



**JUNOS[™]e Internet Software
for E-series[™] Routing Platforms**

**Broadband Access
Configuration Guide**

Release 8.2.x

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS 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 (including the ERX-310, ERX-705, ERX-710, ERX-1410, ERX-1440, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, and T320 routers, T640 routing node, and the JUNOS, JUNOSe, and SDX-300 software) 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.

Copyright © 2007, Juniper Networks, Inc.
All rights reserved. Printed in USA.

JUNOSe™ Internet Software for E-series™ Routing Platforms Broadband Access Configuration Guide, Release 8.2.x

Writing: Mark Barnard, Diane Florio, Bruce Gillham, Sarah Lesway-Ball, Brian Wesley Simmons, Fran Singer

Editing: Ben Mann

Illustration: Nathaniel Woodward

Cover Design: Edmonds Design

Revision History
27 July 2007—Revision 1

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

Software License

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

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 Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and 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, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller. "Embedded Software" means Software which Juniper has embedded in the Juniper 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 the 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 software on multiple computers requires multiple licenses, regardless of whether such computers 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 the Embedded Software on non-Juniper equipment; (j) use the 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 for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

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

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

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

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

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

Table of Contents

	About This Guide	xvii
	Objectives	xvii
	Audience	xvii
	E-series Routers	xviii
	Documentation Conventions.....	xviii
	Related E-series and JUNOSe Documentation	xx
	E-series and JUNOSe Documents.....	xx
	JUNOSe Configuration Guides.....	xxiii
	Obtaining Documentation.....	xxiii
	Documentation Feedback	xxiv
	Requesting Support.....	xxiv
Chapter 1	Configuring Remote Access	1
	Overview	2
	B-RAS Data Flow.....	2
	Configuring IP Addresses for Remote Clients.....	3
	AAA Overview	3
	Platform Considerations.....	3
	B-RAS Protocol Support	4
	References	4
	Before You Configure B-RAS	4
	Configuration Tasks	5
	Configuring a B-RAS License	6
	Mapping a User Domain Name to a Virtual Router.....	7
	Mapping User Requests Without a Valid Domain Name	7
	Mapping User Requests Without a Configured Domain Name	7
	Using DNS	8
	Redirected Authentication	8
	IP Hinting	9
	Setting Up Domain Name and Realm Name Usage	10
	Using the Realm Name as the Domain Name	11
	Using Delimiters Other Than @.....	11
	Using Either the Domain or the Realm as the Domain Name	11
	Specifying the Domain Name or Realm Name Parse Direction.....	12
	Stripping the Domain Name	12
	Domain Name and Realm Name Examples.....	14
	Specifying a Single Name for Users from a Domain	15
	Configuring RADIUS Authentication and Accounting Servers	16
	Server Access	17
	Server Request Processing Limit.....	17
	Authentication and Accounting Methods	17
	Supporting Exchange of Extensible Authentication Protocol Messages	18
	Immediate Accounting Updates.....	19

Duplicate and Broadcast Accounting	19
Configuring AAA Duplicate Accounting	20
Configuring AAA Broadcast Accounting	20
Overriding AAA Accounting NAS Information	20
UDP Checksums	21
Collecting Accounting Statistics	21
Configuring RADIUS AAA Servers	21
SNMP Traps and System Log Messages	33
SNMP Traps	33
System Log Messages	34
Configuring SNMP Traps	34
Configuring Local Authentication Servers	37
Creating the Local Authentication Environment	37
Creating Local User Databases	37
Adding User Entries to Local User Databases	38
Using the username Command	38
Using the aaa local username Command	39
Assigning a Local User Database to a Virtual Router	39
Enabling Local Authentication on the Virtual Router	40
Configuration Commands	40
Local Authentication Example	44
Configuring Name Server Addresses	47
Configuration Tasks	48
DNS Primary and Secondary NMS Configuration	48
WINS Primary and Secondary NMS Configuration	49
Configuring Local Address Servers	49
Local Address Pool Ranges	50
Local Address Pool Aliases	50
Shared Local Address Pools	51
SNMP Thresholds	52
Configuring a Local Address Server	52
Configuring DHCP Features	55
Creating an IP Interface	55
Single Clients per ATM Subinterface	55
Multiple Clients per ATM Subinterface	56
Configuring AAA Profiles	57
Allowing or Denying Domain Names	58
Configuration Example	58
Using Domain Name Aliases	59
Manually Setting NAS-Port-Type Attribute	63
Service-Description Attribute	64
Using RADIUS Route-Download Server to Distribute Routes	65
Format of Downloaded Routes	65
Framed-Route (RADIUS attribute 22)	65
Cisco-AVPair (Cisco VSA 26-1)	65
How the Route-Download Server Downloads Routes	66
Configuring the Route-Download Server to Download Routes	66
Using the AAA Logical Line Identifier to Track Subscribers	69
How the Router Obtains and Uses the LLID	70
RADIUS Attributes in Preauthentication Request	71
Considerations for Using the LLID	72
Configuring the Router to Obtain the LLID for a Subscriber	72
Troubleshooting Subscriber Preauthentication	75

Using VSAs for Dynamic IP Interfaces	75
Traffic Shaping for PPP over ATM Interfaces	76
Mapping Application Terminate Reasons to RADIUS Terminate Codes	77
Configuration Example	78
Configuring Timeout	80
Limiting Active Subscribers	81
Notifying RADIUS of AAA Failure	82
Configuring the SDX Client	82
Setting Baselines	87
Monitoring Remote Access	88

Chapter 2 Configuring RADIUS Attributes 123

Overview	123
RADIUS Services	124
RADIUS Attributes	124
Platform Considerations	125
References	125
Subscriber AAA Access Messages	125
Supported RADIUS IETF Attributes	126
Supported Juniper Networks VSAs	128
Subscriber AAA Accounting Messages	131
Supported RADIUS IETF Attributes	131
Supported Juniper Networks VSAs	134
Tunnel Accounting Messages	135
DSL Forum VSAs in AAA Access and Accounting Messages	136
CLI AAA Messages	137
CLI Commands Used to Modify RADIUS Attributes	138
RADIUS IETF Attributes	138
[4] NAS-IP-Address	138
[5] NAS-Port	139
[8] Framed-IP-Address	142
[9] Framed-Ip-Netmask	143
[13] Framed-Compression	143
[25] Class	144
[30] Called-Station-Id	144
[31] Calling-Station-Id	144
[32] NAS-Identifier	149
[41] Acct-Delay-Time	151
[44] Acct-Session-Id	152
[45] Acct-Authentic	153
[49] Acct-Terminate-Cause	153
[50] Acct-Multi-Session-Id	153
[51] Acct-Link-Count	154
[52] Acct-Input-Gigawords	154
[53] Output-Gigawords	154
[55] Event-Timestamp	155
[61] NAS-Port-Type	155
[64] Tunnel-Type	156
[65] Tunnel-Medium-Type	157
[66] Tunnel-Client-Endpoint	157
[67] Tunnel-Server-Endpoint	157
[68] Acct-Tunnel-Connection	158
[77] Connect-Info	158
[82] Tunnel-Assignment-Id	159

[83] Tunnel-Preference	160
[87] NAS-Port-Id	160
[90] Tunnel-Client-Auth-Id	161
[91] Tunnel-Server-Auth-Id	162
[188] Ascend-Num-In-Multilink	162
All Tunnel Server Attributes	162
Juniper Networks Vendor-Specific Attributes	163
[26-1] Virtual-Router	163
[26-10] Ingress-Policy-Name	163
[26-11] Egress-Policy-Name	164
[26-14] Service-Category	164
[26-15] PCR	165
[26-16] SCR	165
[26-17] MBS	165
[26-24] Pppoe-Description	166
[26-35] Acct-Input-Gigapackets	166
[26-36] Acct-Output-Gigapackets	166
[26-44] Tunnel-Interface-Id	167
[26-51] Disconnect-Cause	167
[26-53] Service-Description	167
[26-55] DHCP-Options	168
[26-56] DHCP-MAC-Address	168
[26-57] DHCP-GI-Address	168
[26-62] MLPPP-Bundle-Name	169
[26-63] Interface-Desc	169
[26-81] L2C-Information	170
[26-92] L2C-Up-Stream-Data	170
[26-93] L2C-Down-Stream-Data	170
DSL Forum Vendor-Specific Attributes	171
Including or Excluding Attributes in RADIUS Messages	172
Ignoring Attributes When Receiving Access-Accept Messages	172
Monitoring RADIUS Included and Ignored Attributes	173

Chapter 3 Configuring RADIUS Dynamic-Request Server 175

Overview	175
Platform Considerations	177
References	177
How RADIUS Dynamic-Request Server Works	177
RADIUS-Initiated Disconnect	177
Disconnect Messages	177
Message Exchange	178
Supported Error-Cause Codes (RADIUS Attribute 101)	178
Qualifications for Disconnect	178
Security/Authentication	179
Configuring RADIUS-Initiated Disconnect	179
RADIUS-Initiated Change of Authorization	179
Change-of-Authorization Messages	180
Message Exchange	180
Supported Error-Cause Codes (RADIUS Attribute 101)	180
Qualifications for Change of Authorization	181
Security/Authentication	181
Configuring RADIUS-Initiated Change of Authorization	181
RADIUS Dynamic-Request Server Commands	182
Monitoring RADIUS Dynamic-Request Servers	183

Chapter 4	Configuring RADIUS Relay Server	187
	Overview	187
	Platform Considerations.....	188
	References	188
	How RADIUS Relay Server Works	189
	Authentication and Addressing.....	189
	Accounting	190
	Terminating the Wireless Subscriber's Connection.....	190
	RADIUS Relay Server and the SDX Application	190
	Using the SDX Application for Addressing.....	191
	Using the SDX Application for Accounting.....	191
	Configuring RADIUS Relay Server Support	191
	Monitoring RADIUS Relay Server	193
Chapter 5	Configuring TACACS+	197
	Overview	197
	AAA Overview	198
	Administrative Login Authentication.....	198
	Privilege Authentication.....	199
	Login Authorization	199
	Accounting	199
	Platform Considerations.....	201
	References	202
	Before You Configure TACACS+	202
	Configuring TACACS+ Support.....	202
	Configuring Authentication.....	203
	Configuring Accounting	203
	Monitoring TACACS+	208
Chapter 6	Configuring L2TP	211
	Overview	212
	Terminology	213
	Implementing L2TP	213
	Sequence of Events on the LAC.....	214
	Sequence of Events on the LNS.....	214
	Packet Fragmentation.....	215
	Platform Considerations.....	216
	Module Requirements.....	216
	ERX-7xx Models, ERX-14xx Models, and the ERX-310 Router	216
	E120 Router and E320 Router.....	217
	Sessions and Tunnels Supported	217
	References	218
	Before You Configure the LAC or LNS	219
	Configuring the LAC	219
	Configuring Calling Number AVP Formats	220
	Configuration Tasks	222
	Example Scenarios.....	222
	Mapping a User Domain Name to an L2TP Tunnel	224
	Mapping from Domain Map Tunnel Mode.....	225
	Mapping from Tunnel Group Tunnel Mode.....	227
	Configuring the RX Speed on the LAC	234

Managing the L2TP Destination Lockout Process	235
Modifying the Lockout Procedure	235
Managing Address Changes Received from Remote Endpoints	238
Configuring the LNS	239
Configuring Maximum LNS Sessions	241
Configuring the RADIUS Connect-Info Attribute on the LNS	243
Selecting Tunnel-Service Modules for LNS Sessions Using MLPPP	244
Overriding All Endpoint Discriminators	245
Enabling Tunnel Switching	246
Enabling Tunnel Selection	247
Failover Between Preference Levels	247
Failover Within a Preference Level	248
Maximum Sessions per Tunnel	249
Weighted Load Balancing	249
Creating Persistent Tunnels	250
Testing Tunnel Configuration	250
Managing L2TP	250
Configuring Disconnect Cause Information	253
Configuring the Receive Window Size	255
Configuring the Default RWS	256
Configuring the RWS on the LAC	257
Configuring the RWS on the LNS	258
Configuring Peer Resynchronization	259
Using the CLI to Configure Peer Resynchronization	260
Using RADIUS to Configure Peer Resynchronization	262
Configuring L2TP Tunnel Switch Profiles	262
Applying the L2TP Tunnel Switch Profile	263
Configuration Guidelines	263
Configuring L2TP AVPs for Relay	264
Configuration Tasks	264
Enabling Tunnel Switching	265
Configuring L2TP Tunnel Switch Profiles	265
Applying L2TP Tunnel Switch Profiles by Using AAA	
Domain Maps	266
Applying L2TP Tunnel Switch Profiles by Using AAA	
Tunnel Groups	267
Applying L2TP Tunnel Switch Profiles by Using RADIUS	268
Applying Default L2TP Tunnel Switch Profiles	269
Configuring the Transmit Connect Speed Calculation Method	270
Calculation Methods	270
Static Layer 2	271
Dynamic Layer 2	271
QoS	271
Actual	272
Calculation Examples	272
Example 1: L2TP Session over ATM 1483 Interface	272
Example 2: L2TP Session over Ethernet VLAN Interface	273
Transmit Connect Speed Reporting Considerations	273
Session Termination for Dynamic Speed Timeout	273
Advisory Speed Precedence for VLANs over Bridged Ethernet	274
Using AAA Domain Maps to Configure the Transmit Connect Speed	
Calculation Method	274
Using AAA Tunnel Groups to Configure the Transmit Connect Speed	
Calculation Method	275

