
Diameter.....	273
Gx-Plus.....	332

## B

backwards compatibility	
ANCP global configuration.....	789
ANCP neighbor configuration.....	786, 789
boot-file statement.....	873
boot-server statement.....	874

BOOTREPLY packets	
DHCP snooping.....	174
braces, in configuration statements.....	lvi
brackets	
angle, in syntax descriptions.....	lv
square, in configuration statements.....	lvi
buffer-size statement	
dynamic CoS.....	875

## C

Calling Number AVP 22	
preventing L2TP LAC from sending.....	246
captive portal content delivery	
dynamic subscriber interfaces.....	615
captive-portal-content-delivery statement.....	876
captive-portal-content-delivery statements	
traceoptions.....	1217
captive-portal-content-delivery-rule-set	
statement.....	877
change of authorization <i>See</i> CoA	
chap statement	
dynamic PPP.....	878
circuit-id statement	
address-assignment pools.....	878
DHCP relay agent.....	879
circuit-type statement	
DHCP local server.....	880
DHCP relay agent.....	881
class of service <i>See</i> CoS	
class-of-service statement	
subscriber access.....	882
classic filters	
components.....	557
processing order.....	557
types.....	556
classic firewall filters	
configuration guidelines.....	558
classifiers statement	
dynamic CoS.....	882
clear-on-abort statement	
DHCP local server.....	883
client attributes	
address-assignment pools.....	72
client configuration information	
DHCP.....	99
client usernames	
DHCP	
unique.....	128

- client-accounting-algorithm statement
    - RADIUS.....884
  - client-authentication-algorithm statement
    - RADIUS.....884
  - client-discover-match statement
    - DHCP local server.....885
    - DHCP relay agent.....886
  - client-id statement.....887
  - client-idle-timeout statement
    - access profile session options.....888
  - client-session-timeout statement
    - access profile session options.....889
  - CoA
    - messages.....36
    - RADIUS.....35
  - coa-immediate-update statement
    - accounting.....889
  - comments, in configuration statements.....lvi
  - connect-actively statement
    - Diameter base protocol.....890
  - conventions
    - text and syntax.....lv
  - CoS
    - IP demux
      - configuring.....709
      - overview.....703
    - RADIUS-provided parameters
      - configuring an access dynamic
        - profile.....697
        - example.....721
        - overview.....689
    - shaping-rate adjustments for subscriber local
      - loops
        - configuration guidelines.....754
        - disabling.....767
        - enabling.....762
        - example.....774
        - overview.....753
    - subscriber access
      - changing services.....693
      - classifiers.....687
      - configuration guidelines.....660
      - configuration overview.....669
      - configuring variables.....698
      - dynamic configuration overview.....671
      - interfaces.....685
      - overview.....659
      - rewrite rules.....686
    - static scheduling and queuing
      - example.....713
      - traffic parameters.....677, 678
  - CoS traffic shaping
    - with ANCP.....790
  - curly braces, in configuration statements.....lvi
  - current-hop-limit statement
    - dynamic router advertisement.....890
  - customer support.....lvi
  - contacting JTAC.....lvi
- D**
  - database-replication statement
    - subscriber session database replication.....891
  - default-lifetime statement
    - dynamic router advertisement.....891
  - default-local-server-group statement.....892
  - default-relay-server-group statement.....893
  - default-value statement
    - dynamic profile variables.....894
  - delay-buffer-rate statement
    - dynamic CoS.....894
  - delimiter statement
    - DHCP local server.....895
    - DHCP relay agent.....896
    - domain maps.....897
  - delimiters
    - domain names.....87
  - demux interfaces
    - unit statement.....1251
  - demux-options statement
    - dynamic IP demux interface.....899
  - demux-source statement
    - dynamic IP demux interfaces.....900
    - dynamic underlying interface.....901
  - demux0 statement
    - dynamic IP demux interface.....898
  - demux0 statements
    - underlying-interface.....1249
  - destination statement
    - Diameter base protocol.....901
    - dynamic PPPoE.....902
  - destination-address statement
    - cpd.....902
  - destination-host statement
    - Gx-Plus.....903
    - JSRC.....903
    - PTSP.....904

destination-prefix-list statement		
captive-portal-content-delivery.....	904	
destination-realm statement		
Gx-Plus.....	905	
JSRC.....	905	
PTSP.....	906	
DHCP		
ARP table population		
overriding.....	117, 172	
authentication services.....	110, 164	
AAA directed logout.....	110, 164	
auto logout.....	120, 180	
client configuration information.....	99	
distinguishing duplicate clients.....	109, 163	
duplicate client IDs.....	108, 162	
duplicate clients		
configuration guidelines.....	109, 163	
duplicate MAC addresses.....	108, 162	
grouping interfaces.....	112, 165	
configuration guidelines.....	113, 166	
maximum clients per interface		
overriding.....	116, 173	
override settings		
deleting.....	122	
unified ISSU.....	6	
unique client usernames.....	128	
user passwords.....	127	
DHCP local server		
address-assignment pool selection.....	111	
address-assignment pools.....	100	
ARP table population		
overriding.....	117, 172	
client auto logout.....	121, 183	
DHCP snooping.....	119, 174	
DHCPv6.....	102	
dynamic client reconfiguration		
authentication token configuration.....	136	
behavior on failure configuration.....	135	
configuration overview.....	133	
number of attempts configuration.....	134	
RADIUS-initiated disconnect		
configuration.....	136	
requesting.....	137	
dynamic profile attachment		
multiple subscribers.....	125, 197	
overview.....	104, 158	
use primary profile.....	125, 197	
graceful Routing Engine switchover.....	139	
grouping interfaces		
options.....	115	
interaction		
address-assignment pools.....	99	
DHCP clients.....	99	
maximum clients per interface		
overriding.....	116, 173	
minimal configuration		
default settings.....	100	
option 50.....	123	
override settings		
deleting.....	122	
overriding default configuration.....	115	
overview.....	98	
per-interface tracing operations.....	144, 203	
specific address.....	123	
tracing operations.....	139, 199	
verifying configuration.....	138	
DHCP local server statements		
attempts.....	864	
boot-file.....	873	
boot-server.....	874	
circuit-type.....	880	
clear-on-abort.....	883	
client-discover-match.....	885	
client-id.....	887	
default-local-server-group.....	892	
delimiter.....	895	
dhcp-local-server.....	908	
dhcpv6.....	914	
dns-server.....	921	
domain-name.....	924	
duplicate-clients-on-interface.....	934	
dynamic-profile.....	937	
forward-snooped-clients.....	967	
group.....	975	
interface.....	1005	
interface-traceoptions.....	1021	
ip-address-first.....	1032	
logical-system-name.....	1041	
mac-address.....	1045	
no-arp.....	1074	
option-60.....	1081	
option-82.....	1084, 1085	
overrides.....	1095	
password.....	1105	
pool-match-order.....	1111	
relay-agent-interface-id.....	1147	
relay-agent-remote-id.....	1148	

- 
- relay-agent-subscriber-id.....1149
  - routing-instance-name.....1167
  - strict.....1198
  - timeout.....1207
  - trace.....1211
  - traceoptions.....1219
  - trigger.....1243
  - username-include.....1267
  - DHCP relay
    - access and access-internal routes.....205, 220
    - active server groups.....196
    - Agent Circuit ID suboption.....193
    - ARP table population
      - overriding.....117, 172
    - automatic binding of stray requests.....187
    - client auto logout.....121, 183
    - configuration examples
      - minimum configuration.....209
      - multiple clients and servers
        - configuration.....209
      - option 60 drop configuration.....214
      - option 60 forward configuration.....213
    - DHCP relay proxy.....156, 196
    - DHCP snooping.....174, 176
    - disabling.....187
    - discarded packets
      - counting.....192
    - dynamic profile attachment
      - multiple subscribers.....125, 197
      - overview.....104, 158
      - use primary profile.....125, 197
    - graceful Routing Engine switchover.....139
    - grouping interfaces
      - options.....167
    - how components interact.....154
    - Layer 2 unicast transmission.....171
    - matching option 60 strings.....189
    - maximum clients per interface
      - overriding.....116, 173
    - nonmatching option 60 strings.....192
    - option 60 information.....189
    - option 82
      - auto logout.....182
    - option 82 information.....192
    - option 82 prefix.....193
    - option 82 textual description.....195
    - override settings
      - deleting.....122
    - overriding broadcast bit.....171
    - overriding default configuration.....168
    - overriding option 82.....170
    - overview.....154
    - overwrite giaddr.....170
    - per-interface tracing operations.....144, 203
    - replacing IP source address.....170
    - sending release messages.....184
    - server groups.....195
    - tracing operations.....139, 199
    - trusting option 82.....172
    - verifying configuration.....198
  - DHCP relay agent
    - DHCP snooping.....178
  - DHCP relay agent statements
    - allow-snooped-clients.....859
    - always-write-giaddr.....860
    - always-write-option-82.....861
    - circuit-id.....879
    - circuit-type.....881
    - client-discover-match.....886
    - default-relay-server-group.....893
    - delimiter.....896
    - disable-relay.....920
    - domain-name.....925
    - drop.....927
    - duplicate-clients-on-interface.....934
    - dynamic-profile.....938
    - forward-snooped-clients.....968
    - group.....977
    - interface.....1007
    - interface-client-limit.....1018
    - interface-traceoptions.....1023
    - layer2-unicast-replies.....1036
    - local-server-group.....1038
    - logical-system-name.....1042
    - mac-address.....1046
    - no-allow-snooped-clients.....1073
    - no-arp.....1075
    - no-bind-on-request.....1076
    - option-60.....1082
    - overrides.....1097
    - password.....1106
    - prefix.....1123
    - proxy-mode.....1134
    - relay-option-60.....1150
    - relay-option-82.....1151
    - relay-server-group.....1152
    - replace-ip-source-with.....1154
    - routing-instance-name.....1168

send-release-on-delete.....	1179
server-group.....	1180
trace.....	1212
traceoptions.....	1221
trust-option-82.....	1244
use-interface-description.....	1261
use-primary.....	1262, 1263
user-prefix.....	1264, 1265
username-include.....	1269
vendor-option.....	1274
DHCP relay proxy.....	1134
enabling.....	196
how components interact.....	156
overview.....	156
DHCP snooping	
BOOTREPLY packets.....	174
DHCP local server.....	119, 174
DHCP relay agent.....	178
disabling.....	176
disabling interfaces.....	174
enabling.....	176
enabling interfaces.....	174
example of DHCP relay agent	
configuration.....	211
DHCP stray requests	
disabling automatic binding.....	187
enabling automatic binding.....	187
DHCP subscriber	
auto logout.....	121, 183
dhcp-attributes statement	
address-assignment pools.....	907
dhcp-local-server statement.....	908
dhcp-relay statement.....	911
DHCPv6 local server	
IA_NA.....	123
overview.....	102
specific address.....	123
verifying configuration.....	138
dhcpv6 statement.....	914
Diameter	
AVPs.....	273
Gx-Plus.....	332
AVPs used by PTSP and the SAE.....	305
message sequences for Gx-Plus.....	335
message sequences for JSRC.....	276
message sequences for PTSP.....	308
messages used by Gx-Plus and the	
PCRF.....	330
messages used by JSRC and the SAE.....	272
messages used by PTSP and the SAE.....	304
Diameter base protocol.....	255
configuration overview.....	259
event log access.....	264
event logging.....	262
filtering trace operation output.....	265
flags for tracing operations.....	265
function information	
verifying.....	267
instance information	
verifying.....	266
log file size.....	264
log filenames.....	263
network element configuration.....	261
network element information	
verifying.....	269
node information	
verifying.....	266
origin attribute configuration.....	260
peer configuration.....	260
peer information	
verifying.....	268
route information	
verifying.....	266
tracing operations.....	262
transport configuration.....	262
troubleshooting configuration.....	269
troubleshooting connectivity.....	270
Diameter base protocol statements	
address.....	848
connect-actively.....	890
destination.....	901
diameter.....	916
forwarding.....	969
function	
network element.....	971
route.....	972
host.....	993
logical-system.....	1039
metric.....	1059
network-element.....	1071
origin.....	1091
peer.....	1109
port.....	1112
priority.....	1125
realm.....	1144
route.....	1162