Using RADIUS to Configure the Transmit Connect Speed Calculation Method	276
Using AAA Default Tunnel Parameters to Configure the Transmit Connect Speed Calculation Method	277
PPP Accounting Statistics	279
Monitoring L2TP	280
Chapter 7 Configuring L2TP Dial-Out	295
Overview	295
Terms	296
Network Model for Dial-Out	296
Dial-Out Process	297
Dial-Out Operational States	298
Chassis	298
Virtual Router	298
Targets	298
Sessions	299
Outgoing Call Setup Details	300
Access-Request Message	300
Access-Accept Message	301
Outgoing Call	301
Mutual Authentication	302
Route Installation	302
Platform Considerations.....	302
References	302
Before You Configure L2TP Dial-Out	303
Configuring L2TP Dial-Out	303
Monitoring L2TP Dial-Out	305
Chapter 8 Configuring DHCP	313
Overview	314
Service Deployment System	314
Platform Considerations.....	314
References	315
Configuring the DHCP Access Model	316
Configuring DHCP Proxy Clients	316
Configuring DHCP Relay and BOOTP Relay	318
Trust-All Method	318
Assigning the Giaddr to Source IP Address	318
Protecting Against Spoofed Giaddr and Relay Agent Option Values	319
Using the Giaddr to Identify the Primary Interface for Dynamic Subscriber Interfaces.....	319
DHCP Relay Configuration and ARP Spoof Checking	319
Including Relay Agent Option Values in the PPPoE Remote Circuit ID	321
Configuring Layer 2 Unicast Transmission Method for Reply Packets to DHCP Clients	321
Using the Broadcast Flag Setting to Control Transmission of DHCP Reply Packets.....	322
Interaction with Layer 2 Unicast Transmission Method	323
DHCP Relay Proxy Behavior for Bound Clients and Address Renewals	324

Configuring Relay Agent Information Option (Option 82) Suboption Values	328
Format of the JUNOS Data Field in the Vendor-Specific Suboption for Option 82	330
Configuration Example—Using DHCP Relay Option 82 to Pass IEEE 802.1p Values to DHCP Servers.....	334
Configuring DHCP Relay Proxy	337
Managing Host Routes	337
Selecting the DHCP Server Response	338
Behavior for Bound Clients and Address Renewals	338
Configuring DHCP Local Server	339
DHCP Local Server Modes	340
DHCPv6 Local Server	340
Equal-Access Mode	341
Standalone Mode	343
Linking Local Address Pools	344
DHCP Local Server Event Logs.....	344
DHCP Local Server SNMP Traps	345
Before You Configure DHCP Local Server	345
Configuration Tasks.....	346
Configuring the DHCP Local Server	346
Configuring Grace Periods for Address Leases	353
Configuring AAA Authentication for DHCP Standalone Mode	355
Differentiating Between Clients with the Same Client ID or Hardware Address.....	358
Logging Out DHCP Local Server Subscribers.....	359
Clearing an IP DHCP Local Server Binding.....	359
Configuring the Router to Work with the SDX Application.....	360
Configuring the DHCPv6 Local Server.....	361
Configuring DHCP External Server Application	363
Interoperating with Ethernet DSLAMs.....	365
Configuring DHCP External Server Support	365
Using Option 60 Strings to Forward Client Traffic to Specific DHCP Servers	367
Configuration Example—Using DHCP Relay Option 60 to Specify Traffic Forwarding	369
Configuring Cable Modem DHCP Relay	370
Viewing and Deleting DHCP Client Bindings	370
Logging DHCP Packet Information	371
Monitoring DHCP.....	372
Chapter 9	399
Configuring Subscriber Management	399
Overview	399
Platform Considerations.....	400
Subscriber Management Attributes	400
Dynamic IP Subscriber Interfaces.....	401
Subscriber Management Procedure.....	401
Configuring Subscriber Management with an External DHCP Server	403
Subscriber Management Commands.....	404
Configuration Examples.....	411
Username with ATM Circuit Identifier and No Circuit Type	412
Username with VLAN Circuit Identifier and Circuit Type	412
Username with MAC Address.....	413
Monitoring Subscriber Management	413

Chapter 10	Configuring Subscriber Interfaces	417
Overview	417	
Relationship to Shared IP Interfaces	418	
Relationship to Primary IP Interfaces	418	
Ethernet Interfaces and VLANs	419	
Moving Interfaces	419	
Preventing IP Spoofing	420	
Routing Protocols	420	
Policies and QoS	420	
Applications	420	
Directing Traffic Toward Special Local Content	420	
Differentiating Traffic for VPNs	421	
Platform Considerations	422	
Interface Specifiers	423	
References	423	
Dynamic Creation of Subscriber Interfaces	424	
DHCP Servers	424	
DHCP Local Server and Address Allocation	424	
DHCP External Server and Address Allocation	424	
DHCP Relay Configuration	425	
Supported Configurations	425	
Packet Detection	426	
Designating Traffic for the Primary IP Interface	426	
Using Framed Routes	426	
Configuring Static Subscriber Interfaces	427	
Using a Destination Address to Demultiplex Traffic	427	
Using a Source Address to Demultiplex Traffic	429	
Configuring Dynamic Subscriber Interfaces	433	
Configuring Dynamic Subscriber Interfaces over Ethernet	433	
Configuring Dynamic Subscriber Interfaces over VLANs	434	
Configuring Dynamic Subscriber Interfaces over Bridged Ethernet	436	
Configuring Dynamic Subscriber Interfaces over GRE Tunnels	437	
Dynamic Subscriber Interface Configuration Example	438	
Monitoring Subscriber Interfaces	445	
Chapter 11	Configuring Service Manager	449
Overview	450	
Service Manager Terms and Acronyms	450	
Platform Considerations	451	
References	451	
Configuration Tasks	452	
Service Definitions	453	
Creating Service Definitions	454	
Managing Your Service Definitions	456	
Referencing Policies in Service Definitions	457	
Referencing QoS Configurations in Service Definitions	458	
Specifying QoS Profiles in a Service Definition	458	
Configuring a QoS Profile for Service Manager	458	
Specifying QoS Profiles in a Service Definition	459	
Specifying QoS Parameter Instances in a Service Definition	459	
Creating a Parameter Instance in a Profile	460	
Specifying QoS Parameter Instances in a Service Definition	460	

Modifying QoS Configurations with Service Manager	461
Modifying Parameter Instances	461
Modifying QoS Configurations in a Single Service Manager Event	463
Modifying QoS Configurations Using Other Sources	463
Removing QoS Configurations Referenced by Service Manager	464
QoS for Service Manager Considerations	465
RADIUS or Service Manager	465
Interoperability with Other Service Components	465
QoS Statistics	465
Ranges	466
Configuring the Service Manager License	466
Managing and Activating Service Sessions	466
Using RADIUS to Manage Subscriber Service Sessions	467
Using RADIUS to Activate Subscriber Service Sessions	468
Service Manager RADIUS Attributes	469
Using Tags with RADIUS Attributes	471
Using RADIUS to Deactivate Service Sessions	471
Setting Thresholds	472
Using the Deactivate-Service Attribute	472
Using Mutex Groups to Activate and Deactivate Subscriber Services	473
Activating and Deactivating Multiple Services	473
Configuring a Mutex Service	474
Configuring RADIUS Accounting for Service Manager	475
Using the CLI to Manage Subscriber Service Sessions	477
Using the CLI to Activate Subscriber Service Sessions	477
Preprovisioning Services	480
Using Service Session Profiles	480
Using the CLI to Deactivate Subscriber Service Sessions	483
Gracefully Deactivating Subscriber Service Sessions	483
Forcing Immediate Deactivation of Subscriber Service Sessions	484
Using Service Session Profiles to Deactivate Service Sessions	485
Configuring Service Manager Statistics	485
Setting Up the Service Definition File for Statistics Collection	486
Enabling Statistics Collection with RADIUS	487
Enabling Statistics Collection with the CLI	487
Service Manager Performance Considerations	488
Service Definition Examples	489
Tiered Service Example	489
Video-on-Demand Service Definition Example	490
Voice-over-IP Service Definition Example	491
Guided Entrance Service Example	492
Guided Entrance Service Definition Example	493
Using CoA Messages with Guided Entrance Services	494
Configuring the HTTP Local Server to Support Guided Entrance	495
Monitoring the HTTP Local Server	498
Monitoring Service Manager	500

Appendix A RADIUS Attribute Descriptions 511

RADIUS IETF Attributes	512
Juniper Networks VSAs	517
DSL Forum VSAs	523
Pass Through RADIUS Attributes	524
References	525

Appendix B	L2TP Disconnect Cause Codes	527
Appendix C	Application Terminate Reasons	531
	AAA Terminate Reasons	531
	L2TP Terminate Reasons	532
	PPP Terminate Reasons	542
	RADIUS Client Terminate Reasons	547
	Index	549

About This Guide

This preface provides the following guidelines for using *JUNOS[™] Internet Software for E-series[™] Routing Platforms Broadband Access Configuration Guide*:

- [Objectives](#) on page xvii
- [Audience](#) on page xvii
- [E-series Routers](#) on page xviii
- [Documentation Conventions](#) on page xviii
- [Related E-series and JUNOS[™] Documentation](#) on page xx
- [Obtaining Documentation](#) on page xxiii
- [Documentation Feedback](#) on page xxiv
- [Requesting Support](#) on page xxiv

Objectives

This guide provides the information you will need to configure routing and remote access on your E-series router.

An E-series router is shipped with the latest system software installed. If you need to install a future release or reinstall the system software, refer to the procedures in *JUNOS[™] System Basics Configuration Guide, Chapter 3, Installing JUNOS[™] Software*.



NOTE: If the information in the latest *JUNOS[™] Release Notes* differs from the information in this guide, follow the *JUNOS[™] Release Notes*.

Audience

This guide is intended for experienced system and network specialists working with E-series routers in an Internet access environment.

E-series Routers

Seven models of E-series routers are available:

- E120 router
- E320 router
- ERX-1440 router
- ERX-1410 router
- ERX-710 router
- ERX-705 router
- ERX-310 router

All models use the same software. For information about all models except the E120 router and the E320 router, see *ERX Hardware Guide, Chapter 1, ERX Overview*. For information about the E120 router and the E320 router, see *E120 and E320 Hardware Guide, Chapter 1, E120 and E320 Overview*.

In the E-series documentation, the term ERX-14xx models refers to both the ERX-1440 router and the ERX-1410 router. Similarly, the term ERX-7xx models refers to both the ERX-710 router and the ERX-705 router. The terms ERX-1440 router, ERX-1410 router, ERX-710 router, ERX-705 router, ERX-310 router, E120 router, and E320 router refer to the specific models.

Documentation Conventions

[Table 1](#) 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.

Table 2 defines text conventions used in this guide and the syntax conventions used primarily in the *JUNOS Command Reference Guide*. For more information about command syntax, see *JUNOS System Basics Configuration Guide, Chapter 2, Command-Line Interface*.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Text Conventions		
Bold typeface	Represents commands and keywords in text.	<ul style="list-style-type: none"> ■ Issue the clock source command. ■ Specify the keyword exp-msg.
Bold sans serif typeface	Represents text that the user must type.	host1(config)# traffic class low-loss1
Fixed-width font	Represents information as displayed on your terminal's screen.	<pre>host1#show ip ospf 2 Routing Process OSPF 2 with Router ID 5.5.0.250 Router is an Area Border Router (ABR)</pre>
<i>Italic typeface</i>	<ul style="list-style-type: none"> ■ Emphasizes words. ■ Identifies variables. ■ Identifies chapter, appendix, and book names. 	<ul style="list-style-type: none"> ■ There are two levels of access, <i>user</i> and <i>privileged</i>. ■ <i>clusterId</i>, <i>ipAddress</i>. ■ <i>Appendix A, System Specifications</i>.
Plus sign (+) linking key names	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Syntax Conventions in the Command Reference Guide		
Plain typeface	Represents keywords.	terminal length
<i>Italic typeface</i>	Represents variables.	<i>mask</i> , <i>accessListName</i>
(pipe symbol)	Represents a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable can be either optional or required.)	diagnostic line
[] (brackets)	Represent optional keywords or variables.	[internal external]
[]* (brackets and asterisk)	Represent optional keywords or variables that can be entered more than once.	[level1 level2 11]*
{ } (braces)	Represent required keywords or variables.	{ permit deny } { in out } { <i>clusterId</i> <i>ipAddress</i> }

Related E-series and JUNOS Documentation

The E-series and JUNOS documentation set consists of several hardware and software guides, which are available in electronic and printed formats.

E-series and JUNOS Documents

[Table 3](#) lists and describes the E-series and JUNOS document set. For a complete list of abbreviations used in this document set, along with their spelled-out terms, see [JUNOS System Basics Configuration Guide, Appendix A, Abbreviations and Acronyms](#).

Table 3: Juniper Networks E-series and JUNOS Technical Publications

Document	Description
E-series Hardware Documentation	
<i>E120 and E320 Quick Start Guide</i>	Shipped in the box with all new E120 and E320 routers. Provides the basic procedures to help you get the routers up and running quickly.
<i>E120 and E320 Hardware Guide</i>	<p>Provides the necessary procedures for getting E120 routers and E320 routers operational, including information about:</p> <ul style="list-style-type: none"> ■ Installing the chassis and modules ■ Connecting cables ■ Powering up the routers ■ Configuring the routers for management access ■ Troubleshooting common issues <p>Describes switch route processor (SRP) modules, line modules, and I/O adapters (IOAs) available for E120 and E320 routers.</p>
<i>E120 and E320 Module Guide</i>	<p>Provides detailed specifications for line modules and IOAs in E120 and E320 routers, and information about the compatibility of these modules with JUNOS software releases.</p> <p>Lists the layer 2 protocols, layer 3 protocols, and applications that line modules and their corresponding IOAs support.</p> <p>Provides module LED information.</p>
<i>E-series Installation Quick Start poster or ERX Quick Start Guide</i>	Shipped in the box with all new ERX routers. Provides the basic procedures to help you get an ERX router up and running quickly.
<i>ERX Hardware Guide</i>	<p>Provides the necessary procedures for getting ERX-14xx models, ERX-7xx models, and ERX-310 routers operational, including information about:</p> <ul style="list-style-type: none"> ■ Installing the chassis and modules ■ Connecting cables ■ Powering up the routers ■ Configuring the routers for management access ■ Troubleshooting common issues <p>Describes switch route processor (SRP) modules, line modules, and I/O modules available for the ERX routers.</p>
<i>ERX Module Guide</i>	<p>Provides detailed specifications for line modules and I/O modules in ERX-14xx models, ERX-7xx models, and ERX-310 routers, and information about the compatibility of these modules with JUNOS software releases.</p> <p>Lists the layer 2 protocols, layer 3 protocols, and applications that line modules and their corresponding I/O modules support.</p> <p>Provides module LED information.</p>

Table 3: Juniper Networks E-series and JUNOS® Technical Publications (continued)

Document	Description
<i>ERX End-of-Life Module Guide</i>	Provides an overview and description of ERX modules that are end-of-life (EOL) and can no longer be ordered for the following routers: <ul style="list-style-type: none"> ■ ERX-7xx models ■ ERX-14xx models ■ ERX-310 router
JUNOS® Software Guides	
<i>JUNOS® System Basics Configuration Guide</i>	Provides information about: <ul style="list-style-type: none"> ■ Planning and configuring your network ■ Using the command-line interface (CLI) ■ Installing JUNOS® software ■ Configuring the Simple Network Management Protocol (SNMP) ■ Managing the router and its modules, including the use of high availability (HA) for SRP redundancy ■ Configuring passwords and security ■ Configuring the router clock ■ Configuring virtual routers
<i>JUNOS® Physical Layer Configuration Guide</i>	Explains how to configure, test, and monitor physical layer interfaces.
<i>JUNOS® Link Layer Configuration Guide</i>	Explains how to configure and monitor static and dynamic link layer interfaces.
<i>JUNOS® IP, IPv6, and IGP Configuration Guide</i>	Explains how to configure and monitor IP, IPv6 and Neighbor Discovery, and interior gateway protocols (RIP, OSPF, and IS-IS).
<i>JUNOS® IP Services Configuration Guide</i>	Explains how to configure and monitor IP routing services. Topics include: <ul style="list-style-type: none"> ■ Routing policies ■ Firewalls ■ Network Address Translation (NAT) ■ J-Flow statistics ■ Bidirectional forwarding detection (BFD) ■ Internet Protocol Security (IPSec) ■ Layer 2 Control (L2C) ■ Digital certificates ■ IP tunnels ■ Layer 2 services over GRE and over MPLS ■ Virtual Router Redundancy Protocol (VRRP)
<i>JUNOS® Multicast Routing Configuration Guide</i>	Explains how to configure and monitor IP multicast routing and IPv6 multicast routing. Topics include: <ul style="list-style-type: none"> ■ Internet Group Management Protocol (IGMP) ■ Protocol Independent Multicast (PIM) ■ Distance Vector Multicast Routing Protocol (DVMRP) ■ Multicast Listener Discovery (MLD)
<i>JUNOS® BGP and MPLS Configuration Guide</i>	Explains how to configure and monitor Border Gateway Protocol (BGP) routing, Multiprotocol Label Switching (MPLS), and related applications, and configure and monitor the virtual private LAN service (VPLS) and layer 2 virtual private networks (L2VPNs).

Table 3: Juniper Networks E-series and JUNOS Technical Publications (continued)

Document	Description
<i>JUNOS Policy Management Configuration Guide</i>	Explains how to configure, manage, and monitor customized policy rules for packet classification, forwarding, filtering, and flow rates. Also describes the packet mirroring feature, which uses secure policies.
<i>JUNOS Quality of Service Configuration Guide</i>	Explains how to configure quality of service (QoS) features to queue, schedule, and monitor traffic flow. These features include: <ul style="list-style-type: none"> ■ Traffic classes and traffic-class groups ■ Drop, queue, QoS, and scheduler profiles ■ QoS parameters ■ Statistics
<i>JUNOS Broadband Access Configuration Guide</i>	Explains how to configure and monitor a remote access environment, which can include the following features: <ul style="list-style-type: none"> ■ Authentication, authorization, and accounting (AAA) ■ Dynamic Host Configuration Protocol (DHCP) ■ Remote Authentication Dial-In User Service (RADIUS) ■ Terminal Access Controller Access Control System (TACACS +) ■ Layer 2 Tunneling Protocol (L2TP) ■ Subscriber management
<i>JUNOS System Event Logging Reference Guide</i>	Describes the JUNOS system logging feature and describes how to use the CLI to monitor your system's log configuration and system events.
<i>JUNOS Command Reference Guide A to M; JUNOS Command Reference Guide N to Z</i>	Together constitute the <i>JUNOS Command Reference Guide</i> . Contain important information about commands implemented in the system software. Use to look up: <ul style="list-style-type: none"> ■ Descriptions of commands and command parameters ■ Command syntax ■ A command's related mode ■ Starting with JUNOS Release 7.1.0, a history of when a command, its keywords, and its variables were introduced or added Use with the JUNOS configuration guides.
<i>JUNOS Comprehensive Index</i>	Provides a complete index of the JUNOS software documentation set.
Release Notes	
<i>JUNOS Release Notes</i>	Provide the latest information about features, changes, known problems, resolved problems, and system maximum values. If the information in the <i>Release Notes</i> differs from the information found in the documentation set, follow the <i>Release Notes</i> . Release notes are included on the corresponding software CD and are available on the Web.

JUNOS^e Configuration Guides

JUNOS^e software configuration guides use a bottom-up approach to describe the relationship of layers, protocols, and interfaces in the configuration process. For more information, see *Layered Approach* in [JUNOS^e System Basics Configuration Guide, Chapter 1, Planning Your Network](#).

The chapters in JUNOS^e software configuration guides typically include the following topics:

- Conceptual and overview information
- Information you need to know or tasks you need to perform before you begin
- Platform-specific issues you need to take into consideration
- Applicable references, such as RFCs and IETF draft documents, about the protocols and features supported by the router
- Required and optional tasks, as step-by-step procedures
- Descriptions and examples of the commands you use
- Illustrations of network topologies
- Examples of command sequences for configuration, testing, and monitoring activities
- Sample displays that result when you issue the **show** command

Obtaining Documentation

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

To order printed copies of this manual and other Juniper Networks technical documents or to order a documentation CD, which contains this manual, contact your sales representative.

Copies of the Management Information Bases (MIBs) available in a software release are included on the software CDs and at <http://www.juniper.net/>.

Documentation Feedback

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

- Document name
- Document part number
- Page number
- Software release version

Requesting Support

For technical support, open a support case using the Case Manager link at <http://www.juniper.net/support/> or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

Chapter 1

Configuring Remote Access

This chapter describes how to configure remote access to an E-series router. This chapter discusses the following topics:

- [Overview](#) on page 2
- [Platform Considerations](#) on page 3
- [References](#) on page 4
- [Before You Configure B-RAS](#) on page 4
- [Configuration Tasks](#) on page 5
- [Configuring a B-RAS License](#) on page 6
- [Mapping a User Domain Name to a Virtual Router](#) on page 7
- [Setting Up Domain Name and Realm Name Usage](#) on page 10
- [Specifying a Single Name for Users from a Domain](#) on page 15
- [Configuring RADIUS Authentication and Accounting Servers](#) on page 16
- [Configuring Local Authentication Servers](#) on page 37
- [Configuring Name Server Addresses](#) on page 47
- [Configuring Local Address Servers](#) on page 49
- [Configuring DHCP Features](#) on page 55
- [Creating an IP Interface](#) on page 55
- [Configuring AAA Profiles](#) on page 57
- [Using RADIUS Route-Download Server to Distribute Routes](#) on page 65
- [Using the AAA Logical Line Identifier to Track Subscribers](#) on page 69
- [Using VSAs for Dynamic IP Interfaces](#) on page 75

- [Mapping Application Terminate Reasons to RADIUS Terminate Codes](#) on page 77
- [Configuring Timeout](#) on page 80
- [Limiting Active Subscribers](#) on page 81
- [Notifying RADIUS of AAA Failure](#) on page 82
- [Configuring the SDX Client](#) on page 82
- [Setting Baselines](#) on page 87
- [Monitoring Remote Access](#) on page 88

Overview

Broadband Remote Access Server (B-RAS) is an application running on your router that:

- Aggregates the output from digital subscriber line access multiplexers (DSLAMs)
- Provides user Point-to-Point Protocol (PPP) sessions or IP-over-Asynchronous Transfer Mode (ATM) sessions
- Enforces quality of service (QoS) policies
- Routes traffic into an Internet service provider's (ISP's) backbone network

A DSLAM collects data traffic from multiple subscribers into a centralized point so that it can be uploaded to the router over an ATM connection via a DS3, OC3, E3, or OC12 link.

The router provides the logical termination for PPP sessions, as well as the interface to authentication and accounting systems.

B-RAS Data Flow

The router performs several tasks for a digital subscriber line (DSL) PPP user to establish a PPP connection. This is an example of the way B-RAS data might flow:

1. Authenticate the subscriber using RADIUS authentication.
2. Assign an IP address to the PPP/IP session via RADIUS, local address pools, or Dynamic Host Configuration Protocol (DHCP).
3. Terminate the PPP encapsulation or tunnel a PPP session.
4. Provide user accounting via RADIUS.



NOTE: For information about configuring RADIUS attributes see [Chapter 2, Configuring RADIUS Attributes](#).

Configuring IP Addresses for Remote Clients

A remote client can obtain an IP address from one of the following:

- RADIUS server
- Local address server
- DHCP proxy client and server
- DHCP relay agent (Bridged IP only)
- DHCP local server
- DHCP external server

For information about configuring DHCP support on the E-series router, see [Chapter 8, Configuring DHCP](#).

For information about how to configure a RADIUS server, see your RADIUS server documentation.

AAA Overview

Collectively, authentication, authorization, and accounting are referred to as AAA. Each has an important but separate function.

- Authentication—Determines who the user is, then determines whether that user should be granted access to the network. The primary purpose is to prevent intruders from networks. It uses a database of users and passwords.
- Authorization—Determines what the user is allowed to do by giving network managers the ability to limit network services to different users.
- Accounting—Tracks what the user did and when they did it. You can use accounting for an audit trail or for billing for connection time or resources used.

Central management of AAA means the information is in a single, centralized, secure database, which is much easier to administer than information distributed across numerous devices.