- routing-instance.....1164
  - traceoptions.....1223
- diameter statement
  - Diameter base protocol.....916
- diameter-instance statement
  - Gx-Plus.....917
  - JSRC.....917
  - PTSP.....918
- directed logout
  - AAA.....110, 164
- disable statement
  - dynamic IGMP.....918
  - dynamic MLD.....919
- disable-calling-number-avp statement.....919
- disable-failover-protocol statement.....920
- disable-relay statement.....920
- discovery table
  - ANCP global configuration.....788
  - ANCP neighbor configuration.....786, 788
- dns-server statement.....921
- documentation
  - comments on.....lvi
- domain map.....80
  - AAA logical system/routing instance.....84
  - access profile.....82
  - address pool.....83
  - configuring.....81
  - domain name.....86
  - dynamic profile.....83, 89
  - target logical system/routing instance.....85
  - tunnel profile.....88
  - verifying configuration.....89
- domain map statements
  - aaa-logical-system.....835
  - aaa-routing-instance.....836
  - access-profile.....840
  - address-pool.....852
  - delimiter.....897
  - domain.....922
  - dynamic-profile.....938
  - map.....1050
  - mask.....1051
  - metric.....1060
  - padn.....1099
  - parse-direction.....1100
  - strip-domain.....1198
  - target-logical-system.....1202
  - target-routing-instance.....1203
  - tunnel-profile.....1246
- domain mapping See domain map
- domain maps See default
- domain names
  - delimiters.....87
  - domain map.....86
  - parsing direction.....87
  - stripping from username.....88
- domain statement
  - domain maps.....922
- domain-name statement
  - address-assignment pools.....923
  - DHCP local server.....924
  - DHCP relay agent.....925
  - static subscribers.....926
- drop statement
  - DHCP relay agent.....927
- drop-profile statement
  - dynamic CoS.....929
  - RED.....929
- drop-profile-map statement
  - dynamic CoS.....930
- dscp statement
  - dynamic classifiers.....931
  - dynamic rewrite rules.....932
- dscp-ipv6 statement
  - dynamic classifiers.....933
  - dynamic rewrite rules.....933
- DSL Forum VSAs.....50
- DTCP See subscriber secure policy
- duplicate clients
  - DHCP.....108, 109, 162, 163
  - configuration guidelines.....109, 163
- duplicate-clients-on-interface statement
  - DHCP local server.....934
  - DHCP relay agent.....934
- duplicate-protection statement
  - dynamic PPPoE.....935
- dynamic client reconfiguration
  - DHCP local server
    - attempts configuration.....134
    - authentication token configuration.....136
    - behavior on failure configuration.....135
    - configuration overview.....133
    - RADIUS-initiated disconnect
      - configuration.....136
      - requesting.....137
- dynamic CoS statements
  - buffer-size.....875
  - class-of-service.....882

classifiers.....	882	configuration guidelines.....	558, 566
delay-buffer-rate.....	894	configuring fast update filters.....	581
drop-profile.....	929	examples.....	597
drop-profile-map.....	930	fast update filter example.....	607
dscp		fast update filters.....	564, 568
dynamic classifiers.....	931	fast update filters syntax.....	567
dynamic rewrite rules.....	932	ordering.....	574
dscp-ipv6		overview.....	555
dynamic classifiers.....	933	permitting expected traffic.....	585
dynamic rewrite rules.....	933	processing order.....	557, 565
excess-priority.....	952	types.....	556
excess-rate.....	952, 953	dynamic firewalls statements	
forwarding-class.....	969	adf.....	853
guaranteed-rate.....	986	family.....	959
ieee-802.1		fast-update-filter.....	964
dynamic classifiers.....	994	filter.....	965
dynamic rewrite rules.....	995	firewall.....	966
inet-precedence		input.....	1003
dynamic classifiers.....	1000	interface-specific.....	1031
dynamic rewrite rules.....	1001	match-order.....	1052
interface.....	1010	output.....	1092
interface-set.....	1020	post-service-filter.....	1113
interfaces.....	1026	precedence.....	1119
loss-priority.....	1044	service.....	1181
output-traffic-control-profile.....	1092	service-filter.....	1182
overhead-accounting.....	1094	service-set.....	1184
priority.....	1126	term.....	1204
protocol.....	1130	dynamic home assignment	
rewrite-rules.....	1159	configuring Mobile IP.....	360
scheduler.....	1174	Dynamic Host Control Protocol See DHCP	
scheduler-map.....	1175	dynamic IGMP statements	
scheduler-maps.....	1176	accounting.....	843
schedulers.....	1177	disable.....	918
shaping-rate.....	1186	group	
traffic-control-profiles.....	1240	with source.....	979
transmit-rate.....	1241	without source.....	979
unit.....	1255	group-limit.....	983
vlan-tag		group-policy.....	985
dynamic classifiers.....	1280	igmp.....	996
dynamic rewrite rules.....	1281	immediate-leave.....	998
dynamic firewall filters		interface.....	1009
applying fast update filters.....	591	no-accounting	
attaching statically created		interface.....	1072
any interface type.....	572	oif-map	
specific family type.....	571	interface.....	1078
attaching with RADIUS.....	573	passive	
basic syntax.....	558	interface.....	1103
classic filters.....	556	promiscuous-mode	
components.....	557, 565	interface.....	1130



- source
  - interface.....1188
- ssm-map
  - interface.....1193
- static
  - interface.....1194
- version
  - interface.....1275
- dynamic IP demux interface statements
  - demux-source.....900
  - family.....960
- dynamic IP demux statements
  - mac-validate.....1048
- dynamic MLD
  - overview.....799
- dynamic MLD interface statements
  - accounting.....844
  - exclude.....956
  - group.....980
  - group-count.....982
  - group-increment.....982
  - group-limit.....984
  - group-policy.....985
  - immediate-leave.....999
  - no-accounting.....844
  - oif-map.....1078
  - passive.....1104
  - source.....1188
  - source-count.....1189
  - source-increment.....1190
  - ssm-map.....1193
  - static.....1195
  - version.....1276
- dynamic MLD statements
  - disable.....919
  - interface.....1011
- dynamic PPP statements
  - chap.....878
  - pap.....1100
  - ppp-options.....1117
- dynamic PPPoE
  - example
    - over dynamic VLAN demux over
      - aggregated Ethernet.....519
    - over static VLAN demux over aggregated
      - Ethernet.....514
- dynamic PPPoE statements
  - destination.....902
  - duplicate-protection.....935
- dynamic-profile.....939
- family.....961
- max-sessions.....1056
- pp0.....1114
- pppoe-options.....1115
- pppoe-underlying-options.....1116
- server.....1179
- underlying-interface.....1250
- unit.....1253
- unnumbered-address.....1260
- dynamic profiles
  - associating fast update filters.....591
  - associating service sets.....595
  - components.....9
  - configuring basic.....391
  - configuring for client access.....395
  - configuring global static
    - subscriber.....289, 290, 294
  - configuring services levels.....397
  - configuring static subscriber group.....293
  - DHCP attachment.....125, 197
    - overview.....104, 158
  - domain map.....83, 89
  - examples.....401, 402, 403, 654
  - interface support.....370
    - overview.....104, 158
  - MLPPP.....402
  - MLPPP attachment.....227, 467
  - modifying.....398
  - overview.....369
  - PPP.....217, 219
  - PPP attachment.....223
  - PPPoE.....403
  - PPPoE interfaces.....217
  - predefined variables.....372
  - router predefined variables.....9
  - tiered service example.....805
  - user-defined variables.....389
  - VLAN.....409
- dynamic profiles statements
  - access.....837
  - attribute.....865
  - default-value.....894
  - dynamic-profiles.....943
  - interface.....1012
    - dynamic routing options.....1014
  - interfaces.....1027
  - keepalives.....1034
  - mandatory.....1049

metric.....	1059	router-advertisement.....	1163
mld.....	1061	valid-lifetime.....	1271
multicast		dynamic service activation	
dynamic routing options.....	1064	during login.....	35
next-hop.....	1072	dynamic service sets	
no-keepalives.....	1077	applying fast update filters.....	595
no-qos-adjust		overview.....	569
dynamic routing options.....	1077	dynamic stacked VLAN	
ppp-subscriber-services.....	1118	password authentication.....	418
predefined-variable-defaults.....	1120	dynamic subscribers	
preference.....	1120	interfaces statement.....	1027
protocols.....	1131	pppoe-underlying-options statement.....	1116
qualified-next-hop.....	1136	dynamic underlying interface statements	
radius.....	1138	demux-source.....	901
route		dynamic variables	
access.....	1160	configuring.....	392, 394
access-internal.....	1161	overview.....	371
router-advertisement.....	1163	dynamic VLAN	
routing-instances.....	1170	authentication.....	424
routing-options.....	1171	dynamic profiles.....	409
tag		any TPID configuration.....	411
access routes.....	1200	any TPID example.....	427
CoS dynamic service profile.....	1200	stacked configuration.....	413
variables.....	1272	stacked VLAN example.....	428
vendor-id.....	1273	standard TPID configuration.....	410
vlan-id.....	1278	standard TPID example.....	427
vlan-tags.....	1283	using routing instances.....	414
dynamic protocols		Ethernet packet types	
overview.....	797	configuring.....	417
dynamic requests		single-tag dynamic profiles.....	417
RADIUS.....	34, 38	stacked dynamic profiles.....	418
dynamic Router Advertisement protocol		general procedure.....	407
overview.....	801	interfaces	
dynamic router advertisement statements		configuring.....	416
autonomous.....	873	flexible tagging example.....	429
current-hop-limit.....	890	single-tag example.....	428
default-lifetime.....	891	single-tag VLAN dynamic profiles.....	416
interface.....	1013	stacked tagging example.....	428
managed-configuration.....	1049	stacked VLAN dynamic profiles.....	416
max-advertisement-interval.....	1053	overview.....	407
min-advertisement-interval.....	1060	password authentication.....	418
no-managed-configuration.....	1049	profile override.....	423
no-other-stateful-configuration.....	1091	ranges.....	419
on-link.....	1079	mixed VLAN.....	422
other-stateful-configuration.....	1091	single-level VLAN.....	419
preferred-lifetime.....	1121	stacked VLAN.....	420
prefix.....	1124	standard ethertype example.....	429
reachable-time.....	1143	verifying configuration.....	426
retransmit-timer.....	1156		

- dynamic-home-assignment statement
  - Mobile IP.....936
- dynamic-profile statement
  - DHCP local server.....937
  - DHCP relay agent.....938
  - domain maps.....938
  - dynamic PPPoE.....939
  - MLPPP.....940
  - PPP.....940
  - PPPoE service name tables.....941
  - static subscribers.....942
- dynamic-profiles
  - interfaces statement.....1027
    - dynamic IP demux.....1027
- dynamic-profiles statement.....943
- E**
  - enable-service statement
    - Mobile IP.....947
  - encapsulation statement
    - dynamic profiles.....948
  - entity-type statement
    - Mobile IP.....951
  - Ethernet interfaces
    - VLAN tagging.....1282
  - ethernet-port-type-virtual statement.....951
  - excess-priority statement
    - dynamic CoS.....952
  - excess-rate statement
    - dynamic scheduling.....952
    - dynamic traffic shaping.....953
  - exclude statement.....954
    - dynamic MLD interface.....956
  - external-authority statement
    - DHCP local server pool matching.....956
- F**
  - failover-within-preference-avp statement.....957
  - family statement
    - address-assignment pools.....958
    - dynamic firewalls.....959
    - dynamic IP demux interface.....960
    - dynamic PPPoE.....961
    - dynamic profiles.....962
  - Fast Ethernet interfaces
    - VLAN tagging.....1282
  - fast update filters.....555
    - actions.....568, 585
    - adding a term once.....569
    - applying to interfaces.....591
    - associating to dynamic profiles.....591
    - basic syntax.....567
    - components.....565
    - configuration guidelines.....566
    - configuring.....581
    - configuring match order.....582
    - configuring terms.....583
    - conflict errors.....586, 589
    - evaluating terms.....587
    - example.....607
    - implied wildcard.....588
    - match conditions.....568, 584
      - implied wildcard.....568
    - names.....566
    - only-at-create.....569
    - overlapping terms.....586, 589
    - overview.....564
    - processing order.....565
  - fast-update-filter statement
    - dynamic firewalls.....964
  - filter statement
    - dynamic firewalls.....965
  - filters
    - verifying configuration.....578, 592
  - firewall
    - fast update filter actions.....585
    - fast update filter match conditions.....584
  - firewall filters See dynamic firewall filters
    - classic filters.....556
    - configuring fast update filters.....581
    - fast update filters.....555, 564
    - overview.....556
  - firewall statement
    - dynamic profiles.....966
  - font conventions.....lv
  - forward-snooped-clients statement
    - DHCP local server.....967
    - DHCP relay agent.....968
  - forwarding statement
    - Diameter base protocol.....969
  - forwarding-class statement
    - dynamic CoS.....969
    - subscriber secure policy.....970
  - from statement
    - captive-portal-content-delivery.....970

function statement	
Diameter base protocol	
network element.....	971
route.....	972

## G

gateway-name statement	
tunnels	
LAC.....	973
LNS.....	972
general authentication service	
tracing operations.....	74
generic statement	
Mobile IP.....	973
Gigabit Ethernet interfaces	
VLAN tagging.....	1282
global statement	
Gx-Plus.....	974
grace-period statement.....	974
graceful Routing Engine switchover	
DHCP.....	139
graceful Routing Engine switchover (GRES)	
L2TP LAC.....	239
GRES See graceful Routing Engine switchover (GRES)	
group	
configuring static subscriber.....	292
group statement	
DHCP local server.....	975
DHCP relay agent.....	977
dynamic IGMP	
with source.....	979
without source.....	979
dynamic MLD interface.....	980
static subscribers.....	981
group-count statement	
dynamic MLD interface.....	982
group-increment statement	
dynamic MLD interface.....	982
group-limit statement	
dynamic IGMP.....	983
dynamic MLD interface.....	984
group-policy statement	
dynamic IGMP.....	985
dynamic MLD interface.....	985
guaranteed-rate statement	
dynamic CoS.....	986

Gx-Plus	
configuration overview.....	339
Diameter message sequences.....	335
Diameter messages.....	330
interactions with the PCRF.....	335
number of outstanding requests	
configuring.....	341
overview.....	329
partition	
configuring.....	340
provisioning subscribers.....	341
tracing operations.....	74
verifying.....	266, 267
gx-plus statement	
Gx-Plus.....	987
Gx-Plus statements	
destination-host.....	903
destination-realm.....	905
diameter-instance.....	917
global.....	974
gx-plus.....	987
max-outstanding-requests.....	1055
partition.....	1101
provisioning-order.....	1133

## H

hardware-address statement.....	987
highUtilization statement	
address-assignment pools.....	988
highUtilization-v6 statement	
address-assignment pools.....	988
home agent	
configuration overview.....	358
home agent, Mobile IP See Mobile IP home agent	
home-agent statement	
Mobile IP	
dynamic home assignment rule.....	989
IP address rule.....	990
networks.....	991
home-agent-address statement	
Mobile IP.....	992
host statement	
address-assignment pools.....	993
Diameter base protocol.....	993
HTTP redirect	
configuring subscriber interfaces.....	615

- 
- HTTP service
    - example configuring attached to a dynamic interface.....621
    - example configuring attached to a static interface.....621
    - example configuring within a service set.....620
  - I
  - IA\_NA
    - DHCPv6 local server.....123
  - icons defined, notice.....liv
  - identification statement
    - tunnels.....994
  - idle timeout
    - subscriber access.....54
  - ieee-802.1 statement
    - dynamic classifiers.....994
    - dynamic rewrite rules.....995
  - ietf-mode statement
    - ANCP.....995
  - IGMP
    - enabling.....996, 1132
    - version.....1275
  - igmp statement
    - dynamic IGMP.....996
  - ignore statement.....997
  - immediate-leave statement
    - dynamic IGMP.....998
    - dynamic MLD interface.....999
  - immediate-update statement
    - accounting.....1000
  - inet-precedence statement
    - dynamic classifiers.....1000
    - dynamic rewrite rules.....1001
  - inner-tag-protocol-id statement
    - dynamic VLAN interfaces.....1001
  - inner-vlan-id statement
    - dynamic VLAN interfaces.....1002
  - input statement
    - dynamic service sets.....1003
  - input-vlan-map statement
    - dynamic interfaces.....1004
  - interface delete events
    - maintaining subscribers.....123, 124, 185
  - interface groups
    - DHCP local server
      - configuration guidelines.....113, 166
      - options.....115
    - DHCP relay
      - configuration guidelines.....113, 166
      - options.....167
      - enabling static subscribers to log in.....296
      - forcing static subscribers to log out.....296
  - interface ranges
    - DHCP configuration guidelines.....113, 166
  - interface statement
    - DHCP local server.....1005
    - DHCP relay agent.....1007
    - dynamic CoS.....1010
    - dynamic IGMP.....1009
    - dynamic MLD.....1011
    - dynamic neighbor discovery.....1013
    - dynamic profiles.....1012
    - multicast
      - dynamic routing options.....1014
    - static subscriber group.....1015
    - static subscribers username.....1016
  - interface-client-limit statement
    - DHCP local server.....1017
    - DHCP relay agent.....1018
  - interface-delete statement
    - subscriber management.....1019
  - interface-description-format statement.....1019
  - interface-set statement
    - ANCP.....1030
    - dynamic CoS.....1020
  - interface-specific statement
    - dynamic firewalls.....1031
  - interface-traceoptions statement
    - DHCP local server.....1021
    - DHCP relay agent.....1023
  - interfaces
    - enabling static subscribers to log in.....296
    - forcing static subscribers to log out.....296
    - unit statement.....1257
  - interfaces statement
    - ANCP.....1025
    - dynamic CoS.....1026
    - dynamic profiles.....1027
    - subscriber secure policy.....1024
  - Internet Group Management Protocol See IGMP
  - IP demultiplexing interface statements
    - unit.....1251

ip-address statement.....	1031
ip-address-first statement.....	1032
ISSU See see unified ISSU	

## J

### JSRC

authorizing subscribers.....	281
configuration overview.....	279, 288
Diameter message sequences.....	276
Diameter messages.....	272
interactions with the SAE.....	276
managing subscribers.....	271
partition	
assigning.....	281
configuring.....	280
provisioning services.....	271
provisioning static subscribers.....	283
provisioning subscribers.....	282
tracing operations.....	74
verifying.....	266, 267

### jsrc statement

JSRC.....	1033
-----------	------

### JSRC statements

authentication-order.....	872
destination-host.....	903
destination-realm.....	905
diameter-instance.....	917
jsrc.....	1033
jsrc-partition.....	1033
partition.....	1101
provisioning-order.....	1133

### jsrc-partition statement

JSRC.....	1033
-----------	------

### Juniper Networks VSAs.....

corresponding predefined variables.....	385
supported.....	45

## K

### keepalives statement

dynamic profiles.....	1034
-----------------------	------

### key statement

Mobile IP.....	1035
----------------	------

## L

### L2TP

verifying configuration.....	250
------------------------------	-----

### L2TP (Layer 2 Tunneling Protocol)

defining.....	231
event logging.....	247

failover.....	238
log file size and number.....	248
peer resynchronization.....	238
terminology.....	233
tracing operations.....	247
tunnel profile configuration.....	242
LAC address.....	242
LAC hostname.....	242
LNS address.....	242
LNS hostname.....	242
logical system.....	242
maximum sessions.....	242
password.....	242
preference.....	242
profile name.....	242
routing instance.....	242
tunnel assignment ID.....	242
tunnel identifier.....	242
tunnel medium.....	242
tunnel type.....	242

L2TP access concentrator. See LAC (L2TP access concentrator)

### L2TP failover protocol

preventing L2TP LAC from negotiating.....	246
---	-----

### L2TP LAC

GRES.....	239
subscriber secure policy.....	627

### L2TP LAC statements

disable-calling-number-avp.....	919
disable-failover-protocol.....	920
failover-within-preference.....	957
weighted-load-balancing.....	1284

### L2TP statements

tracoptions.....	1225
------------------	------

### LAC (L2TP access concentrator)

configuration overview.....	241
disabling Calling Number AVP 22.....	246
disabling L2TP failover protocol.....	246
flags for tracing operations.....	249
function.....	231
log file access for tracing operations.....	248
log filenames.....	247
regular expressions for tracing	
operations.....	249
tunnel selection failover configuration.....	244
tunnel selection methods.....	235
tunnel selection parameter configuration.....	244
weighted load balancing configuration.....	245

lawful intercept See subscriber secure policy

- 
- Layer 2 Tunneling Protocol. *See* L2TP (Layer 2 Tunneling Protocol)
  - layer2-unicast-replies statement.....1036
  - license requirements
    - address-assignment pools.....74
    - subscriber access.....6
    - subscriber secure policy.....628
  - link statement
    - address-assignment pools.....1037
  - local-server-group statement.....1038
  - log files
    - access to Diameter base protocol.....264
    - access to Mobile IP.....364
    - collecting for Juniper Technical Support.....12
    - configuring ANCP trace.....792
    - configuring Diameter base protocol trace.....262
    - configuring L2TP trace.....247
    - configuring Mobile IP trace.....361
    - configuring static subscribers trace.....297
    - filenames for Diameter base protocol.....263
    - filenames for L2TP LAC.....247
    - filenames for Mobile IP.....363
    - filenames for subscriber management
      - database.....59
    - filenames for subscriber management session
      - database replication.....64
    - number of ANCP.....793
    - number of Diameter base protocol.....264
    - number of L2TP.....248
    - number of Mobile IP.....363
    - number of static subscribers.....298
    - number of subscriber management
      - database.....59
    - number of subscriber management session
      - database replication.....62
    - profile properties.....325
    - size of ANCP.....793
    - size of Diameter base protocol.....264
    - size of L2TP.....248
    - size of Mobile IP.....363
    - size of packet-triggered subscribers.....314
    - size of PTSP.....325
    - size of static subscribers.....298
    - size of subscriber management database.....59
    - size of subscriber management session
      - database replication.....62
  - logical interface statements
    - family.....962
    - logical-interface-fpc-redundancy statement
      - aggregated Ethernet.....1039
    - logical-system statement.....1040
      - Diameter base protocol.....1039
      - tunnels.....1040
    - logical-system-name statement
      - DHCP local server.....1041
      - DHCP relay agent.....1042
      - static subscribers.....1043
  - loss-priority statement
    - dynamic CoS.....1044
- M**
- MAC address validation
    - dynamic subscriber interfaces
      - configuring.....448
      - overview.....437
    - static subscriber interfaces
      - configuring.....448
  - mac-address statement
    - access internal routes.....1047
    - DHCP local server.....1045
    - DHCP relay agent.....1046
  - mac-validate statement.....1048
  - maintain-subscriber statement
    - subscriber management.....1048
  - maintaining subscribers
    - interface delete events.....123, 124, 185
    - verifying configuration.....125, 186
  - managed-configuration statement
    - dynamic router advertisement.....1049
  - mandatory statement
    - dynamic profile variables.....1049
  - manuals
    - comments on.....lvi
  - map statement
    - domain maps.....1050
  - mask statement
    - domain maps.....1051
  - match conditions
    - fast update filters
      - implied wildcard.....568
  - match-direction statement
    - content-delivery-captive-portal.....1051
  - match-order statement
    - dynamic firewalls.....1052
  - max-advertisement-interval statement
    - dynamic router advertisement.....1053

max-outstanding-requests statement		
Gx-Plus.....	1055	
max-sessions statement		
dynamic PPPoE.....	1056	
PPPoE service name tables.....	1057	
tunnels.....	1058	
maximum-discovery-table-entries statement		
ANCP.....	1053	
maximum-helper-restart-time statement		
ANCP.....	1054	
maximum-lease-time statement.....	1054	
medium statement		
tunnels.....	1058	
metric statement		
Diameter base protocol.....	1059	
domain maps.....	1060	
dynamic profiles.....	1059	
min-advertisement-interval statement		
dynamic router advertisement.....	1060	
MLD		
enabling.....	1061	
mld statement		
dynamic profiles.....	1061	
MLPPP		
dynamic PPP subscriber services.....	226	
dynamic profile attachment.....	227, 467, 940	
dynamic profiles.....	402	
enabling PPP subscriber services.....	226	
hardware requirements for PPP subscriber		
services.....	226	
PPP subscriber services overview.....	225	
Mobile IP		
access type configuration.....	361	
accounting method.....	360	
authentication method.....	358	
configuration overview.....	357	
dynamic home assignment		
configuration.....	360	
event log access.....	364	
event logging.....	361	
filtering trace operation output.....	364	
flags for tracing operations.....	365	
local authentication attributes.....	359	
log file size.....	363	
log filenames.....	363	
registration request authentication.....	358	
tracing operations.....	361	
WiMAX operation.....	361	
Mobile IP home agent		
AAA.....	348	
accounting.....	351	
agent discovery.....	345	
authentication.....	348	
home address assignment.....	345	
mobile node registration.....	348	
overview.....	345	
Mobile IP statements		
access-type.....	842	
algorithm.....	858	
authenticate.....	867	
dynamic-home-assignment.....	936	
enable-service.....	947	
entity-type.....	951	
generic.....	973	
home-agent		
dynamic home assignment rule.....	989	
IP address rule.....	990	
networks.....	991	
home-agent-address.....	992	
key.....	1035	
mobile-ip.....	1062	
nai.....	1065	
order.....	1090	
peer.....	1108	
registration-lifetime.....	1146	
replay-method.....	1155	
revocation-required.....	1158	
spi.....	1192	
statistics.....	1197	
timestamp-tolerance.....	1209	
traceoptions.....	1229	
virtual-network.....	1277	
wimax.....	1284	
mobile-ip statement		
Mobile IP.....	1062	
mode statement.....	1063	
multicast		
configuration statements.....	1064	
multicast statement		
dynamic routing options.....	1064	
Multiservices DPC		
configuring PTSP.....	318	
<b>N</b>		
nai statement		
Mobile IP.....	1065	
name-server statement.....	1066	