Platform Considerations

B-RAS services are supported on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

B-RAS Protocol Support

The E-series router supports the following protocols for B-RAS services:

- PPP
- PPP over Ethernet (PPPoE)
- Bridged Ethernet
- Layer 2 Tunneling Protocol (L2TP), both L2TP access concentrator (LAC) and L2TP network server (LNS)

References

For more information about the topics covered in this chapter, see the following documents:

[RFC 2748—The COPS \(Common Open Policy Service\) Protocol \(January 2000\)](#)

[RFC 2865—Remote Authentication Dial In User Service \(RADIUS\) \(June 2000\)](#)

[RFC 3084—COPS Usage for Policy Provisioning \(COPS-PR\) \(March 2001\)](#)

[RFC 3159—Structure of Policy Provisioning Information \(SPPI\) \(August 2001\)](#)

[RFC 3198—Terminology for Policy-Based Management \(November 2001\)](#)

[RFC 3318—Framework Policy Information Base \(March 2003\)](#)

JUNOS Release Notes, Appendix A, System Maximums—Refer to the Release Notes corresponding to your software release for information about the number of concurrent RADIUS requests that the router supports for authentication and accounting servers.

Before You Configure B-RAS

Before you begin to configure B-RAS, you need to collect the following information for the RADIUS authentication and accounting servers:

- IP addresses
- User Datagram Protocol (UDP) port numbers
- Secret keys

Configuration Tasks

Each configuration task is presented in a separate section in this chapter. Most of the B-RAS configuration tasks are optional.

To configure B-RAS, perform the following tasks:

1. Configure a B-RAS license.
2. (Optional) Map a user domain name to a virtual router. By default, all requests go through a default router.
3. (Optional) Set up domain name and realm name usage.
4. (Optional) Specify a single name for users from a domain.
5. Configure an authentication server on the router.
6. (Optional) Configure UDP checksums.
7. (Optional) Configure an accounting server on the router.
8. (Optional) Configure Domain Name System (DNS) and Windows Internet Name Service (WINS) name server addresses.
9. (Optional) Configure a local address pool for remote clients.
10. (Optional) Configure one or more DHCP servers.
11. Create a PPP interface on which the router can dynamically create an IP interface.
12. (Optional) Configure AAA profiles.
13. (Optional) Use vendor-specific attributes (VSAs) for Dynamic Interfaces.
14. (Optional) Set idle or session timeout.
15. (Optional) Limit the number of active subscribers on a virtual router (VR) or port.
16. (Optional) Set up the router to notify RADIUS when a user fails AAA.
17. (Optional) Configure a RADIUS download server on the router.
18. (Optional) Configure the Service Deployment System (SDX) client.
19. (Optional) Set baselines for AAA statistics or RADIUS authentication and accounting statistics.

Configuring a B-RAS License

From Global Configuration mode, configure a B-RAS license:

```
host1(config)#license b-ras k3n91s6gtj
```

B-RAS licenses are available in various sizes to enable subscriber access for up to one of the following maximum number of simultaneous active IP, LAC, and bridged Ethernet interfaces:

- 4000
- 8000
- 16,000
- 32,000
- 48,000



NOTE: To use a B-RAS license for 16,000 or more interfaces, each of your SRP modules must have 1 gigabyte (GB) of memory.

license b-ras

- Use to specify the B-RAS license.
- The license is a unique string of up to 15 alphanumeric characters.



NOTE: Acquire the license from Juniper Networks Customer Service or your Juniper Networks sales representative.

- You can purchase licenses that allow up to 2,000, 4,000, 8,000, 16,000, 32,000, or 48,000 simultaneous active IP, LAC, and bridged Ethernet interfaces.
- Example

```
host1(config)#license b-ras jwmR4k8D
```
- Use the **no** version to disable the license.

Mapping a User Domain Name to a Virtual Router

You can configure RADIUS authentication, accounting, and local address pools for a specific virtual router and then map a user domain to that virtual router.

The router keeps track of the mapping between domain names and virtual-routers. Use the **aaa domain-map** command to map a user domain to a virtual router.



NOTE: This domain name is not the NT domain sometimes found on the Dialup Networking dialog box.

When the router is configured to require authentication of a PPP user, the router checks for the appropriate user domain-name-to-virtual-router mapping. If it finds a match, the router sends a RADIUS authentication request to the RADIUS server configured for the specific virtual router.

Mapping User Requests Without a Valid Domain Name

You can create a mapping between a domain name called **default** and a specific virtual router so that the router can map user names that contain a domain name that does not have an explicit map.

If a user request is submitted with a domain name for which the router cannot find a match, the router looks for a mapping between the domain name **default** and a virtual router. If a match is found, the user's request is processed according to the RADIUS server configured for the named virtual router. If no entry is found that maps **default** to a specific virtual router, the router sends the request to the RADIUS server configured on the default virtual router.

Mapping User Requests Without a Configured Domain Name

You can map a domain name called **none** to a specific virtual router so that the router can map user names that do not contain a domain name.

If a user request is submitted without a domain name, the router looks for a mapping between the domain name **none** and a virtual router. If a match is found, the user's request is processed according to the RADIUS server configured for the named virtual router. If the router does not find the domain name **none**, it checks for the domain name **default**. If no matching entries are found, the router sends the request to the server configured on the default virtual router.

Using DNIS

The E-series router supports dialed number identification service (DNIS). With DNIS, if users have a called number associated with them, the router searches the domain map for the called number. If it finds a match, the router uses the matching domain map entry information to authenticate the user. If the router does not find a match, it searches the domain map using normal processing.



NOTE: For DNIS to work, the router must be acting as the LNS. Also, the phone number configured in the **aaa domain-map** command must be an exact match to the value passed by L2TP in the called number AVP (AVP 21).

For example, as specified in the following sequence, a user calling 9785551212 would be terminated in vrouter_88, while a user calling 8005554433 is terminated in vrouter_100.

```
host1(config)#aaa domain-map 9785551212 vrouter_88
host1(config)#aaa domain-map 8005554433 vrouter_100
```

Redirected Authentication

Redirected authentication provides a way to offload AAA activity on the router, by providing the domain-mapping-like feature remotely on the RADIUS server. Redirected authentication works as follows:

1. The router sends an authentication request (in the form of a RADIUS access-request message) to the RADIUS server that is configured in the default VR.
2. The RADIUS server determines the user's AAA VR context and returns this information in a RADIUS response message to the router.
3. The router then behaves in similar fashion as if it had received the VR context from the local domain map.



NOTE: If the default VR does not exist, authentication fails.

To maintain local control, the only VR allowed to redirect authentication is the default VR. Also, to prevent loopbacks, the redirection may occur only once to a non-default VR.

To maintain flexibility, the redirection response may include idle time or session attributes that are considered as default unless the redirected authentication server overrides them. For example, if the RADIUS server returns the VR context along with an idle timeout attribute with the value set to 20 minutes, the router uses this idle timeout value unless the RADIUS server configured in the VR context returns a different value.

Since the router supports the RADIUS User-Name attribute [1] in the RADIUS response message, the default VR RADIUS server may override the user's name (this can be a stripped name or an entirely different name). Overriding is useful for the case when the user enters a login name containing a domain name that is significant only to the RADIUS server in the default VR.

IP Hinting

You can allocate an address before authentication of PPP sessions. This address is included in the Access-Request sent to the authentication server as an IP address hint.

aaa domain-map

- Use to map a user domain name to a virtual router or a loopback interface.
- When you specify only the domain name, the command sets the mode to Domain Map Configuration.
- Example


```
host1(config)#aaa domain-map juniper.net vrouter_1
host1(config)#aaa domain-map none vrouter_all_purpose
host1(config)#aaa domain-map default vrouter_all_purpose
host1(config)#aaa domain-map 8005558934 vrouter_78
host1(config)#aaa domain-map westford.com
host1(config-domain-map)#
```
- Use the **no** version to delete the map entry.

ip-hint

- Use to preallocate an IP address for the remote B-RAS user before authenticating the remote user.
- The address is passed as a *hint* in the authentication request.
- Example


```
host1(config-domain-map)#ip-hint enable
```
- Use the **no** version to disable the feature.

ipv6-local-interface

- Use to map a user domain name to an IP version 6 (IPv6) loopback interface.
- The local interface identifies the interface information to use on the local (E-series) side of the subscriber's interface.
- Example


```
host1(config)#aaa domain-map westford.com
host1(config-domain-map)#ipv6-local-interface 2001:db8::8000
```
- Use the **no** version to delete the entry.

ipv6-router-name

- Use to map a user domain name to an IPv6 virtual router in Domain Map Configuration mode.
- Example


```
host1(config)#aaa domain-map westford.com
host1(config-domain-map)#ipv6-router-name vrouter6
```
- Use the **no** version to delete the entry.

local-interface

- Use to map a user domain name to a loopback interface.
- The local interface identifies the interface information to use on the local (E-series) side of the subscriber's interface.
- Example


```
host1(config)#aaa domain-map westford.com
host1(config-domain-map)#local-interface 10.10.5.30
```
- Use the **no** version to delete the entry.

router-name

- Use to map a user domain name to a virtual router.
- Example


```
host1(config)#aaa domain-map westford.com
host1(config-domain-map)#router-name vROUT
```
- Use the **no** version to delete the entry.

Setting Up Domain Name and Realm Name Usage

To provide flexibility in how the router handles different types of usernames, the software lets you specify the part of a username to use as the domain name, how the domain name is designated, and how the router parses names. It also allows you to set whether or not the router strips the domain name from the username before it sends the username to the RADIUS server.

By default, the router parses usernames as follows:

```
realmName/personalName@domainName
```

The string to the left of the forward slash (/) is the realm name, and the string to the right of the at-symbol (@) is the domain name. For example, in the username `juniper/jill@abc.com`, `juniper` is the realm name and `abc.com` is the domain name.

The router allows you to:

- Use the realm name as the domain name.
- Use delimiters other than / to designate the realm name.
- Use delimiters other than @ to designate the domain name.
- Use either the domain or the realm as the domain name when the username contains both a realm and domain name.
- Change the direction in which the router searches for the domain name or the realm name.

To provide these features, the router allows you to specify delimiters for the domain name and realm name. You can use up to eight one-character delimiters each for domain and realm names. The router also lets you specify how it parses usernames to determine which part of a username to use as the domain name.

Using the Realm Name as the Domain Name

Typically, a realm appears before the user field and is separated with the / character; for example, `usEast/jill@abc.com`. To use the realm name `usEast` rather than `abc.com` as the domain name, set the realm name delimiter to /. For example:

```
host1(config)#aaa delimiter realmName /
```

This command causes the router to use the string to the left of the / as the domain name. If the realm name delimiter is null (the default), the router will not search for the realm name.

Using Delimiters Other Than @

You can set up the router to recognize delimiters other than @ to designate the domain name. Suppose there are two users: `bob@abc.com` and `pete!xyz.com`, and you want to use both of their domain names. In this case you would set the domain name delimiter to @ and !. For example:

```
host1(config)#aaa delimiter domainName @!
```

Using Either the Domain or the Realm as the Domain Name

If the username contains both a realm name and a domain name delimiter, you can use either the domain name or the realm name as the domain name. As previously mentioned, the router treats usernames with multiple delimiters as though the realm name is to the left of the realm delimiter and the domain name is to the right of the domain delimiter.

If you set the parse order to:

- domain-first—The router searches for a domain name first. For example, for username `usEast/lori@abc.com`, the domain name is `abc.com`.
- realm-first—The router searches for a realm name first and uses the realm name as the user's domain name. For username `usEast/lori@abc.com`, the domain is `usEast`.

For example, if you set the delimiter for the realm name to / and set the delimiter for the domain name to @, the router parses the realm first by default. The username `usEast/lori@abc.com` results in a domain name of `usEast`. To cause the parsing to return `abc.com` as the domain, enter the **aaa parse-order domain-first** command.

Specifying the Domain Name or Realm Name Parse Direction

You can specify the direction—either left to right or right to left—in which the router performs the parsing operation when identifying the realm name or domain name. This feature is particularly useful if the username contains nested realm or domain names. For example, for a username of `userjohn@abc.com@xyz.com`, you can identify the domain as either `abc.com@xyz.com` or as `xyz.com`, depending on the parse direction that you specify.

You use either the **left-to-right** or **right-to-left** keywords with one of the following keywords to specify the type of search and parsing that the router performs:

- **domainName**—The router searches for the next domain delimiter value in the direction specified. When it reaches a delimiter, the router uses anything to the right of the delimiter as the domain name. Domain parsing is from right to left by default.
- **realmName**—The router searches for the next realm delimiter value in the direction specified. When it reaches a delimiter, the router uses anything to the left of the delimiter as the realm name. Realm parsing is from left to right by default.
- Example

```
host1(config)#aaa parse-direction domainName left-to-right
```

Stripping the Domain Name

The router provides feature that strips the domain name from the username before it sends the name to the RADIUS server in an Access-Request message. You can enable or disable this feature using the **strip-domain** command.