- nas-identifier statement.....1066
- nas-port-extended-format statement.....1067
- neighbor
  - parameters for ANCP.....786
- neighbor statement
  - ANCP
    - for all neighbors.....1068
    - for unique access identifier.....1068
- neighbor-discovery-router-advertisement
  - statement
    - address-assignment pools.....1069
- netbios-node-type statement.....1069
- network element
  - configuring Diameter.....261
- network statement.....1070
- network-element statement
  - Diameter base protocol.....1071
- next-hop statement
  - dynamic profiles.....1072
- no-accounting statement
  - dynamic IGMP
    - interface.....1072
  - dynamic MLD interface.....844
- no-allow-snooped-clients statement
  - DHCP relay agent.....1073
- no-arp statement
  - DHCP local server.....1074
  - DHCP relay agent.....1075
- no-bind-on-request statement
  - DHCP relay agent.....1076
- no-keepalives statement
  - dynamic profiles.....1077
- no-managed-configuration statement
  - dynamic router advertisement.....1049
- no-other-stateful-configuration statement
  - dynamic router advertisement.....1091
- no-qos-adjust statement
  - dynamic routing options.....1077
- non-link-protected aggregated Ethernet interfaces
  - manually rebalancing subscribers.....485
  - periodically rebalancing subscribers.....485
  - rebalancing subscribers.....485
- notice icons defined.....liv
- O**
- olf-map statement
  - dynamic IGMP
    - interface.....1078
  - dynamic MLD interface.....1078
- on-link statement
  - dynamic router advertisement.....1079
- option 50
  - DHCP local server.....123
- option 60 information
  - DHCP relay.....189
- option 60 strings
  - DHCP relay.....189, 192
- option 82
  - DHCP relay
    - auto logout.....182
- option 82 information
  - DHCP relay.....192
- option 82 prefix
  - DHCP relay.....193
- option 82 textual description
  - DHCP relay.....195
- option statement.....1080
- option-60 statement
  - DHCP local server.....1081
  - DHCP relay agent.....1082
- option-82 statement
  - address-assignment pools.....1083
  - DHCP local server authentication.....1084
  - DHCP local server pool matching.....1085
  - DHCP relay agent.....1086
- option-match statement.....1087
- options
  - RADIUS server.....28, 29
- options statement
  - RADIUS.....1088
- order statement
  - accounting.....1089
  - Mobile IP.....1090
- origin attributes
  - configuring Diameter endpoint.....260
- origin statement
  - Diameter base protocol.....1091
- other-stateful-configuration statement
  - dynamic router advertisement.....1091
- output statement
  - dynamic service sets.....1092
- output-traffic-control-profile statement
  - dynamic CoS.....1092
- output-vlan-map statement
  - dynamic interfaces.....1093
- outstanding requests
  - Gx-Plus, configuring.....341

overhead-accounting statement	
dynamic CoS.....	1094
overrides statement	
DHCP local server.....	1095
DHCP relay agent.....	1097

## P

packet-triggered subscribers.....	309
flags for tracing operations.....	314, 326
log file size.....	314
log filenames for tracing operations.....	313
monitoring.....	327
profile properties.....	325
record type.....	326
tracing operations.....	313, 324
packet-triggered subscribers and policy control See PTSP	
packet-triggered-subscribers statement.....	1098
packet-triggered-subscribers-partition statement.....	1099
padn statement	
domain maps.....	1099
pap statement	
dynamic PPP.....	1100
parentheses, in syntax descriptions.....	lv
parse-direction statement	
domain maps.....	1100
partition	
Gx-Plus, configuring.....	340
JSRC, assigning.....	281
JSRC, configuring.....	280
partition statement	
Gx-Plus.....	1101
JSRC.....	1101
PTSP.....	1102
passive statement	
dynamic IGMP	
interface.....	1103
dynamic MLD interface.....	1104
password	
configuring global static subscriber authentication.....	290
configuring static subscriber group authentication.....	294
stacked VLAN range.....	418
VLAN range.....	418

password statement	
DHCP local server.....	1105
DHCP relay agent.....	1106
static subscribers.....	1107
passwords	
DHCP users.....	127
PCRF	
interactions with Gx-Plus.....	335
peer	
configuring Diameter.....	260
peer statement	
Diameter base protocol	
network element.....	1109
remote peer.....	1109
Mobile IP.....	1108
per-interface tracing operations	
DHCP local server.....	144, 203
DHCP relay.....	144, 203
physical interfaces	
VLAN tagging.....	1282
pool statement	
address-assignment pools.....	1110
pool-match-order statement.....	1111
pop statement	
dynamic VLAN interfaces.....	1111
port statement	
Diameter base protocol.....	1112
RADIUS servers.....	1112
post-service-filter statement	
dynamic service sets.....	1113
pp0 statement	
dynamic PPPoE.....	1114
PPP	
access and access-internal routes.....	205, 220
dynamic profile attachment.....	223, 940
dynamic profile creation.....	219
dynamic profiles.....	217
verifying subscriber management	
configuration.....	223
PPP subscriber services	
enabling on non-Ethernet interfaces.....	226
hardware requirements on non-Ethernet interfaces.....	226
MLPPP bundle interfaces.....	226
on MLPPP, overview.....	225
ppp-options statement	
dynamic PPP.....	1117
ppp-subscriber-services statement	
dynamic profiles.....	1118

- 
- PPPoE
    - dynamic profiles.....403
    - dynamic subscriber interfaces
      - benefits.....527
      - configuration examples.....547, 549
      - configuration overview.....531, 535
      - configuring the underlying interface.....541
      - configuring with additional options.....539
      - configuring with basic options.....536
      - creating with PPPoE service name
        - tables.....543
      - PPPoE overview.....527
      - verifying the configuration.....544
    - example
      - dynamic PPPoE over dynamic VLAN
        - demux over aggregated Ethernet.....519
      - dynamic PPPoE over static VLAN demux
        - over aggregated Ethernet.....514
      - static PPPoE over static VLAN demux over
        - aggregated Ethernet.....509
    - service name tables
      - creating dynamic PPPoE subscriber
        - interfaces.....543
      - evaluation order for matching client
        - information.....552
  - PPPoE family
    - on underlying interface configuration.....486
  - pppoe-options statement
    - dynamic PPPoE.....1115
  - pppoe-underlying-options statement
    - static and dynamic PPPoE.....1116
  - pre-ietf mode
    - ANCP global configuration.....789
    - ANCP neighbor configuration.....786, 789
  - pre-ietf-mode statement
    - ANCP.....1125
  - precedence statement.....1119
  - predefined variables.....372
    - corresponding RADIUS attributes and
      - VSAs.....385
  - predefined-variable-defaults statement
    - dynamic CoS.....1120
  - preference statement
    - dynamic profiles.....1120
    - tunnels.....1121
  - preferred-lifetime statement.....1121
  - prefix statement
    - address-assignment pools.....1122
    - DHCP relay agent.....1123
    - dynamic router advertisement.....1124
  - priority statement
    - Diameter base protocol.....1125
    - dynamic CoS.....1126
  - profile statement
    - subscriber access.....1127
  - promiscuous-mode statement
    - dynamic IGMP
      - interface.....1130
  - protocol statement
    - dynamic CoS.....1130
  - protocols statement
    - dynamic profiles.....1131
  - provisioning-order statement
    - subscriber services.....1133
  - proxy-arp statement.....1133
  - proxy-mode statement.....1134
  - PTSP
    - configuration overview.....311, 317
    - configuring forward rules.....322
    - configuring forwarding instance.....322
    - configuring rules.....319
    - configuring service sets.....322
    - configuring services interface.....318
    - configuring static policies.....319
    - configuring static rule sets.....321
    - configuring static rules.....319
    - Diameter AVPs.....305
    - Diameter message sequences.....308
    - Diameter messages.....304
    - flags for tracing operations.....326
    - interactions with the SAE.....308
    - log file size.....325
    - log filenames for tracing operations.....325
    - managing subscribers.....304
    - monitoring.....327
    - overview.....303
    - profile properties.....325
    - provisioning packet-triggered
      - subscribers.....309
    - provisioning services.....304
    - record type.....326
    - tracing operations.....313, 324
    - verifying.....266, 267
  - push statement
    - dynamic VLAN interfaces.....1135

**Q**

qos-adjust statement	
ANCP.....	1135
qualified-next-hop statement	
dynamic profiles.....	1136

**R**

<b>RADIUS</b>	
Acct-Off messages.....	22
Acct-On messages.....	22
CoA.....	35
CoS parameters for initial services	
configuring an access dynamic	
profile.....	697
example.....	721
overview.....	689
dynamic requests.....	34, 38
RADIUS attributes.....	39
corresponding predefined variables.....	385
defining L2TP tunnels.....	242
ignoring and excluding.....	31
supported.....	39
RADIUS dynamic request information	
verifying.....	38
RADIUS server	
configuring interaction with.....	20
configuring parameters.....	26
options.....	28, 29
RADIUS servers See subscriber secure policy	
configuration example.....	91
specifying.....	27
radius statement	
dynamic profile variables.....	1138
subscriber access.....	1137
radius-disconnect statement	
DHCP local server.....	1139
radius-flow-tap service See subscriber secure policy	
radius-flow-tap statement.....	1140
RADIUS-initiated disconnect.....	37
messages.....	37
radius-server statement.....	1141
range statement	
address-assignment pools.....	1142
reachable-time statement	
dynamic router advertisement.....	1143
realm statement	
Diameter base protocol.....	1144
rebalance-periodic statement	
aggregated Ethernet.....	1143
reconfigure statement	
DHCP local server.....	1145
registration	
Mobile IP mobile node.....	348
registration-lifetime statement	
Mobile IP.....	1146
relay-agent-interface-id statement.....	1147
relay-agent-remote-id statement.....	1148
relay-agent-subscriber-id statement.....	1149
relay-option-60 statement.....	1150
relay-option-82 statement	
deleting.....	192, 1151
relay-server-group statement.....	1152
remote-gateway statement	
tunnels.....	1153
remote-id statement.....	1153
replace-ip-source-with statement.....	1154
replay-method statement	
Mobile IP.....	1155
restart time	
ANCP global configuration.....	789
resynchronization, peer	
L2TP.....	238
retransmit-timer statement	
dynamic router advertisement.....	1156
retry statement.....	1156
revert-interval statement.....	1157
revocation-required statement	
Mobile IP.....	1158
rewrite-rules statement	
dynamic CoS.....	1159
route statement	
access internal	
dynamic profiles.....	1161
Diameter base protocol.....	1162
dynamic profiles.....	1160
router statement	
address-assignment pools.....	1162
router-advertisement statement	
dynamic profiles.....	1163
routing-instance statement	
Diameter base protocol peer.....	1164
Diameter transport.....	1164
PPPoE service name tables.....	1166
RADIUS.....	1163
tunnels.....	1165

- 
- routing-instance-name statement
    - DHCP local server.....1167
    - DHCP relay agent.....1168
    - static subscribers.....1169
  - routing-instances statement
    - dynamic profiles.....1170
  - routing-options statement
    - dynamic profiles.....1171
  - rpf-check statement.....1172
  - rule statement
    - captive-portal-content-delivery.....1173
  - rule-set statement
    - captive-portal-content-delivery.....1174
  - S**
  - SAE
    - interactions with JSRC.....276
    - interactions with PTSP.....308
  - scheduler statement
    - dynamic CoS.....1174
  - scheduler-map statement
    - dynamic CoS
      - association with traffic-control
        - profile.....1175
  - scheduler-maps statement
    - dynamic CoS
      - scheduler map configuration.....1176
  - schedulers statement
    - dynamic CoS.....1177
  - secret statement
    - access.....1178
    - tunnels.....1178
  - send-release-on-delete statement
    - DHCP relay agent.....1179
  - server groups
    - DHCP relay.....195
  - server statement
    - dynamic PPPoE.....1179
  - server-group statement.....1180
  - server-identifier statement
    - address-assignment pools.....1180
  - service name tables
    - PPPoE
      - evaluation order for matching client
        - information.....552
  - service name tables, PPPoE
    - creating dynamic PPPoE subscriber
      - interfaces.....543
  - service provisioning
    - packet-triggered subscribers with PTSP.....309
    - static subscribers with JSRC.....283
    - with JSRC.....271
    - with PTSP.....304
  - service sets
    - applying to interfaces.....595
    - associating to dynamic profiles.....595
    - dynamic.....569
  - service statement
    - dynamic service sets.....1181
  - service-filter statement
    - dynamic service sets.....1182
  - service-name-table statement
    - PPPoE underlying interface.....1183
  - service-set statement
    - dynamic service sets.....1184
  - service-sets
    - verifying configuration.....596
  - services statement
    - captive-portal-content-delivery.....1185
  - session options
    - subscriber access.....54
  - session options statements
    - client-idle-timeout.....888
    - client-session-timeout.....889
  - session timeout
    - subscriber access.....54
  - session-options statement
    - access profile.....1185
  - shaping-rate adjustments.....752
    - for subscriber local loops.....781
      - configuration guidelines.....754
      - disabling.....767
      - enabling.....762
      - example.....774
      - overview.....753
  - shaping-rate statement
    - dynamic CoS.....1186
  - silent failover
    - L2TP.....238
  - sip-server-address statement.....1187
  - sip-server-domain-name statement.....1187
  - SNMPv3 traps
    - subscriber secure policy.....645
    - subscriber secure policy configuration.....646

source statement		
dynamic IGMP		
interface.....	1188	
dynamic MLD interface.....	1188	
source-address statement		
RADIUS.....	1189	
source-count statement		
dynamic MLD interface.....	1189	
source-gateway statement		
tunnels.....	1190	
source-increment statement		
dynamic MLD interface.....	1190	
source-ipv4-address statement.....	1191	
spi statement		
Mobile IP.....	1192	
SRC		
packet-triggered subscriber management with		
PTSP.....	309	
SAE interactions with JSRC.....	276	
SAE interactions with PTSP.....	308	
static subscriber management with JSRC.....	283	
subscriber management with JSRC.....	271	
subscriber management with PTSP.....	304	
ssm-map statement		
dynamic IGMP		
interface.....	1193	
dynamic MLD interface.....	1193	
static PPPoE		
example		
over static VLAN demux over aggregated		
Ethernet.....	509	
static PPPoE statements		
pppoe-underlying-options.....	1116	
static statement		
dynamic IGMP		
interface.....	1194	
dynamic MLD interface.....	1195	
static subscriber group statements		
interface.....	1015	
static subscriber statements		
access-profile.....	841	
aggregate-clients.....	857	
authentication.....	870	
domain-name.....	926	
dynamic-profile.....	942	
group.....	981	
interface.....	1016	
logical-system-name.....	1043	
password.....	1107	
routing-instance.....	1169	
static-subscribers.....	1196	
traceoptions.....	1234	
user-prefix.....	1266	
username-include.....	1270	
static subscribers.....	283	
configuring interface groups.....	292	
event logging.....	297	
flags for tracing operations.....	299	
forcing logout.....	296	
forcing logout for interface groups.....	296	
global access profile.....	289	
global authentication password.....	290	
global dynamic profile.....	289, 290, 294	
global username.....	291	
group.....	292	
group access profile.....	293	
group authentication password.....	294	
group dynamic profile.....	293	
group username.....	295	
interfaces statement.....	1027	
log file access for tracing operations.....	298	
log file size and number.....	298	
log filenames for tracing operations.....	298	
pppoe-underlying-options statement.....	1116	
regular expressions for tracing		
operations.....	299	
resetting login state for an interface.....	296	
resetting login state for interface groups.....	296	
tracing operations.....	297	
static-subscribers statement.....	1196	
statistics statement		
access.....	1197	
strict statement		
DHCP local server.....	1198	
strip-domain statement		
domain maps.....	1198	
subscriber AAA information		
verifying.....	65	
subscriber access		
configuration overview.....	9	
environment.....	4	
license requirements.....	6	
managing access and services.....	8	
operation flow.....	7	
overview.....	3	
support.....	5	

- subscriber interface statements
  - .....1253
  - access-concentrator.....838
  - address.....848
  - chap.....878
  - demux-options.....899
  - demux-source.....900, 901
  - demux0.....898
  - destination.....902
  - duplicate-protection.....935
  - dynamic-profile.....939
  - family.....960, 961, 962
  - interfaces.....1027
  - mac-validate.....1048
  - max-sessions.....1056
  - mode.....1063
  - pap.....1100
  - pp0.....1114
  - ppp-options.....1117
  - pppoe-options.....1115
  - pppoe-underlying-options.....1116
  - proxy-arp.....1133
  - rpf-check.....1172
  - server.....1179
  - underlying-interface.....1249, 1250
  - unit.....1251, 1257
  - unnumbered-address.....1259, 1260
  - vlan-tagging.....1282
- subscriber interfaces
  - captive portal content delivery
    - configuring .....615
  - configuring in dynamic profiles.....439
  - example
    - dynamic PPPoE over dynamic VLAN
      - demux over aggregated Ethernet.....519
    - dynamic PPPoE over static VLAN demux
      - over aggregated Ethernet.....514
    - gigabit Ethernet VLAN.....452
    - gigabit Ethernet VLAN with multiple logical
      - units.....451
    - gigabit Ethernet VLAN with no
      - autonegotiation.....452
    - IP demux over aggregated Ethernet.....492
    - loopback.....452
    - static PPPoE over static VLAN demux over
      - aggregated Ethernet.....509
    - VLAN over aggregated
      - Ethernet.....489, 494
- IP demux
  - configuring.....443, 444
  - guidelines.....436
  - overview.....435
- IP demux over aggregated Ethernet
  - example.....492
  - overview.....472
- overview.....5, 433
- PPPoE
  - benefits.....527
  - configuration examples.....547, 549
  - configuration overview.....531
  - configuring the underlying interface.....541
  - configuring with additional options.....539
  - configuring with basic options.....536
  - dynamic configuration overview.....535
  - PPPoE overview.....527
  - verifying the configuration.....544
- PPPoE family on underlying interface.....486
- VLAN
  - configuring.....440
  - overview.....434
- VLAN demux
  - guidelines.....436
  - overview.....435
- VLAN demux over aggregated Ethernet
  - overview.....472
- VLAN over aggregated Ethernet
  - configuring.....479
  - example.....489, 494
  - overview.....471
- subscriber local loops
  - CoS shaping-rate adjustments
    - configuration guidelines.....754
    - disabling.....767
    - enabling.....762
    - example.....774
    - overview.....753
  - CoS shaping-rate adjustments with
    - ANCP.....781
- subscriber management
  - packet-triggered.....309
  - static.....283
  - with JSRC.....271
  - with PTSP.....304
- subscriber management database
  - flags for tracing operations.....60
  - log file access for tracing operations.....59
  - log file size and number.....59

log filenames.....	59
regular expressions for tracing operations.....	60
tracing operations.....	58
subscriber management session database replication	
flags for tracing operations.....	64
log file access for tracing operations.....	63
log file size and number.....	62
log filenames.....	64
regular expressions for tracing operations.....	63
tracing operations.....	61
subscriber management statements	
interface-delete.....	1019
maintain-subscriber.....	1048
subscriber-management.....	1199
traceoptions.....	1236
subscriber provisioning	
Gx-Plus.....	341
JSRC.....	282
subscriber secure policy	
architecture.....	628
configuration guidelines.....	631
configuring DTCP-initiated.....	641
configuring RADIUS-initiated.....	635
configuring SNMPv3 traps.....	646
considerations.....	638
DTCP.....	644, 651
DTCP configuration.....	642
dynamic profile example.....	403, 654
L2TP LAC subscribers.....	627
LAES compliance.....	645
license requirements.....	628
overview.....	625
RADIUS server configuration.....	639
radius-flow-tap service.....	631
radius-flow-tap service configuration.....	632
RADIUS-initiated.....	636
SNMPv3 trap example.....	655
SNMPv3 traps.....	645
system resources.....	636, 642
terminating.....	639
using RADIUS.....	649
subscriber service session	
accounting statistics.....	25, 576
subscriber session	
accounting statistics.....	24
subscriber session database statements	
database-replication.....	891
traceoptions.....	1238
subscriber session options	
configuration overview.....	55
subscriber-management statement	
subscriber management.....	1199
subscribers	
identifying ANCP.....	787
support, technical See technical support	
swap statement	
dynamic VLAN interfaces.....	1199
syntax conventions.....	lv
<b>T</b>	
tag statement	
access.....	1200
dynamic profile variables.....	1200
dynamic profiles access route.....	1200
tag-protocol-id statement	
dynamic VLAN map.....	1201
target logical system/routing instance	
domain map.....	85
target-logical-system statement	
domain maps.....	1202
target-routing-instance statement	
domain maps.....	1203
targeted-distribution statement	
aggregated Ethernet.....	1203
technical support	
collecting logs for.....	12
contacting JTAC.....	lvi
term statement	
captive-portal-content-delivery.....	1205
fast update filters.....	1204
tftp-server statement.....	1205
then statement	
captive-portal-content-delivery.....	1206
time-based accounting	
Mobile IP.....	360
timeout statement	
access.....	1208
DHCP local server.....	1207
timeouts	
idle and session.....	54
timestamp-tolerance statement	
Mobile IP.....	1209
token statement	
DHCP local server.....	1210



- trace operations
  - collecting logs for Juniper technical support.....12
  - filtering output for Diameter base protocol.....265
  - filtering output for Mobile IP.....364
- trace statement
  - DHCP local server.....1211
  - DHCP relay agent.....1212
- traceoptions statement
  - address-assignment pools.....1213
  - ANCP.....1215
  - captive-portal-content-delivery.....1217
  - DHCP local server.....1219
  - DHCP relay agent.....1221
  - Diameter base protocol.....1223
  - general authentication service.....1213
  - L2TP.....1225
  - Mobile IP.....1229
  - PTSP.....1232
  - static subscribers.....1234
  - subscriber management.....1236
  - subscriber session database replication.....1238
- tracing operations
  - address-assignment pools.....74
  - ANCP.....792
  - DHCP local server.....139, 199
  - DHCP local server interface-specific.....1021
  - DHCP relay.....139, 199
  - DHCP relay interface-specific.....1023
  - Diameter base protocol.....262
  - general authentication service.....74
  - Gx-Plus.....74
  - JSRC.....74
  - L2TP.....247
  - Mobile IP.....361
  - packet-triggered subscribers.....313, 324
  - PTSP.....313, 324
  - static subscribers.....297
  - subscriber management database.....58
  - subscriber management session database replication.....61
- traffic mirroring See subscriber secure policy
- traffic shaping
  - ANCP CoS.....790
- traffic-control-profiles statement
  - dynamic CoS.....1240
- transmit-rate statement
  - dynamic CoS.....1241
- transport
  - configuring Diameter.....262
- transport statement.....1242
- trigger statement
  - DHCP local server.....1243
- troubleshooting subscriber access
  - collecting logs for Juniper Technical Support.....12
- trust-option-82 statement.....1244
- tunnel profile
  - domain map.....88
- tunnel profile, L2TP
  - configuration.....242
- tunnel selection failover
  - configuring for L2TP LAC.....244
- tunnel statement
  - tunnels.....1245
- tunnel statements
  - address
    - remote gateway.....849
    - source gateway.....850
  - gateway-name
    - remote gateway.....972
    - source gateway.....973
  - identification.....994
  - logical-system.....1040
  - max-sessions.....1058
  - medium.....1058
  - preference.....1121
  - remote-gateway.....1153
  - routing-instance.....1165
  - secret.....1178
  - source-gateway.....1190
  - tunnel.....1245
  - tunnel-profile.....1247
  - type.....1248
- tunnel-profile statement
  - domain maps.....1246
  - tunnels.....1247
- type statement
  - tunnels.....1248
- U**
- underlying-interface statement
  - dynamic PPPoE.....1250
  - dynamic profiles.....1249
- unified ISSU
  - DHCP access model.....6