By default, the domain name is the text after the last `@` character. However, if you changed the domain name parsing using the **aaa delimiter**, **aaa parse-order**, or **aaa parse direction** commands, the router strips the domain name and delimiter that result from the parsing.

aaa delimiter

- Use to configure delimiters for the domain and realm names. Specify one of the following keywords:
 - **domainName**—Configures domain name delimiters. The default domain name delimiter is `@`.
 - **realmName**—Configures realm name delimiters. The default realm name delimiter is NULL (no character). In this case, realm parsing is disabled (having no delimiter disables realm parsing).
- You can specify up to eight delimiters each for domain name and realm name.
- Example

```
host1(config)#aaa delimiter domainName @*/
```
- Use the **no** version to return to the default.

aaa parse-direction

- Use to specify the direction the router uses to parse the username for the domain or realm name.
 - **domainName**—Specifies that the domain name is parsed. The router performs domain parsing from right to left by default.
 - **realmName**—Specifies that the realm name is parsed. The router performs realm parsing from left to right by default.
 - **left-to-right**—Router searches from the left-most character. When the router reaches a realm delimiter, it uses anything to the left of the delimiter as the domain. When the router reaches a domain delimiter, it uses anything to the right of the delimiter as the domain.
 - **right-to-left**—Router searches from the right-most character. When the router reaches a realm delimiter, it uses anything to the left of the delimiter as the domain. When the router reaches a domain delimiter, it uses anything to the right of the delimiter as the domain.
- Example


```
host1(config)#aaa parse-direction domainName left-to-right
```
- Use the **no** version to return to the default: right-to-left parsing for domain names and left-to-right parsing for realm names.

aaa parse-order

- Use to specify which part of a username the router uses as the domain name. If a user's name contains both a realm name and a domain name, you can configure the router to use either name as the domain name.
 - **domain-first**—Router searches for a domain name first. When the router reaches a domain delimiter, it uses anything to the right of the delimiter as the domain name. For example, if the username is usEast/lori@abc.com, the domain name is abc.com. If the router does not find a domain name, it then searches for a realm name if the realm delimiter is specified.
 - **realm-first**—Router searches for a realm name first. When the router reaches a realm delimiter, it uses anything to the left of the delimiter as the domain. For example, if the username is usEast/lori@abc.com, the domain name is usEast. If no realm name is found, the router searches for a domain name.
- Example


```
host1(config)#aaa parse-order domain-first
```
- Use the **no** version to return to the default, realm first.

strip-domain

- Use to strip the domain name from the username before sending an access-request message to the RADIUS server.
- By default, the domain name is the text after the last @ character. However, if you change the domain name parsing by using the **aaa delimiter**, **aaa parse-order**, or **parse-direction** command, the router strips the domain name and delimiter that result from the parsing.
- To stop stripping the username, use the **disable** keyword.
- Example


```
host1(config)#aaa domain-map xyz.com
host1(config-domain-map)#strip-domain enable
```
- Use the **no** version to return to the default, disabled.

Domain Name and Realm Name Examples

This section provides examples of possible domain or realm name results that you might obtain, depending on the commands and options you specify. This example uses the following username:

username: usEast/userjohn@abc.com@xyz.com

The router is configured with the following commands:

```
host1(config)#aaa delimiter domainName @!
host1(config)#aaa delimiter realmName /
```

[Table 4](#) shows the username and domain name that result from the parsing action of the various commands.

Table 4: Username and Domain Name Examples

Command	Resulting Username	Resulting Domain Name
aaa parse-order realm-first	userjohn@abc.com@xyz.com	usEast
aaa parse-order domain-first	userjohn@abc.com	xyz.com
aaa parse-direction domainName right-to-left	userjohn@abc.com	xyz.com
aaa parse-direction domainName left-to-right	userjohn	abc.com@xyz.com
aaa parse-direction realmName right-to-left	userjohn@abc.com@xyz.com	usEast
aaa parse-direction realmName left-to-right	userjohn@abc.com@xyz.com	usEast

Specifying a Single Name for Users from a Domain

Assigning a single username and a single password for all users associated with a domain provides better compatibility with some RADIUS servers. You can use this feature for domains that require the router to tunnel, but not terminate, PPP sessions.

When users request a PPP session, they specify usernames and passwords. During the negotiations for the PPP session, the router authenticates legitimate users.



NOTE: This feature works only for users authenticated by Password Authentication Protocol (PAP) and not by Challenge Handshake Authentication Protocol (CHAP).

If you configure this feature, the router substitutes the specified username and password for all authenticated usernames and passwords associated with that domain.

There are two options for this feature. The router can:

- Substitute the domain name for each username and one new password for each existing password.

For example, if the domain name is xyz.com and you specify the password xyz_domain, the router associates the username xyz.com and the password xyz_domain with all users from xyz.com.

- Substitute one new username for each username and one new password for each existing password.

For example, if the domain name is xyz.com and you specify the username xyz_group and the password xyz_domain, the router associates these identifiers with all users from xyz.com.

To use a single username and a single password for all users from a domain:

1. Access Domain Map Configuration mode using the **aaa domain-map** command.
2. Specify the new username and password using the **override-user** command.

aaa domain-map

- Use to map a domain name to a virtual router or to access Domain Map Configuration mode.

- Example

```
host1(config)#aaa domain-map xyz.com
host1(config-domain-map)#
```

- Use the **no** version to delete the map entry.

override-user

- Use to specify a single username and single password for all users from a domain in place of the values received from the remote client.
- Use only for domains that require the router to tunnel and not terminate PPP sessions.
- If you specify a password only, the router substitutes the domain name for the username and associates the new password with the user. If you specify a password only and you have configured the domain name *none* with the **aaa domain-map** command, the router rejects any users without domain names.
- If you specify a name and password, the router associates both the new name and password with the user.
- Example

```
host1(config-domain-map)#override-user name boston password abc
```
- Use the **no** version to revert to the original username.

Configuring RADIUS Authentication and Accounting Servers

The number of RADIUS servers you can configure depends on available memory.

The order in which you configure servers determines the order in which the router contacts those servers on behalf of clients.

Initially, a RADIUS client sends a request to a RADIUS authentication or accounting server. The RADIUS server uses the configured IP address, the UDP port number, and the secret key to make the connection. The RADIUS client waits for a response for a configurable timeout period and then retransmits the request. The RADIUS client retransmits the request for a user-configurable retry limit.

- If there is no response from the primary RADIUS server, the RADIUS client submits the request to the secondary RADIUS server using the timeout period and retry limit configured for the secondary RADIUS server.
- If the connection attempt fails for the secondary RADIUS server, the router submits the request to the tertiary server and so on until it either is granted access on behalf of the client or there are no more configured servers.
- If another authentication server is not configured, the router attempts the next method in the method list; for accounting server requests, the information is dropped.

For example, suppose that you have configured the following authentication servers: Auth1, Auth2, Auth3, Auth4, and Auth5. Your router attempts to send an authentication request to Auth1. If Auth1 is unavailable, the router submits the request to Auth2, then Auth3, and so on until an available server is found. If Auth5, the last configured authentication server, is not available, the router attempts the next method in the methods list. If the only method configured is RADIUS, then the router notifies the client that the request has been denied.

Server Access

The router offers two options by which servers are accessed:

- Direct—The first authentication or accounting server that you configure is treated as the primary authentication or accounting server, the next server configured is the secondary, and so on.
- Round-robin—The first configured server is treated as a primary for the first request, the second server configured as primary for the second request, and so on. When the router reaches the end of the list of servers, it starts again at the top of the list until it comes full cycle through the list.

Use the **radius algorithm** command to specify the server access method.

When you configure the first RADIUS accounting server, a RADIUS Acct-On message is sent. When you delete the last accounting server, a RADIUS Acct-Off message is sent.

Server Request Processing Limit

Authentication servers and accounting servers use different UDP ports on the router. This enables the same IP address to be used for both an authentication server and an accounting server. Note however, that the same IP address cannot be used for multiple authentication servers or for multiple accounting servers.



NOTE: For information about the number of concurrent RADIUS requests that the router supports for authentication and accounting servers, see *JUNOS Release Notes, Appendix A, System Maximums*.

The E-series router listens to UDP source (or local) port 50000 for RADIUS authentication responses and to UDP source port 50016 for RADIUS accounting responses. Each UDP source port supports a maximum of 255 RADIUS requests. When the 255 limit is reached, the router opens the next source port. When the requests-per-server limit is reached, the router submits the request to the next configured server.

Authentication and Accounting Methods

When you configure AAA authentication and accounting services for your B-RAS environment, one important task is to specify the authentication and accounting method used. The JUNOS software gives you the flexibility to configure authentication or accounting methods based on the type of subscriber. This feature allows you to enable RADIUS authentication for some subscribers, while disabling authentication completely for other subscribers. Similarly, you can enable RADIUS accounting for some subscribers, but no accounting for others. For example, you might use RADIUS authentication for ATM 1483 subscribers, while granting IP subscriber management interfaces access without authentication (using the **none** keyword).

You can specify the authentication or accounting method you want to use, or you can specify multiple methods in the order in which you want them used. For example, if you specify the **radius** keyword followed by the **none** keyword when configuring authentication, AAA initially attempts to use RADIUS authentication. If no RADIUS servers are available, AAA uses no authentication. The JUNOS software currently supports **radius** and **none** as accounting methods and **radius**, **none**, and **local** as authentication methods. See [Configuring Local Authentication Servers](#) on page 37 for information about local authentication.

You can configure authentication and accounting methods based on the following types of subscribers:

- ATM 1483
- Tunnels (for example, L2TP tunnels)
- PPP
- RADIUS relay server
- IP subscriber management interfaces



NOTE: IP subscriber management interfaces are static or dynamic interfaces that are created or managed by the JUNOS software's subscriber management feature.

Supporting Exchange of Extensible Authentication Protocol Messages

Extensible Authentication Protocol (EAP) is a protocol that supports multiple methods for authenticating a peer before allowing network layer protocols to transmit over the link. JUNOS software supports the exchange of EAP messages between JUNOS applications, such as PPP, and an external RADIUS authentication server.

The JUNOS software's AAA service accepts and passes EAP messages between the JUNOS application and the router's internal RADIUS authentication server. The internal RADIUS authentication server, which is a RADIUS client, provides EAP pass-through—the RADIUS client accepts the EAP messages from AAA, and sends the messages to the external RADIUS server for authentication. The RADIUS client then passes the response from the external RADIUS authentication server back to the AAA service, which then sends a response to the JUNOS application. The AAA service and the internal RADIUS authentication service do not process EAP information—both simply act as pass-through devices for the EAP message.

The router's local authentication server and TACACS+ authentication servers do not support the exchange of EAP messages. These type of servers deny access if they receive an authentication request from AAA that includes an EAP message. EAP messages do not affect the **none** authentication configuration, which always grants access.

The local RADIUS authentication server uses the following RADIUS attributes when exchanging EAP messages with the external RADIUS authentication server:

- Framed-MTU (attribute 12)—Used if AAA passes an MTU value to the internal RADIUS client
- State (attribute 24)—Used in Challenge-Response messages from the external server and returned to the external server on the subsequent Access-Request
- Session-Timeout (attribute 27)—Used in Challenge-Response messages from the external server
- EAP-Message (attribute 79)—Used to fragment EAP strings into 253-byte fragments (the RADIUS limit)
- Message-Authenticator (attribute 80)—Used to authenticate messages that include an EAP-Message attribute

For additional information on configuring PPP to use EAP authentication, see *Extensible Authentication Protocol* in *JUNOS Link Layer Configuration Guide, Chapter 4, Configuring Point-to-Point Protocol*.

Immediate Accounting Updates

You can use the **aaa accounting immediate-update** command to configure immediate accounting updates on a per-VR basis. If you enable this feature, the E-series router sends an Acct-Update message to the accounting server immediately on receipt of a response (ACK or timeout) to the Acct-Start message.

This feature is disabled by default. Use the **enable** keyword to enable immediate updates and the **disable** keyword to halt them.

The accounting update contains 0 (zero) values for the input/output octets/packets and 0 (zero) for uptime. If you have enabled duplicate or broadcast accounting, the accounting update goes to both the primary virtual router context and the duplicate or broadcast virtual router context.

Duplicate and Broadcast Accounting

Normally, the JUNOS software sends subscriber-related AAA accounting information to the virtual router that authenticates the subscriber. If an operational virtual router is configured that is different from the authentication router, it also receives the accounting information. You can optionally configure duplicate or broadcast AAA accounting, which sends the accounting information to additional virtual routers simultaneously. The accounting information continues to be sent to the authenticating virtual router, but not to the operational virtual router.

Both the duplicate and broadcast accounting features are supported on a per-virtual router context, and enable you to specify particular accounting servers that you want to receive the accounting information.

For example, you might use broadcast accounting to send accounting information to a group of your private accounting servers. Or you might use duplicate accounting to send the accounting information to a customer's accounting server.

- Duplicate accounting—Sends the accounting information to a particular virtual router
- Broadcast accounting—Sends the accounting information to a group of virtual routers. An accounting virtual router group can contain up to four virtual routers and the E-series router supports a maximum of 100 virtual router groups. The accounting information continues to be sent to the duplicate accounting virtual router, if one is configured.

Configuring AAA Duplicate Accounting

To configure and enable duplicate accounting on a virtual router, you use the **aaa accounting duplication** command with the name of the accounting server that will receive the information. For example, to enable duplicate accounting for the default virtual router:

```
host1(config)#aaa accounting duplication xyzCompanyServer
```

Configuring AAA Broadcast Accounting

To configure and enable broadcast accounting on a virtual router:

1. Create the virtual router group and enter VR Group Configuration mode:

```
host1(config)#aaa accounting vr-group groupXyzCompany
host1(vr-group-config)#
```

2. Add up to four virtual routers to the group. The accounting information will be sent to all virtual routers in the group.

```
host1(vr-group-config)#aaa virtual-router 1 vrXyz1
host1(vr-group-config)#aaa virtual-router 2 vrXyz2
host1(vr-group-config)#aaa virtual-router 3 vrXyz3
host1(vr-group-config)#exit
host1(config)#
```

3. Enable broadcast accounting. Enter the correct virtual router context, and specify the virtual router group whose virtual routers will receive the accounting information.

```
host1(config)#virtual-router opVr100
host1:opVr100(config)#aaa accounting broadcast groupXyzCompany
```

Overriding AAA Accounting NAS Information

AAA accounting packets normally include two RADIUS attributes—NAS-IP-Address [4] and NAS-Identifier [32]—of the virtual router that generates the accounting information. You can override the default configuration and specify that accounting packets from particular broadcast virtual routers instead include the NAS-IP-Address and NAS-Identifier attributes of the authenticating virtual router.

To override the normal AAA accounting NAS information, access the correct virtual router context, and use the **radius override nas-info** command. For example:

```
host1(config)#virtual-router vrXyz1
host1:vrXyz1(config)#radius override nas-info
host1:vrXyz1(config)#virtual-router vrXyz2
host1:vrXyz2(config)#radius override nas-info
host1:vrXyz3(config)#exit
host1(config)#
```

UDP Checksums

Each virtual router on which you configure B-RAS is enabled to perform UDP checksums by default. You can disable and reenable UDP checksums.

Collecting Accounting Statistics

You can use the **aaa accounting statistics** command to specify how the AAA server collects statistics on the sessions it manages. Use the **volume-time** keyword to specify that AAA notifies applications to collect a full set of statistics from each of their connections. Use the **time** keyword to specify that only the uptime status is collected for each connection. Collecting only uptime information reduces the amount of data sent to AAA and is a more efficient use of system resources for customers that do not need a full set of statistics. The router collects a full set of statistics by default.

Configuring RADIUS AAA Servers

The number of RADIUS servers you can configure depends on available memory. The router has an embedded RADIUS client for authentication and accounting.



NOTE: You can configure B-RAS with RADIUS accounting, but without RADIUS authentication. In this configuration, the username and password on the remote end are not authenticated and can be set to any value.

You must assign an IP address to a RADIUS authentication or accounting server to configure it.

If you do not configure a primary authentication or accounting server, all authentication and accounting requests will fail. You can configure other servers as backup in the event that the primary server cannot be reached. Configure each server individually.

To configure an authentication or accounting RADIUS server:

1. Specify the authentication or accounting server address.

```
host1(config)#radius authentication server 10.10.10.1
host1(config-radius)#
or
host1(config)#radius accounting server 10.10.10.6
host1(config-radius)#
```

2. (Optional) Specify a UDP port for RADIUS authentication or accounting server requests.

```
host1(config-radius)#udp-port 1645
```

3. Specify an authentication or accounting server secret.

```
host1(config-radius)#key gismo
```

4. (Optional) Specify the number of retries the router makes to an authentication or accounting server before it attempts to contact another server.

```
host1(config-radius)#retransmit 2
```

5. (Optional) Specify the number of seconds between retries.

```
host1(config-radius)#timeout 5
```

6. (Optional) Specify the maximum number of outstanding requests.

```
host1(config-radius)#max-sessions 100
```

7. (Optional) Specify the amount of time to remove a server from the available list when a timeout occurs.

```
host1(config-radius)#deadtime 10
```

8. (Optional) In Global Configuration mode, specify whether the E-series router should move on to the next RADIUS server when the router receives an Access-Reject message for the user it is authenticating.

```
host1(config)#radius rollover-on-reject enable
```

9. (Optional) Enable duplicate address checking.

```
host1(config)aaa duplicate-address-check enable
```

10. (Optional) Specify that duplicate accounting records be sent to the accounting server for a virtual router.

```
host1(config)#aaa accounting duplication routerBoston
```

11. (Optional) Enter the correct virtual router context, and specify the virtual router group to which broadcast accounting records are sent.

```
host1(config)#virtual-router vrSouth25
host1:vrSouth25(config)#aaa accounting broadcast westVrGroup38
host1:vrSouth25(config)#exit
```

12. (Optional) Specify that immediate accounting updates be sent to the accounting server when a response is received to an Acct-Start message.

```
host1(config)#aaa accounting immediate-update
```

13. (Optional) Specify whether the router collects all statistics or only the uptime status.

```
host1(config)#aaa accounting time
```

14. (Optional) Specify that tunnel accounting be enabled or disabled.

```
host1(config)#radius tunnel-accounting enable
```

15. (Optional) Specify the default authentication and accounting methods for the subscribers.

```
host1(config)#aaa authentication ppp default radius none
```

16. (Optional) Disable UDP checksums on virtual routers you configure for B-RAS.

```
host1:(config)#virtual router boston
host1:boston(config)#radius udp-checksum disable
```

aaa accounting broadcast

- Use to enable AAA broadcast accounting on a virtual router. Specifies that accounting records be sent to the accounting servers on the virtual routers in the named virtual router group.
- A virtual router group can be used in any virtual router context, not just the context in which it is created.
- Example

```
host1(config)#virtual-router vrSouth25
host1:vrSouth25(config)#aaa accounting broadcast westVrGroup38
host1:vrSouth25(config)#exit
```

- Use the **no** version to disable the AAA broadcast accounting.

aaa accounting default

- Use to specify the accounting method used for a particular type of subscriber.
- Specify one of the following types of subscribers:
 - **atm1483**; this keyword is not supported
 - **tunnel**
 - **ppp**
 - **radius-relay**
 - **ipsec**
 - **ip** (IP subscriber management interfaces)



NOTE: IP subscriber management interfaces are static or dynamic interfaces that are created or managed by the JUNOS software's subscriber management feature.

NOTE: Although the **atm1483** keyword is available in the CLI for this command, that subscriber type is not supported. The router does not support accounting for ATM 1483 subscribers.

- Specify one of the following types of accounting methods:
 - **radius**—RADIUS accounting for the specified subscribers.
 - **none**—No accounting is done for the specified subscribers.
 - **radius none**—Multiple types of accounting; used in the order specified. For example, **radius none** specifies that RADIUS accounting is initially used; however, if RADIUS servers are not available, no accounting is done.
- Example
`host1(config)#aaa accounting ppp default radius`
- Use the **no** version to set the accounting protocol to the default, **radius**.

aaa accounting duplication

- Use to enable AAA duplicate accounting on a virtual router. Specifies that duplicate accounting records be sent to the accounting server on another virtual router.
- Example
`host1(config)#aaa accounting duplication routerBoston`
- Use the **no** version to disable the feature.

aaa accounting immediate-update

- Use to send an accounting update to the accounting server immediately on receipt of a response for an Acct-Start message.
- Use the **enable** keyword to enable immediate updates. Use the **disable** keyword to disable immediate updates. Immediate updates are disabled by default.
- Example
`host1(config)#aaa accounting immediate-update enable`
- Use the **no** version to restore the default condition, disabling immediate updates.

aaa accounting interval

- Use to specify the accounting interval between updates.
- Select an interval in minutes from 10–1440. The default is 0, which means that the feature is disabled.
- Example

```
host1(config)#aaa accounting interval 60
```
- Use the **no** version to turn off interim accounting.

aaa accounting statistics

- Use to specify how the AAA server collects statistics on the sessions it manages.
- Use the **volume-time** keyword to collect all statistics for the sessions.
- Use the **time** keyword to collect only the uptime status of the sessions. Collecting only uptime information is more efficient because less data is sent to AAA.
- Example

```
host1(config)#aaa accounting statistics time
```
- Use the **no** version to restore the default, in which all statistics are collected.

aaa accounting vr-group

- Use to create an accounting virtual router group and enter VR Group Configuration mode. Virtual routing groups are used for AAA broadcast accounting.
- A virtual router group can have up to four virtual routers. The accounting servers of the virtual routers in the group receive broadcast accounting records that are forwarded to the group.
- The E-series router supports a maximum of 100 virtual router groups.
- When creating a virtual router group, you must add at least one virtual router to the group; otherwise, the group is not created.
- A virtual router group can be used in any virtual router context, not just the context in which it is created.
- Example

```
host1(config)#aaa accounting vr-group westVrGroup38
host1(config-vr-group)#
```
- Use the **no** version to delete the accounting virtual router group.

aaa authentication default

- Use to specify the authentication method used for a particular type of subscriber.
- Specify one of the following types of subscribers:
 - **atm1483**
 - **tunnel**
 - **ppp**
 - **radius-relay**
 - **ipsec**
 - **ip** (IP subscriber management interfaces)



NOTE: IP subscriber management interfaces are static or dynamic interfaces that are created or managed by the JUNOS software's subscriber management feature.

- Specify one of the following types of accounting methods:
 - **radius**—RADIUS authentication for the specified subscribers.
 - **none**—Grants the specified subscribers access without authentication.
 - **radius none**—Multiple types of authentication; used in the order specified. For example, **radius none** specifies that RADIUS authentication is initially used; however, if RADIUS servers are not available, users are granted access without authentication.
- Example

```
host1(config)#aaa authentication ip default radius
```
- Use the **no** version to set the authentication protocol to the default, **radius**.

aaa duplicate-address-check

- Use to enable or disable routing table address lookup or duplicate address check.
- The router checks the routing table for returned addresses for PPP users. If the address existed, then the user was denied access.
- You can disable this routing table address lookup or duplicate address check with the **aaa duplicate-address-check** command.
- Example

```
host1(config)#aaa duplicate-address-check enable
```
- There is no **no** version.

aaa virtual-router

- Use to add virtual routers to a virtual router group. During AAA broadcast accounting, accounting records are sent to the accounting servers on the virtual routers in the named virtual router group.
- You can add up to four virtual routers to a virtual router group. Use the *indexInteger* parameter to specify the order (1–4) in which the virtual routers receive the accounting information. The *indexInteger* is used with the **no** version to delete a specific virtual router from a group (see Example 2).
- A virtual router name consists of 1–32 alphanumeric characters.
- The virtual router names in the group must be unique. An error message appears if you enter a duplicate name.
- Example 1

```
host1(config)#aaa accounting vr-group westVrGroup38
host1(config-vr-group)#aaa virtual-router 1 vrWestA
host1(config-vr-group)#aaa virtual-router 2 vrWestB
host1(config-vr-group)#aaa virtual-router 4 vrSouth1
```

- Example 2
- Use the **no** version of the command with the *indexInteger* parameter to delete a specific virtual router from a group. If all virtual routers in a group are deleted, the group is also deleted; a group must contain at least one virtual router.

```
host1(config-vr-group)#no aaa virtual-router 2
```

deadtime

- Use to configure the amount of time (0–30 minutes) that a server is marked as unavailable if a request times out for the configured retry count.
- If a server fails to answer a request, the router marks it *unavailable*. The router does not send requests to the server until the router receives a response from the server or until the configured time is reached, whichever occurs first.
- If all servers fail to answer a request, then instead of marking all servers as unavailable, all servers are marked as available.
- To turn off the deadtime mechanism, specify a value of 0.
- Example

```
host1(config)#radius authentication server 10.10.0.1
host1(config-radius)#deadtime 10
```

- Use the **no** version to set the time to the default value, 0

key

- Use to configure secrets on the primary, secondary, and tertiary authentication servers.
- The authentication or accounting server secret is a text string used by RADIUS to encrypt the client and server *authenticator* field during exchanges between the router and a RADIUS authentication server. The router encrypts PPP PAP passwords using this text string.
- The default is no server secret.

- Example

```
host1(config)#radius authentication server 10.10.8.1
host1(config-radius)#key gismo
```
- Use the **no** version to remove the secret.



NOTE: Authentication fails if no key is specified for the authentication server.

logout subscribers

- Use to issue an administrative reset to the user's connection to disconnect the user.
- From Privileged Exec mode, you can log out **all** subscribers, or log out subscribers by **username**, **domain**, **virtual-router**, or **port**.
- This command applies to PPP users, as well as to non-PPP DHCP users.
- Example

```
host1#logout subscribers username bmurphy
```
- There is no **no** version.

max-sessions

- Use to configure the number of outstanding requests supported by an authentication or accounting server.
- If the request limit is reached, the router sends the request to the next server.



NOTE: For information about the number of concurrent RADIUS requests that the router supports for authentication and accounting servers, see *JUNOS Release Notes, Appendix A, System Maximums*.