unified ISSU state	
verifying.....	7
unit statement	
demux interfaces.....	1251
dynamic CoS.....	1255
dynamic PPPoE.....	1253
interfaces.....	1257
unnumbered-address statement.....	1259
dynamic PPPoE.....	1260
update-interval statement.....	1260
use-interface-description statement.....	1261
use-primary statement	
DHCP local server.....	1262
DHCP relay agent.....	1263
user-defined variables.....	389 See variables,
u s e r - d e f i n e d	
user-prefix statement	
DHCP local server.....	1264
DHCP relay agent.....	1265
static subscribers.....	1266
username	
configuring global static subscriber.....	291
configuring static subscriber group.....	295
username information	
AAA authentication.....	425
username-include statement	
DHCP local server.....	1267
DHCP relay agent.....	1269
static subscribers.....	1270
<b>V</b>	
valid-lifetime statement.....	1271
variables	
overview.....	371
predefined.....	372
user-defined.....	389
variables statement	
dynamic profile variables.....	1272
variables, Junos OS predefined	
dynamic CoS (schedulers)	
\$junos-cos-scheduler.....	689
\$junos-cos-scheduler-bs.....	689
\$junos-cos-scheduler-dropfile-any.....	689
\$junos-cos-scheduler-dropfile-high.....	689
\$junos-cos-scheduler-dropfile-low.....	689
\$junos-cos-scheduler-dropfile-medium-high.....	689
\$junos-cos-scheduler-dropfile-medium-low.....	689
\$junos-cos-scheduler-pri.....	689
\$junos-cos-scheduler-tx.....	689
example.....	721
overview.....	689
dynamic CoS (traffic-control-profiles)	
example.....	721
overview.....	689
variables, Junos predefined	
corresponding RADIUS attributes and	
VSAs.....	385
defaults.....	1120
dynamic CoS (schedulers)	
\$junos-cos-scheduler.....	1177
\$junos-cos-scheduler-bs.....	875
\$junos-cos-scheduler-dropfile-any.....	929
\$junos-cos-scheduler-dropfile-high.....	929
\$junos-cos-scheduler-dropfile-low.....	929
\$junos-cos-scheduler-dropfile-medium-high.....	929
\$junos-cos-scheduler-dropfile-medium-low.....	929
\$junos-cos-scheduler-pri.....	1126
\$junos-cos-scheduler-tx.....	1241
configuring an access dynamic	
profile.....	697
dynamic CoS (traffic control profiles)	
\$junos-cos-delay-buffer-rate.....	894
\$junos-cos-excess-priority.....	952
\$junos-cos-excess-rate.....	953
\$junos-cos-overhead-accounting.....	1094
\$junos-cos-scheduler-excess-rate.....	952
dynamic CoS (traffic-control-profiles)	
\$junos-cos-guaranteed-rate.....	986
\$junos-cos-scheduler-map.....	1175
\$junos-cos-scheduler-shaping-rate.....	1186
\$junos-cos-shaping-rate.....	1186
configuring an access dynamic	
profile.....	697
vendor-id statement	
dynamic profile variables.....	1273
vendor-option statement.....	1274
vendor-specific attributes	
defining L2TP tunnels.....	242
supported.....	45
version statement	
dynamic IGMP	
interface.....	1275
dynamic MLD interface.....	1276
virtual-network statement	
Mobile IP.....	1277
VLAN See dynamic VLAN	
VLAN tagging.....	1282

vlan-id statement.....	1278
dynamic VLAN map	
rewriting at ingress or egress.....	1279
vlan-nas-port-stacked-format statement.....	1279
vlan-tag statement	
dynamic classifiers.....	1280
dynamic rewrite-rules.....	1281
vlan-tagging statement.....	1282
vlan-tags statement.....	1283
VSAs	
corresponding predefined variables.....	385
DSL Forum.....	50
supported.....	45

## W

walled garden	
example configuring as an HTTP service	
rule.....	620
example configuring as service filter.....	619
weighted load balancing	
configuring for L2TP LAC.....	245
weighted-load-balancing statement.....	1284
wimax statement	
Mobile IP.....	1284
wins-server statement.....	1285
wireless roaming	
Mobile IP.....	345



# Index of Statements and Commands

## A

aaa-logical-system statement		
domain maps.....	835	
aaa-routing-instance statement		
domain maps.....	836	
abatedUtilization statement		
address-assignment pools.....	836	
abatedUtilization-v6 statement		
address-assignment pools.....	837	
access profile		
session options.....	54	
access profile statements		
session-options.....	1185	
access statement		
dynamic profiles.....	837	
access-concentrator statement.....	838	
access-identifier statement		
ANCP.....	839	
access-internal statement		
dynamic profiles.....	839	
access-profile statement		
domain maps.....	840	
static subscribers.....	841	
access-type statement		
Mobile IP.....	842	
accounting statement		
access profile.....	843	
dynamic IGMP		
interface.....	843	
dynamic MLD interface.....	844	
accounting-port statement.....	844	
accounting-server statement.....	845	
accounting-session-id-format statement.....	845	
accounting-stop-on-access-deny statement.....	846	
accounting-stop-on-failure statement.....	846	
active-server-group statement.....	847	
address statement.....	849	
Diameter base protocol.....	848	
interface.....	848	
tunnels		
LAC.....	850	
LNS.....	849	
address-assignment pools		
abatedUtilization.....	836	
abatedUtilization-v6.....	837	
highUtilization.....	988	
highUtilization-v6.....	988	
router advertisement.....	1069	
address-assignment statement		
address-assignment pools.....	851	
address-pool statement		
domain maps.....	852	
adf statement		
dynamic firewalls.....	853	
adjacency-timer statement		
ANCP.....	854	
aggregate-clients statement		
DHCP local server.....	855	
DHCP relay agent.....	856	
static subscribers.....	857	
aggregated Ethernet		
targeted distribution of		
subscribers.....	1039, 1143, 1203	
algorithm statement		
Mobile IP.....	858	
allow-snooped-clients statement		
DHCP relay agent.....	859	
always-write-giaddr statement		
DHCP relay agent.....	860	
always-write-option-82 statement		
DHCP relay agent.....	861	
ancp statement		
ANCP.....	862	
ANCP statements		
access-identifier.....	839	
adjacency-timer.....	854	
ancp.....	862	

ietf-mode.....	995
interface-set.....	1030
interfaces.....	1025
maximum-discovery-table-entries.....	1053
maximum-helper-restart-time.....	1054
neighbor	
for all neighbors.....	1068
for unique access identifier.....	1068
pre-ietf-mode.....	1125
qos-adjust.....	1135
traceoptions.....	1215
application statement.....	863
attempts statement	
DHCP local server.....	864
attribute statement	
dynamic profile variables.....	865
attributes statement.....	866
authenticate statement	
Mobile IP.....	867
authentication statement	
DHCP local server.....	868
DHCP relay agent.....	869
static subscribers.....	870
authentication-order statement	
access.....	871
authentication-server statement.....	872
authorization-order statement	
JSRC.....	872
autonomous statement	
dynamic router advertisement.....	873

## B

boot-file statement.....	873
boot-server statement.....	874
buffer-size statement	
dynamic CoS.....	875

## C

captive-portal-content-delivery statements	
traceoptions.....	1217
circuit-id statement	
address-assignment pools.....	878
DHCP relay agent.....	879
circuit-type statement	
DHCP local server.....	880
DHCP relay agent.....	881
class-of-service statement	
subscriber access.....	882

classifiers statement	
dynamic CoS.....	882
clear-on-abort statement	
DHCP local server.....	883
client-accounting-algorithm statement	
RADIUS.....	884
client-authentication-algorithm statement	
RADIUS.....	884
client-discover-match statement	
DHCP local server.....	885
DHCP relay agent.....	886
client-id statement.....	887
client-idle-timeout statement	
access profile session options.....	888
client-session-timeout statement	
access profile session options.....	889
coa-immediate-update statement	
accounting.....	889
connect-actively statement	
Diameter base protocol.....	890
current-hop-limit statement	
dynamic router advertisement.....	890

## D

database-replication statement	
subscriber session database replication.....	891
default-lifetime statement	
dynamic router advertisement.....	891
default-local-server-group statement.....	892
default-relay-server-group statement.....	893
default-value statement	
dynamic profile variables.....	894
delay-buffer-rate statement	
dynamic CoS.....	894
delimiter statement	
DHCP local server.....	895
DHCP relay agent.....	896
domain maps.....	897
demux interfaces	
unit statement.....	1251
demux-options statement	
dynamic IP demux interface.....	899
demux-source statement	
dynamic IP demux interfaces.....	900
dynamic underlying interface.....	901
demux0 statement	
dynamic IP demux interface.....	898
demux0 statements	
underlying-interface.....	1249

destination statement		
Diameter base protocol.....	901	
dynamic PPPoE.....	902	
destination-address statement		
cpcd.....	902	
destination-host statement		
Gx-Plus.....	903	
JSRC.....	903	
PTSP.....	904	
destination-prefix-list statement		
captive-portal-content-delivery.....	904	
destination-realm statement		
Gx-Plus.....	905	
JSRC.....	905	
PTSP.....	906	
DHCP local server statements		
attempts.....	864	
boot-file.....	873	
boot-server.....	874	
circuit-type.....	880	
clear-on-abort.....	883	
client-discover-match.....	885	
client-id.....	887	
default-local-server-group.....	892	
delimiter.....	895	
dhcp-local-server.....	908	
dhcpv6.....	914	
dns-server.....	921	
domain-name.....	924	
duplicate-clients-on-interface.....	934	
dynamic-profile.....	937	
group.....	975	
interface.....	1005	
ip-address-first.....	1032	
logical-system-name.....	1041	
mac-address.....	1045	
no-arp.....	1074	
option-60.....	1081	
option-82.....	1084, 1085	
overrides.....	1095	
password.....	1105	
pool-match-order.....	1111	
relay-agent-interface-id.....	1147	
relay-agent-remote-id.....	1148	
relay-agent-subscriber-id.....	1149	
routing-instance-name.....	1167	
timeout.....	1207	
traceoptions.....	1219	
trigger.....	1243	
username-include.....	1267	
DHCP relay agent statements		
allow-snooped-clients.....	859	
circuit-id.....	879	
circuit-type.....	881	
client-discover-match.....	886	
default-relay-server-group.....	893	
delimiter.....	896	
disable-relay.....	920	
domain-name.....	925	
duplicate-clients-on-interface.....	934	
dynamic-profile.....	938	
group.....	977	
interface.....	1007	
interface-client-limit.....	1018	
layer2-unicast-replies.....	1036	
local-server-group.....	1038	
logical-system-name.....	1042	
mac-address.....	1046	
no-allow-snooped-clients.....	1073	
no-arp.....	1075	
option-60.....	1082	
overrides.....	1097	
password.....	1106	
proxy-mode.....	1134	
relay-option-60.....	1150	
relay-option-82.....	1151	
relay-server-group.....	1152	
replace-ip-source-with.....	1154	
routing-instance-name.....	1168	
send-release-on-delete.....	1179	
server-group.....	1180	
traceoptions.....	1221	
trust-option-82.....	1244	
use-interface-description.....	1261	
use-primary.....	1262, 1263	
user-prefix.....	1264, 1265	
username-include.....	1269	
vendor-option.....	1274	
dhcp-attributes statement		
address-assignment pools.....	907	
dhcp-local-server statement.....	908	
dhcp-relay statement.....	911	
dhcpv6 statement.....	914	
Diameter base protocol statements		
address.....	848	
connect-actively.....	890	
destination.....	901	

diameter.....	916	duplicate-clients-on-interface statement	
forwarding.....	969	DHCP local server.....	934
function		DHCP relay agent.....	934
network element.....	971	duplicate-protection statement	
route.....	972	dynamic PPPoE.....	935
host.....	993	dynamic CoS statements	
logical-system.....	1039	buffer-size.....	875
metric.....	1059	class-of-service.....	882
network-element.....	1071	delay-buffer-rate.....	894
origin.....	1091	drop-profile.....	929
peer.....	1109	drop-profile-map.....	930
port.....	1112	dscp	
priority.....	1125	dynamic classifiers.....	931
realm.....	1144	dynamic rewrite rules.....	932
route.....	1162	dscp-ipv6	
routing-instance.....	1164	dynamic classifiers.....	933
traceoptions.....	1223	dynamic rewrite rules.....	933
diameter statement		excess-priority.....	952
Diameter base protocol.....	916	excess-rate.....	952, 953
diameter-instance statement		forwarding-class.....	969
Gx-Plus.....	917	guaranteed-rate.....	986
JSRC.....	917	ieee-802.1	
PTSP.....	918	dynamic classifiers.....	994
disable statement		dynamic rewrite rules.....	995
dynamic IGMP.....	918	inet-precedence	
dynamic MLD.....	919	dynamic classifiers.....	1000
disable-relay statement.....	920	dynamic rewrite rules.....	1001
dns-server statement.....	921	interfaces.....	1026
domain statement		loss-priority.....	1044
domain maps.....	922	output-traffic-control-profile.....	1092
domain-name statement		overhead-accounting.....	1094
address-assignment pools.....	923	priority.....	1126
DHCP local server.....	924	protocol.....	1130
DHCP relay agent.....	925	scheduler.....	1174
static subscribers.....	926	scheduler-map.....	1175
drop statement		scheduler-maps.....	1176
DHCP relay agent.....	927	schedulers.....	1177
drop-profile statement		shaping-rate.....	1186
dynamic CoS.....	929	traffic-control-profiles.....	1240
drop-profile-map statement		transmit-rate.....	1241
dynamic CoS.....	930	unit.....	1255
dscp statement		vlan-tag	
dynamic classifiers.....	931	dynamic classifiers.....	1280
dynamic rewrite rules.....	932	dynamic rewrite rules.....	1281
dscp-ipv6 statement		dynamic firewalls statements	
dynamic classifiers.....	933	family.....	959
dynamic rewrite rules.....	933	fast-update-filter.....	964
		filter.....	965
		firewall.....	966



input.....	1003	immediate-leave.....	999
interface-specific.....	1031	no-accounting.....	844
match-order.....	1052	oif-map.....	1078
output.....	1092	passive.....	1104
post-service-filter.....	1113	source.....	1188
precedence.....	1119	source-count.....	1189
service.....	1181	source-increment.....	1190
service-filter.....	1182	ssm-map.....	1193
service-set.....	1184	static.....	1195
term.....	1204	version.....	1276
dynamic IGMP statements		dynamic MLD statements	
accounting.....	843	disable.....	919
disable.....	918	interface.....	1011
group		dynamic PPP statements	
with source.....	979	chap.....	878
without source.....	979	pap.....	1100
group-policy.....	985	ppp-options.....	1117
igmp.....	996	dynamic PPPoE statements	
immediate-leave.....	998	destination.....	902
interface.....	1009	duplicate-protection.....	935
no-accounting		dynamic-profile.....	939
interface.....	1072	family.....	961
oif-map		max-sessions.....	1056
interface.....	1078	pp0.....	1114
passive		pppoe-options.....	1115
interface.....	1103	pppoe-underlying-options.....	1116
promiscuous-mode		server.....	1179
interface.....	1130	underlying-interface.....	1250
source		unit.....	1253
interface.....	1188	unnumbered-address.....	1260
ssm-map		dynamic profiles statements	
interface.....	1193	access.....	837
static		attribute.....	865
interface.....	1194	default-value.....	894
version		dynamic-profiles.....	943
interface.....	1275	interface.....	1012
dynamic IP demux interface statements		dynamic routing options.....	1014
demux-source.....	900	interfaces.....	1027
family.....	960	keepalives.....	1034
dynamic IP demux statements		mandatory.....	1049
mac-validate.....	1048	metric.....	1059
dynamic MLD interface statements		mld.....	1061
accounting.....	844	multicast	
exclude.....	956	dynamic routing options.....	1064
group.....	980	next-hop.....	1072
group-count.....	982	no-keepalives.....	1077
group-increment.....	982	no-qos-adjust	
group-limit.....	984	dynamic routing options.....	1077
group-policy.....	985	predefined-variable-defaults.....	1120

preference.....	1120
protocols.....	1131
qualified-next-hop.....	1136
radius.....	1138
route	
access.....	1160
router-advertisement.....	1163
routing-instances.....	1170
tag	
access routes.....	1200
CoS dynamic service profile.....	1200
variables.....	1272
vendor-id.....	1273
vlan-tags.....	1283
dynamic router advertisement statements	
autonomous.....	873
current-hop-limit.....	890
default-lifetime.....	891
interface.....	1013
managed-configuration.....	1049
max-advertisement-interval.....	1053
min-advertisement-interval.....	1060
no-managed-configuration.....	1049
no-other-stateful-configuration.....	1091
on-link.....	1079
other-stateful-configuration.....	1091
preferred-lifetime.....	1121
prefix.....	1124
reachable-time.....	1143
retransmit-timer.....	1156
router-advertisement.....	1163
valid-lifetime.....	1271
dynamic underlying interface statements	
demux-source.....	901
dynamic-home-assignment statement	
Mobile IP.....	936
dynamic-profile statement	
DHCP local server.....	937
DHCP relay agent.....	938
domain maps.....	938
dynamic PPPoE.....	939
MLPPP.....	940
PPP.....	940
PPPoE service name tables.....	941
static subscribers.....	942
dynamic-profiles statement.....	943
<b>E</b>	
enable-service statement	
Mobile IP.....	947
encapsulation statement	
dynamic profiles.....	948
entity-type statement	
Mobile IP.....	951
ethernet-port-type-virtual statement.....	951
excess-priority statement	
dynamic CoS.....	952
excess-rate statement	
dynamic scheduling.....	952
dynamic traffic shaping.....	953
exclude statement.....	954
dynamic MLD interface.....	956
external-authority statement	
DHCP local server pool matching.....	956
<b>F</b>	
family statement	
address-assignment pools.....	958
dynamic firewalls.....	959
dynamic IP demux interface.....	960
dynamic profiles.....	962
fast-update-filter statement	
dynamic firewalls.....	964
filter statement	
dynamic firewalls.....	965
firewall statement	
dynamic profiles.....	966
forward-snooped-clients statement	
DHCP local server.....	967
DHCP relay agent.....	968
forwarding statement	
Diameter base protocol.....	969
forwarding-class statement	
dynamic CoS.....	969
subscriber secure policy.....	970
from statement	
captive-portal-content-delivery.....	970
function statement	
Diameter base protocol	
network element.....	971
route.....	972

**G**

gateway-name statement	
tunnels	
LAC.....	973
LNS.....	972
generic statement	
Mobile IP.....	973
global statement	
Gx-Plus.....	974
grace-period statement.....	974
group statement	
DHCP local server.....	975
DHCP relay agent.....	977
dynamic IGMP	
with source.....	979
without source.....	979
dynamic MLD interface.....	980
static subscribers.....	981
group-count statement	
dynamic MLD interface.....	982
group-increment statement	
dynamic MLD interface.....	982
group-limit statement	
dynamic IGMP.....	983
dynamic MLD interface.....	984
group-policy statement	
dynamic IGMP.....	985
dynamic MLD interface.....	985
guaranteed-rate statement	
dynamic CoS.....	986
gx-plus statement	
Gx-Plus.....	987
Gx-Plus statements	
destination-host.....	903
destination-realm.....	905
diameter-instance.....	917
global.....	974
gx-plus.....	987
max-outstanding-requests.....	1055
partition.....	1101
provisioning-order.....	1133

**H**

hardware-address statement.....	987
highUtilization statement	
address-assignment pools.....	988
highUtilization-v6 statement	
address-assignment pools.....	988

home-agent statement	
Mobile IP	
dynamic home assignment rule.....	989
IP address rule.....	990
networks.....	991
home-agent-address statement	
Mobile IP.....	992
host statement	
address-assignment pools.....	993
Diameter base protocol.....	993
<b>I</b>	
identification statement	
tunnels.....	994
idle timeout	
subscriber access.....	54
ieee-802.1 statement	
dynamic classifiers.....	994
dynamic rewrite rules.....	995
ietf-mode statement	
ANCP.....	995
igmp statement	
dynamic IGMP.....	996
ignore statement.....	997
immediate-leave statement	
dynamic IGMP.....	998
dynamic MLD interface.....	999
immediate-update statement	
accounting.....	1000
inet-precedence statement	
dynamic classifiers.....	1000
dynamic rewrite rules.....	1001
inner-tag-protocol-id statement	
dynamic VLAN interfaces.....	1001
inner-vlan-id statement	
dynamic VLAN interfaces.....	1002
input statement	
dynamic service sets.....	1003
input-vlan-map statement	
dynamic interfaces.....	1004
interface statement	
DHCP local server.....	1005
DHCP relay agent.....	1007
dynamic CoS.....	1010
dynamic IGMP.....	1009
dynamic MLD.....	1011
dynamic neighbor discovery.....	1013
dynamic profiles.....	1012

multicast	
dynamic routing options.....	1014
static subscriber group.....	1015
static subscribers username.....	1016
interface-client-limit statement	
DHCP local server.....	1017
DHCP relay agent.....	1018
interface-description-format statement.....	1019
interface-set statement	
ANCP.....	1030
dynamic CoS.....	1020
interface-specific statement	
dynamic firewalls.....	1031
interface-traceoptions statement	
DHCP local server.....	1021
DHCP relay agent.....	1023
interfaces statement	
ANCP.....	1025
dynamic CoS.....	1026
dynamic profiles.....	1027
subscriber secure policy.....	1024
IP demultiplexing interface statements	
unit.....	1251
ip-address statement.....	1031
ip-address-first statement.....	1032

## J

JSRC	
authorizing subscribers.....	281
jsrc statement	
JSRC.....	1033
JSRC statements	
authentication-order.....	872
destination-host.....	903
destination-realm.....	905
diameter-instance.....	917
jsrc.....	1033
jsrc-partition.....	1033
partition.....	1101
provisioning-order.....	1133
jsrc-partition statement	
JSRC.....	1033

## K

keepalives statement	
dynamic profiles.....	1034
key statement	
Mobile IP.....	1035

## L

L2TP statements	
traceoptions.....	1225
layer2-unicast-replies statement.....	1036
link statement	
address-assignment pools.....	1037
local-server-group statement.....	1038
logical interface statements	
family.....	962
logical-interface-fpc-redundancy statement	
aggregated Ethernet.....	1039
logical-system statement.....	1040
Diameter base protocol.....	1039
tunnels.....	1040
logical-system-name statement	
DHCP local server.....	1041
DHCP relay agent.....	1042
static subscribers.....	1043
loss-priority statement	
dynamic CoS.....	1044

## M

mac-address statement	
access internal routes.....	1047
DHCP local server.....	1045
DHCP relay agent.....	1046
mac-validate statement.....	1048
managed-configuration statement	
dynamic router advertisement.....	1049
mandatory statement	
dynamic profile variables.....	1049
map statement	
domain maps.....	1050
mask statement	
domain maps.....	1051
match-direction statement	
content-delivery-captive-portal.....	1051
match-order statement	
dynamic firewalls.....	1052
max-advertisement-interval statement	
dynamic router advertisement.....	1053
max-outstanding-requests statement	
Gx-Plus.....	1055
max-sessions statement	
dynamic PPPoE.....	1056
PPPoE service name tables.....	1057
tunnels.....	1058
maximum-discovery-table-entries statement	
ANCP.....	1053