- The same IP address can be used for both an authentication and accounting server (but not for multiple servers of the same type). The router uses different UDP ports for authentication servers and accounting servers.
- For each multiple of 255 requests (the RADIUS protocol limit), the router opens a new UDP source (or local) port on the server to send and receive RADIUS requests and responses.
- Example

```
host1(config)#radius authentication server 10.10.0.1
host1(config-radius)#max-sessions 100
```
- Use the **no** version to restore the default value, 255.

no radius client

- Use to remove all RADIUS servers for the virtual router context and to delete the E-series RADIUS client for the virtual router context.
- Example
host1:boston(config)#**no radius client**
- There is no affirmative version of this command; there is only a **no** version.

radius algorithm

- Use to specify the algorithm—either **direct** or **round-robin**—that the E-series RADIUS client uses to contact the RADIUS server.
- Example
host1(config)#**radius algorithm round-robin**
- Use the **no** version to set the algorithm to the default, **direct**.

radius override nas-info

- Use to configure the RADIUS client to include the NAS-IP-Address [4] and NAS-Identifier [32] RADIUS attributes of the authenticating virtual router in accounting packets when the client performs AAA broadcast accounting. Normally, the accounting packets include the NAS-IP-Address and NAS-Identifier of the virtual router that generated the accounting information.
- This override operation is a per-virtual router specification; use this command in the correct virtual router context.
- This command is ignored if the authenticating virtual router does not have a configured RADIUS server.
- Example
host1(config)#**virtual-router vrXyz1**
host1:vrXyz1(config)#**radius override nas-info**
host1:vrXyz1(config)#**exit**
- Use the **no** version to restore inclusion of the NAS-IP-Address [4] and NAS-Identifier [32] RADIUS attributes of the virtual router that requested the accounting information.

radius rollover-on-reject

- Use to specify whether the router rolls over to the next RADIUS server when the router receives an Access-Reject message for the user it is authenticating.
- Example
host1(config)#**radius rollover-on-reject enable**
- Use the **no** version to set the default of disable.

radius accounting server**radius authentication server**

- Use to specify the IP address of **authentication** and **accounting** servers.
- Example


```
host1(config)#radius authentication server 10.10.10.1
host1(config-radius)exit
host1(config)#radius authentication server 10.10.10.2
host1(config-radius)exit
host1(config)#radius authentication server 10.10.10.3
host1(config-radius)exit
host1(config)#radius accounting server 10.10.10.20
host1(config-radius)exit
host1(config)#radius accounting server 10.10.10.30
```
- Use the **no** version to delete the instance of the RADIUS server.

radius tunnel-accounting

- Use to specify that tunnel accounting be enabled or disabled.
- This command turns on accounting messages: Tunnel-Start, Tunnel-Stop, Tunnel-Reject, Tunnel-Link-Start, Tunnel-Link-Stop, and Tunnel-Link-Reject, as described in RFC 2867.
- Your router supports tunnel accounting for the L2TP LAC and LNS.
- Example


```
host1(config)#radius tunnel-accounting enable
```
- Use the **no** version to set the default, disabled.

radius udp-checksum

- Use to disable UDP checksums on virtual routers you configure for B-RAS.
- Issue this command in the context of the appropriate virtual router.
- Example


```
host1(config)#virtual router boston
host1:boston(config)#radius udp-checksum disable
```
- Use the **no** version to reenables UDP checksums on virtual routers you configure for B-RAS.

radius update-source-addr

- Use to specify an alternate source IP address for the router to use rather than the default router ID.
- Example


```
host1(config)#radius update-source-addr 192.168.40.23
```
- Use the **no** version to delete the parameter so that the router uses the router ID.

retransmit

- Use to set the maximum number of times that the router retransmits a RADIUS packet to an authentication or accounting server.
- If there is no response from the primary RADIUS authentication or accounting server in the specified number of retries, the client sends the request to the secondary server. If there is no response from the secondary server, the router sends the request to the tertiary server, and so on.
- Example

```
host1(config)#radius authentication server 10.10.8.1
host1(config-radius)#retransmit 2
```
- Use the **no** version to set the value to the default, 3 retransmits.

test aaa

- Use to verify RADIUS authentication and accounting and IP address assignment setup.
- You must specify either a PPP or Multilink PPP (MLPPP) user. PPP indicates a regular PPP user. MLPPP simulates Multilink PPP so that if multiple test commands are issued, all test users are bound by the same address.
- The command uses a username and password and attempts to authenticate a user, get an address assignment, and issue a start accounting request.
- Optionally, you can specify the virtual router context in which to authenticate the user.
- The command pauses for several seconds, then terminates the session by issuing a stop accounting request and an address release.
- Example

```
host1#test aaa ppp jsmith mypassword virtual-router charlie2
```



NOTE: Specifying the password to associate with the username is optional. Specifying a virtual router is optional.

- There is no **no** version.

timeout

- Use to set the number of seconds before the router retransmits a RADIUS packet to an authentication or accounting server.
- If the interval is reached and there is no response from the primary RADIUS authentication or accounting server, the router attempts another retry. When the retry limit is reached, the client sends the request to the secondary server. When the retry limit for the secondary server is reached, the router attempts to reach the tertiary server, and so on.



NOTE: After the fourth retransmission, the configured timeout value is ignored, and the router uses a backoff algorithm that increases the timeout between each succeeding transmission.

The backoff algorithm is:

$$\text{timeout} = 2^{\text{retry-count}} + (\text{random}() \text{ modulo } 2^{\text{retry-count}})$$

g013623

- Example

```
host1(config)#radius authentication server 10.10.0.1
host1(config-radius)#timeout 5
```

- Use the **no** version to restore the default value, 3 seconds.



NOTE: When a RADIUS server times out or when it has no available RADIUS identifier values, the router removes the RADIUS server from the list of available servers for a period of time. The router restores all configured servers to the list if it is about to remove the last server. Restoring the servers avoids having an empty server list.

udp-port

- Use to configure the UDP port on the router where the RADIUS authentication servers reside. The router uses this port to communicate with the RADIUS authentication servers.
- For an authentication server, specify a port number in the range 0–65536. The default is 1812.
- For an accounting server, specify a port number in the range 0–65536. The default is 1813.
- Example


```
host1(config)#radius authentication server 10.10.9.1
host1(config-radius)#udp-port 1645
```
- Use the **no** version to set the port number to the default value.

SNMP Traps and System Log Messages

The router can send Simple Network Management Protocol (SNMP) traps to alert network managers when:

- A RADIUS server fails to respond to a request.
- A RADIUS server that previously failed to respond to a request (and was consequently removed from the list of active servers) returns to active service.

Returning to active service means that the E-series RADIUS client receives a valid response to an outstanding RADIUS request after the server is marked unavailable.

- All RADIUS servers within a VR context fail to respond to a request.

The router also generates system log messages when RADIUS servers fail to respond or when they return to active service; no configuration is required for system log messages.

SNMP Traps

The router generates SNMP traps and system log messages as follows:

- If the first RADIUS server fails to respond to the RADIUS request, the E-series RADIUS client issues a system log message and, if configured, an SNMP trap indicating that the RADIUS server timed out. The E-series RADIUS client will not issue another system log message or SNMP trap regarding this RADIUS server until the deadtime expires, if configured, or for 3 minutes if deadtime is not configured.
- The E-series RADIUS client then sends the RADIUS request to the second configured RADIUS server. If the second RADIUS server fails to respond to the RADIUS request, the E-series RADIUS client again issues a system log message and, if configured, an SNMP trap indicating that the RADIUS server timed out.
- This process continues until either the E-series RADIUS client receives a valid response from a RADIUS server or the list of configured RADIUS servers is exhausted. If the list of RADIUS servers is exhausted, the E-series RADIUS client issues a system log message and, if configured, an SNMP trap indicating that all RADIUS servers have timed out.

If the E-series RADIUS client receives a RADIUS response from a “dead” RADIUS server during the deadtime period, the RADIUS server is restored to active status.

If the router receives a valid RADIUS response to an outstanding RADIUS request, the E-series client issues a system log message and, if configured, an SNMP trap indicating that the RADIUS server is now available.

System Log Messages

You do not need to configure system log messages. The router automatically sends them when individual servers do not respond to RADIUS requests and when all servers on a VR fail to respond to requests. The following are the formats of the warning level system log messages:

RADIUS [authentication | accounting] server *serverAddress* unavailable in VR *virtualRouterName* [; trying *nextServerAddress*]

RADIUS no [authentication | accounting] servers responding in VR *virtualRouterName*

RADIUS [authentication | accounting] server *serverAddress* available in VR *virtualRouterName*

Configuring SNMP Traps

This section describes how to configure the router to send traps to SNMP when RADIUS servers fail to respond to messages, and how to configure SNMP to receive the traps.

To set up the router to send traps:

1. (Optional) Enable SNMP traps when a particular RADIUS authentication server fails to respond to Access-Request messages.

host1(config)#radius trap auth-server-not-responding enable

2. (Optional) Enable SNMP traps when all of the configured RADIUS authentication servers on a VR fail to respond to Access-Request messages.

host1(config)#radius trap no-auth-server-responding enable

3. (Optional) Enable SNMP traps when a RADIUS authentication server returns to active service.

host1(config)#radius trap auth-server-responding enable

4. (Optional) Enable SNMP traps when a RADIUS accounting server fails to respond to a RADIUS accounting request.

host1(config)#radius trap acct-server-not-responding enable

5. (Optional) Enable SNMP traps when all of the RADIUS accounting servers on a VR fail to respond to a RADIUS accounting request.

host1(config)#radius trap no-acct-server-responding enable

6. (Optional) Enable SNMP traps when a RADIUS accounting server returns to active service.

host1(config)#radius trap acct-server-responding enable

To set up SNMP to receive RADIUS traps:

1. Set up the appropriate SNMP community strings.

```
host1(config)#snmp-server community admin view everything rw
host1(config)#snmp-server community private view user rw
host1(config)#snmp-server community public view everything ro
```

2. Specify the interface whose IP address is the source address for SNMP traps.

```
host1(config)#snmp-server trap-source fastEthernet 0/0
```

3. Configure the host that should receive the SNMP traps.

```
host1(config)#snmp-server host 10.10.132.93 version 2c 3 udp-port 162 radius
```

4. Enable the SNMP router agent to receive and forward RADIUS traps.

```
host1(config)#snmp-server enable traps radius
```

5. Enable the SNMP on the router.

```
host1(config)#snmp-server
```



NOTE: For more information about these SNMP commands, see [Configuring Traps](#) in *JUNOS System Basics Configuration Guide, Chapter 4, Configuring SNMP*.

radius trap acct-server-not-responding

- Use to enable or disable SNMP traps when a particular RADIUS accounting server fails to respond to a RADIUS accounting request.
- The associated SNMP object is rsRadiusClientTrapOnAcctServerUnavailable.
- Example

```
host1(config)#radius trap acct-server-not-responding enable
```
- Use the **no** version to return to the default setting, disable.

radius trap acct-server-responding

- Use to enable or disable SNMP traps when a RADIUS accounting server returns to service after being marked as unavailable.
- The associated SNMP object is rsRadiusClientTrapOnAcctServerAvailable.
- This command affects only the current VR context.
- Example

```
host1(config)#radius trap acct-server-responding enable
```
- Use the **no** version to restore the default, disable.

radius trap auth-server-not-responding

- Use to enable or disable SNMP traps when a RADIUS authentication server fails to respond to a RADIUS Access-Request message.
- The associated SNMP object is rsRadiusClientTrapOnAuthServerUnavailable.
- Example
host1(config)#**radius trap auth-server-not-responding enable**
- Use the **no** version to return to the default setting, disabled.

radius trap auth-server-responding

- Use to enable RADIUS to send SNMP traps when a RADIUS authentication server returns to service after being marked as unavailable.
- The associated SNMP object is rsRadiusClientTrapOnAuthServerAvailable.
- This command affects only the current VR context.
- Example
host1(config)#**radius trap auth-server-responding enable**
- Use the **no** version to restore the default setting, disabled.

radius trap no-acct-server-responding

- Use to enable or disable SNMP traps when all of the configured RADIUS accounting servers per VR fail to respond to a RADIUS accounting request.
- The associated SNMP object is rsRadiusClientTrapOnNoAcctServerAvailable.
- Example
host1(config)#**radius trap no-acct-server-responding enable**
- Use the **no** version to return to the default setting, disabled.

radius trap no-auth-server-responding

- Use to enable or disable SNMP traps when all of the configured RADIUS authentication servers per VR fail to respond to a RADIUS Access-Request message.
- The associated SNMP object is rsRadiusClientTrapOnNoAuthServerAvailable.
- Example
host1(config)#**radius trap no-auth-server-responding enable**
- Use the **no** version to return to the default setting, disabled.