maximum-helper-restart-time statement		
ANCP.....	1054	
maximum-lease-time statement.....	1054	
medium statement		
tunnels.....	1058	
metric statement		
Diameter base protocol.....	1059	
domain maps.....	1060	
dynamic profiles.....	1059	
min-advertisement-interval statement		
dynamic router advertisement.....	1060	
mld statement		
dynamic profiles.....	1061	
Mobile IP statements		
access-type.....	842	
algorithm.....	858	
authenticate.....	867	
dynamic-home-assignment.....	936	
enable-service.....	947	
entity-type.....	951	
generic.....	973	
home-agent		
dynamic home assignment rule.....	989	
IP address rule.....	990	
networks.....	991	
home-agent-address.....	992	
key.....	1035	
mobile-ip.....	1062	
nai.....	1065	
order.....	1090	
peer.....	1108	
registration-lifetime.....	1146	
replay-method.....	1155	
revocation-required.....	1158	
spi.....	1192	
statistics.....	1197	
timestamp-tolerance.....	1209	
traceoptions.....	1229	
virtual-network.....	1277	
wimax.....	1284	
mobile-ip statement		
Mobile IP.....	1062	
mode statement.....	1063	
multicast statement		
dynamic routing options.....	1064	
<b>N</b>		
nai statement		
Mobile IP.....	1065	
name-server statement.....	1066	
nas-identifier statement.....	1066	
nas-port-extended-format statement.....	1067	
neighbor statement		
ANCP		
for all neighbors.....	1068	
for unique access identifier.....	1068	
neighbor-discovery-router-advertisement		
statement		
address-assignment pools.....	1069	
netbios-node-type statement.....	1069	
network statement.....	1070	
network-element statement		
Diameter base protocol.....	1071	
next-hop statement		
dynamic profiles.....	1072	
no-accounting statement		
dynamic IGMP		
interface.....	1072	
dynamic MLD interface.....	844	
no-allow-snooped-clients statement		
DHCP relay agent.....	1073	
no-arp statement		
DHCP local server.....	1074	
DHCP relay agent.....	1075	
no-bind-on-request statement		
DHCP relay agent.....	1076	
no-keepalives statement		
dynamic profiles.....	1077	
no-managed-configuration statement		
dynamic router advertisement.....	1049	
no-other-stateful-configuration statement		
dynamic router advertisement.....	1091	
no-qos-adjust statement		
dynamic routing options.....	1077	
<b>O</b>		
oif-map statement		
dynamic IGMP		
interface.....	1078	
dynamic MLD interface.....	1078	
on-link statement		
dynamic router advertisement.....	1079	
option statement.....	1080	
option-60 statement		
DHCP local server.....	1081	
DHCP relay agent.....	1082	

option-82 statement	
address-assignment pools.....	1083
DHCP local server authentication.....	1084
DHCP local server pool matching.....	1085
DHCP relay agent.....	1086
option-match statement.....	1087
options statement	
RADIUS.....	1088
order statement	
accounting.....	1089
Mobile IP.....	1090
origin statement	
Diameter base protocol.....	1091
other-stateful-configuration statement	
dynamic router advertisement.....	1091
output statement	
dynamic service sets.....	1092
output-traffic-control-profile statement	
dynamic CoS.....	1092
output-vlan-map statement	
dynamic interfaces.....	1093
overhead-accounting statement	
dynamic CoS.....	1094
overrides statement	
DHCP local server.....	1095
DHCP relay agent.....	1097
<b>P</b>	
packet-triggered-subscribers statement.....	1098
packet-triggered-subscribers-partition	
statement.....	1099
padn statement	
domain maps.....	1099
parse-direction statement	
domain maps.....	1100
partition statement	
Gx-Plus.....	1101
JSRC.....	1101
PTSP.....	1102
passive statement	
dynamic IGMP	
interface.....	1103
dynamic MLD interface.....	1104
password statement	
DHCP local server.....	1105
DHCP relay agent.....	1106
static subscribers.....	1107
peer statement	
Diameter base protocol	
network element.....	1109
remote peer.....	1109
Mobile IP.....	1108
pool statement	
address-assignment pools.....	1110
pool-match-order statement.....	1111
pop statement	
dynamic VLAN interfaces.....	1111
port statement	
Diameter base protocol.....	1112
RADIUS servers.....	1112
post-service-filter statement	
dynamic service sets.....	1113
pp0 statement	
dynamic PPPoE.....	1114
ppp-subscriber-services statement	
dynamic profiles.....	1118
pppoe-options statement	
dynamic PPPoE.....	1115
pppoe-underlying-options statement	
static and dynamic PPPoE.....	1116
pre-ietf-mode statement	
ANCP.....	1125
precedence statement.....	1119
predefined-variable-defaults statement	
dynamic CoS.....	1120
preference statement	
dynamic profiles.....	1120
tunnels.....	1121
preferred-lifetime statement.....	1121
prefix statement	
address-assignment pools.....	1122
DHCP relay agent.....	1123
dynamic router advertisement.....	1124
priority statement	
Diameter base protocol.....	1125
dynamic CoS.....	1126
profile statement	
subscriber access.....	1127
promiscuous-mode statement	
dynamic IGMP	
interface.....	1130
protocol statement	
dynamic CoS.....	1130
protocols statement	
dynamic profiles.....	1131

provisioning-order statement	
subscriber services.....	1133
proxy-arp statement.....	1133
proxy-mode statement.....	1134
push statement	
dynamic VLAN interfaces.....	1135

## Q

qos-adjust statement	
ANCP.....	1135
qualified-next-hop statement	
dynamic profiles.....	1136

## R

radius statement	
dynamic profile variables.....	1138
subscriber access.....	1137
radius-disconnect statement	
DHCP local server.....	1139
radius-flow-tap statement.....	1140
radius-server statement.....	1141
range statement	
address-assignment pools.....	1142
reachable-time statement	
dynamic router advertisement.....	1143
realm statement	
Diameter base protocol.....	1144
rebalance-periodic statement	
aggregated Ethernet.....	1143
reconfigure statement	
DHCP local server.....	1145
registration-lifetime statement	
Mobile IP.....	1146
relay-agent-interface-id statement.....	1147
relay-agent-remote-id statement.....	1148
relay-agent-subscriber-id statement.....	1149
relay-option-60 statement.....	1150
relay-server-group statement.....	1152
remote-gateway statement	
tunnels.....	1153
remote-id statement.....	1153
replace-ip-source-with statement.....	1154
replay-method statement	
Mobile IP.....	1155
retransmit-timer statement	
dynamic router advertisement.....	1156
retry statement.....	1156
revert-interval statement.....	1157

revocation-required statement	
Mobile IP.....	1158
rewrite-rules statement	
dynamic CoS.....	1159
route statement	
access internal	
dynamic profiles.....	1161
Diameter base protocol.....	1162
dynamic profiles.....	1160
router statement	
address-assignment pools.....	1162
router-advertisement statement	
dynamic profiles.....	1163
routing-instance statement	
Diameter base protocol peer.....	1164
Diameter transport.....	1164
PPPoE service name tables.....	1166
RADIUS.....	1163
tunnels.....	1165
routing-instance-name statement	
DHCP local server.....	1167
DHCP relay agent.....	1168
static subscribers.....	1169
routing-instances statement	
dynamic profiles.....	1170
routing-options statement	
dynamic profiles.....	1171
rpf-check statement.....	1172
rule-set statement	
captive-portal-content-delivery.....	1174

## S

scheduler statement	
dynamic CoS.....	1174
scheduler-map statement	
dynamic CoS	
association with traffic-control	
profile.....	1175
scheduler-maps statement	
dynamic CoS	
scheduler map configuration.....	1176
schedulers statement	
dynamic CoS.....	1177
secret statement	
access.....	1178
tunnels.....	1178
send-release-on-delete statement	
DHCP relay agent.....	1179

server statement		
dynamic PPPoE.....	1179	
server-group statement.....	1180	
server-identifier statement		
address-assignment pools.....	1180	
service statement		
dynamic service sets.....	1181	
service-filter statement		
dynamic service sets.....	1182	
service-name-table statement		
PPPoE underlying interface.....	1183	
service-set statement		
dynamic service sets.....	1184	
services statement		
captive-portal-content-delivery.....	1185	
session options		
subscriber access.....	54	
session options statements		
client-idle-timeout.....	888	
client-session-timeout.....	889	
session timeout		
subscriber access.....	54	
session-options statement		
access profile.....	1185	
shaping-rate statement		
dynamic CoS.....	1186	
sip-server-address statement.....	1187	
sip-server-domain-name statement.....	1187	
source statement		
dynamic IGMP		
interface.....	1188	
dynamic MLD interface.....	1188	
source-address statement		
RADIUS.....	1189	
source-count statement		
dynamic MLD interface.....	1189	
source-gateway statement		
tunnels.....	1190	
source-increment statement		
dynamic MLD interface.....	1190	
source-ipv4-address statement.....	1191	
spi statement		
Mobile IP.....	1192	
ssm-map statement		
dynamic IGMP		
interface.....	1193	
dynamic MLD interface.....	1193	
static PPPoE statements		
pppoe-underlying-options.....	1116	
static statement		
dynamic IGMP		
interface.....	1194	
dynamic MLD interface.....	1195	
static subscriber group statements		
interface.....	1015	
static subscriber statements		
access-profile.....	841	
aggregate-clients.....	857	
authentication.....	870	
domain-name.....	926	
dynamic-profile.....	942	
group.....	981	
interface.....	1016	
logical-system-name.....	1043	
password.....	1107	
routing-instance.....	1169	
static-subscribers.....	1196	
traceoptions.....	1234	
user-prefix.....	1266	
username-include.....	1270	
static-subscribers statement.....	1196	
statistics statement		
access.....	1197	
strict statement		
DHCP local server.....	1198	
strip-domain statement		
domain maps.....	1198	
subscriber interface statements		
.....	1253	
access-concentrator.....	838	
address.....	848	
chap.....	878	
demux-options.....	899	
demux-source.....	900, 901	
demux0.....	898	
destination.....	902	
duplicate-protection.....	935	
dynamic-profile.....	939	
family.....	960, 961, 962	
interfaces.....	1027	
mac-validate.....	1048	
max-sessions.....	1056	
mode.....	1063	
pap.....	1100	
pp0.....	1114	
ppp-options.....	1117	
pppoe-options.....	1115	
pppoe-underlying-options.....	1116	



proxy-arp.....	1133	subscriber management.....	1236
rpf-check.....	1172	subscriber session database replication.....	1238
server.....	1179	traffic-control-profiles statement	
underlying-interface.....	1249, 1250	dynamic CoS.....	1240
unit.....	1251, 1257	transmit-rate statement	
unnumbered-address.....	1259, 1260	dynamic CoS.....	1241
vlan-tagging.....	1282	transport statement.....	1242
swap statement		trigger statement	
dynamic VLAN interfaces.....	1199	DHCP local server.....	1243
<b>T</b>		trust-option-82 statement.....	1244
tag statement		tunnel statement	
dynamic profile variables.....	1200	tunnels.....	1245
dynamic profiles access route.....	1200	tunnel-profile statement	
tag-protocol-id statement		domain maps.....	1246
dynamic VLAN map.....	1201	tunnels.....	1247
target-logical-system statement		type statement	
domain maps.....	1202	tunnels.....	1248
target-routing-instance statement		<b>U</b>	
domain maps.....	1203	underlying-interface statement	
targeted-distribution statement		dynamic PPPoE.....	1250
aggregated Ethernet.....	1203	dynamic profiles.....	1249
term statement		unit statement	
fast update filters.....	1204	demux interfaces.....	1251
tftp-server statement.....	1205	dynamic CoS.....	1255
then statement		dynamic PPPoE.....	1253
captive-portal-content-delivery.....	1206	interfaces.....	1257
timeout statement		unnumbered-address statement.....	1259
access.....	1208	dynamic PPPoE.....	1260
DHCP local server.....	1207	update-interval statement.....	1260
timestamp-tolerance statement		use-interface-description statement.....	1261
Mobile IP.....	1209	use-primary statement	
token statement		DHCP local server.....	1262
DHCP local server.....	1210	DHCP relay agent.....	1263
trace statement		user-prefix statement	
DHCP local server.....	1211	DHCP local server.....	1264
DHCP relay agent.....	1212	DHCP relay agent.....	1265
traceoptions statement		static subscribers.....	1266
address-assignment pools.....	1213	username-include statement	
ANCP.....	1215	DHCP local server.....	1267
captive-portal-content-delivery.....	1217	DHCP relay agent.....	1269
DHCP local server.....	1219	static subscribers.....	1270
DHCP relay agent.....	1221	<b>V</b>	
Diameter base protocol.....	1223	valid-lifetime statement.....	1271
general authentication service.....	1213	variables statement	
L2TP.....	1225	dynamic profile variables.....	1272
Mobile IP.....	1229	vendor-id statement	
PTSP.....	1232	dynamic profile variables.....	1273
static subscribers.....	1234		

vendor-option statement.....	1274
version statement	
dynamic IGMP	
interface.....	1275
dynamic MLD interface.....	1276
virtual-network statement	
Mobile IP.....	1277
vlan-id statement.....	1278
dynamic VLAN map	
rewriting at ingress or egress.....	1279
vlan-nas-port-stacked-format statement.....	1279
vlan-tag statement	
dynamic classifiers.....	1280
dynamic rewrite-rules.....	1281
vlan-tagging statement.....	1282
vlan-tags statement.....	1283

## W

wimax statement	
Mobile IP.....	1284
wins-server statement.....	1285