Configuring Local Authentication Servers

The AAA local authentication server enables the E-series router to provide local PAP and CHAP user authentication for subscribers. The router also provides limited authorization, using the IP address, IP address pool, and operational virtual router parameters. When a subscriber logs on to the E-series router that is using local authentication, the subscriber is authenticated against user entries in a local user database; the optional parameters are assigned to subscribers after the subscriber is authenticated.

Creating the Local Authentication Environment

To create your local authentication environment:

1. Create local user databases—Create the default database or a named database.
2. Add entries to local user databases—Add user entries to the database. A database can contain information for multiple users.
3. Assign a local user database to the virtual router—Specify the database that the virtual router will use to authenticate subscribers.
4. Enable local authentication on the virtual router—Specify the **local** method as an AAA authentication method used by the virtual router.

Creating Local User Databases

When a subscriber connects to an E-series router that is using local authentication, the local authentication server uses the entries in the local user database selected by the virtual router to authenticate the subscriber.

A local authentication server can have multiple local user databases, and each database can have entries for multiple subscribers. The default local user database, if it exists, is used for local authentication by default. The E-series router supports a maximum of 100 user entries. A maximum of 100 databases can be configured.

To create a local user database, use the **aaa local database** command and the name of the database; use the name **default** to create the default local user database:

```
host1(config)#aaa local database westLocal40
```

Adding User Entries to Local User Databases

The local authentication server uses the information in a local user database to authenticate a subscriber. A local user database can contain information for multiple users.

The E-series router provides two commands for adding entries to local user databases: the **username** command and the **aaa local username** command. You can specify the following parameters:

- Username—Name associated with the subscriber.
- Passwords and secrets—Single words that can be encrypted or unencrypted. Passwords use two-way encryption, and secrets use one-way encryption. Both passwords and secrets can be used with PAP authentication; however, only passwords can be used with CHAP authentication.
- IP address—The IP address to assign to the subscriber (**aaa local username** command only).
- IP address pool—The IP address pool used to assign the subscriber's IP address (**aaa local username** command only).
- Operational virtual router—The virtual router to which the subscriber is assigned. This parameter is applicable only if the subscriber is authenticated by the default virtual router (**aaa local username** command only).

Using the username Command

The **username** command is similar to the command used by some third-party vendors. The command can be used to add entries in the default local user database; it is not supported for named local user databases. The IP address, IP address pool, and operational virtual router parameters are not supported in the **username** command. However, after the user is added to the default local user database, you can use the **aaa local username** command with a database name **default** to enter Local User Configuration mode and add the additional parameters.



NOTE: If the default local user database does not exist, the **username** command creates this database and adds the user entry to the database.

To add a subscriber and password or secret to the default local user database, complete the following step:

```
host1(config)#username rockyB password rockyPassword
```

Using the **aaa local username** Command

To enter Local User Configuration mode and add user entries to a local user database, use the following commands:

1. Specify the subscriber's username and the database you want to use. Use the database name **default** to specify the default local user database. This command also puts the router into Local User Configuration mode.

```
host1(config)# aaa local username cksmith database westLocal40
host1(config-local-user)#
```



NOTE: You can use the **aaa local username** command to add or modify user entries to a default database that was created by the **username** command.

2. (Optional) Specify the type of encryption algorithm and the password or secret that the subscriber must use to connect to the router. A subscriber can be assigned either a password or a secret, but not both. For example:

```
host1(config-local-user)#password 8 iTakes2%
```

3. (Optional) Specify the IP address to assign to the subscriber.

```
host1(config-local-user)#ip-address 192.168.101.19
```

4. (Optional) Specify the IP address pool used to assign the subscriber's IP address.

```
host1(config-local-user)#ip-address-pool svPool2
```

5. (Optional) Assign the subscriber to an operational virtual router. This parameter is applicable only if the subscriber is authenticated in the default virtual router.

```
host1(config-local-user)#operational-virtual-router boston2
```

Assigning a Local User Database to a Virtual Router

Use the procedure in this section to assign a local user database to a virtual router. The virtual router uses the database for local authentication when the subscriber connects to the E-series router. Use the following commands in Global Configuration mode:



NOTE: If you do not specify a local user database, the virtual router selects the default database by default. This applies to all virtual routers.

1. Specify the virtual router name.

```
host1(config)# virtual-router cleveland
```

2. Specify the database to use for authentication on this virtual router.

```
host1:cleveland(config)# aaa local select database westLocal40
```

Enabling Local Authentication on the Virtual Router

On the E-series router, RADIUS is the default AAA authentication method for PPP subscribers. Use the commands in this section to specify that the local authentication method is used.

To enable local authentication on the default router, use the following command:

```
host1(config)# aaa authentication ppp default local
```

To enable local authentication on a specific virtual router, first select the virtual router:

```
host1(config)# virtual-router cleveland  
host1:cleveland(config)# aaa authentication ppp default local
```

Configuration Commands

Use the following commands to configure the local authentication server.

aaa authentication default

- Use to specify that the local authentication method is used to authenticate PPP subscribers on the default virtual router or on the selected virtual router.



NOTE: You can specify multiple authentication methods; for example, **aaa authentication ppp default local radius**. If, during local authentication, the matching user entry is not found in a populated database or if it is found and rejected, the authentication procedure terminates. However, if the specified local user database is empty or if it does not exist, the authentication process uses the next authentication method specified (RADIUS in this case).

- Example
host1(config)#**aaa authentication ppp default local radius**
- Use the **no** version to restore the default authentication method of **radius**.

aaa local database

- Use to create a local user database.
- Use the database name **default** to specify the default local user database, or enter a name for the specific local user database.
- Example
host1(config)#**aaa local database westLocal40**
- Use the **no** version to delete the specified database and all entries in the database.

aaa local select database

- Use to assign the local user database that the virtual router uses for local authentication.
- Example

```
host1(config)#virtual-router cleveland
host1:cleveland(config)#aaa local select database westLocal40
```
- Use the **no** version to restore the default setting, which uses the default local user database for local authentication.

aaa local username

- Use to configure a user entry in the specified local user database and to enter Local User Configuration mode.
- The username must be unique within a particular database; however, the same username can be used in different databases.
- Use the database name **default** to configure the username in the default local user database.



NOTE: The router supports usernames up to 64 characters long; however, PAP and CHAP support is limited to 31-character usernames.

- Example

```
host1(config)#aaa local username cksmith database westLocal40
```
- Use the **no** version to delete the user entry from the specified local user database. Use the database name **default** to delete the user entry from the default local user database.

ip-address

- Use to specify the IP address parameter for a user entry in the local user database. The address is negotiated with the subscriber after the subscriber is authenticated.
- Example

```
host1(config-local-user)#ip-address 192.168.42.6
```
- Use the **no** version to delete the IP address parameter from the user entry in the local user database.

ip-address-pool

- Use to specify the IP address pool parameter for a user entry in the local user database. The address pool is used to assign an IP address to the subscriber; the address is negotiated with the subscriber after the subscriber is authenticated.
- Example
`host1(config-local-user)#ip-address-pool svPool2`
- Use the **no** version to delete the IP address pool parameter from the user entry in the local user database.

operational-virtual-router

- Use to specify the virtual router parameter for a user entry in the local user database. The subscriber is assigned to the operational virtual router only if the default virtual router performs the authentication.
- If authentication is performed by a non-default virtual router, then the subscriber is assigned to the same virtual router that performs authentication, regardless of this parameter setting.
- Example
`host1(config-local-user)#operational-virtual-router boston2`
- Use the **no** version to delete the operational virtual router parameter from the user entry in the local user database.

password

- Use to add a password to a user entry in the local user database. The password is used to authenticate a subscriber, and is encrypted by means of a two-way encryption algorithm.



NOTE: CHAP authentication requires that passwords and secrets be stored in clear text or use two-way encryption. Two-way encryption is not supported for the **secret** command. Therefore, use the **password** command if you want to enable encryption for subscribers that use CHAP authentication.

- The new password replaces any current password or secret.
- Specify one of the following encryption algorithms, followed by the password:
 - 0—An unencrypted password; this is the default
 - 8—A two-way encrypted password
- Example
`host1(config-local-user)#password 0 myPassword`
- Use the **no** version to delete the password or secret from the user entry in the local user database.

secret

- Use to add a secret to a user entry in the local user database. The secret is used to authenticate a subscriber, and is encrypted by means of the Message Digest 5 (MD5) encryption algorithm.



NOTE: CHAP authentication requires that passwords and secrets be stored in clear text or use two-way encryption. Two-way encryption is not supported for the **secret** command. Therefore, use the **password** command if you want to enable encryption for subscribers that use CHAP authentication.

- The new secret replaces any current password or secret.
- Specify one of the following encryption algorithms, followed by the secret:
 - 0—An unencrypted secret; this is the default
 - 5—An MD5-encrypted secret
- Example
`host1(config-local-user)#secret 5 Q3&t9REwk45jxSM#fj$z`
- Use the **no** version to delete the secret or password from the user entry in the local user database.

username

- Use to configure a user entry and optional password or secret in the default local user database. This command creates the database if it does not already exist.
- Optionally, specify a password or secret that is assigned to the user in the default local user database, or specify that no password is required for the particular username.
 - Specify one of the following encryption algorithms, followed by the password:
 - 0—An unencrypted password; this is the default
 - 8—A two-way encrypted password
 - Specify one of the following encryption algorithms, followed by the secret:
 - 0—An unencrypted secret; this is the default
 - 5—An MD5-encrypted secret
- Use the **nopassword** keyword to remove the password or secret



NOTE: CHAP authentication requires that passwords and secrets be stored in clear text or use two-way encryption. Two-way encryption is not supported for the **secret** command. Therefore, use the **password** command if you want to enable encryption for subscribers that use CHAP authentication.

- Example
`host1(config-local-user)#username cksmith secret 5 Q3&t9REwk45jxSM#fj$z`
- Use the **no** version to delete the username entry from the default local user database.

Local Authentication Example

This example creates a sample local authentication environment. The steps in this example:

1. Create a named local user database (**westfordLocal40**).
2. Configure the database **westfordLocal40**.
 - Add users **btjones** and **maryrdavis** and their attributes to the database.
3. Create the default local database using the optional **username** command.
 - Add optional subscriber parameters for user **cksmith** to the default database.
4. Assign the default local user database to virtual router **cleveland**; assign database **westfordLocal40** to the default virtual router and to virtual router **chicago**.
5. Enable AAA authentication methods **local** and **none** on all virtual routers.
6. Use the **show** commands to display information for the local authentication environment (various **show** command displays are listed after the example).

Example 1 This example shows the commands you use to create the AAA local authentication environment.

```
host1(config)#aaa local database westfordLocal40
host1(config)#aaa local username btjones database westfordLocal40
host1(config-local-user)#secret 38schillCy
host1(config-local-user)#ip-address-pool addressPoolA
host1(config-local-user)#operational-virtual-router boston2
host1(config-local-user)#exit
host1(config)#aaa local username maryrdavis database westfordLocal40
host1(config-local-user)#secret 0 dav1sSecret99
host1(config-local-user)#ip-address 192.168.20.106
host1(config-local-user)#operational-virtual-router boston1
host1(config-local-user)#exit
host1(config)#username cksmith password 0 yourPassword1
host1(config)#aaa local username cksmith database default
host1(config-local-user)#ip-address-pool addressPoolA
host1(config-local-user)#operational-virtual-router boston2
host1(config-local-user)#exit
host1(config)#virtual-router cleveland
host1(config)#aaa local select database default
host1(config)#virtual-router default
host1(config)#aaa local select database westfordLocal40
host1(config)#virtual-router chicago
host1(config)#aaa local select database westfordLocal40
host1(config)#virtual-router default
host1(config)#aaa authentication ppp default local none
```

Example 2 This example verifies that local authentication is configured on the router.

```
host1#show aaa authentication ppp default
local none
```

Example 3 This example uses the **show configuration category aaa local-authentication** command with the **databases** keyword to show the local user databases that are configured on the router.

```
host1#show configuration category aaa local-authentication databases
! Configuration script being generated on TUE NOV 09 2004 12:50:18 UTC
! Juniper Edge Routing Switch ERX-1400
! Version: 6.1.0 (November 8, 2004 18:31)
! Copyright (c) 1999-2004 Juniper Networks, Inc. All rights reserved.
!
! Commands displayed are limited to those available at privilege level 15
!
! NOTE: This script represents only a subset of the full system configuration.
! The category displayed is: aaa local-authentication databases
!
hostname host1
aaa new-model
aaa local database default
aaa local database westfordLocal40
```

Example 4 This example uses the **local-authentication users** keywords to show the configured users and their parameters. The password for **username cksmith** is displayed unencrypted because the default setting of disabled or no for the **service password-encryption** command is used for the example. Secrets are always displayed encrypted.

```
host1#show configuration category aaa local-authentication users
! Configuration script being generated on THU NOV 11 2004 13:40:41 UTC
! Juniper Edge Routing Switch ERX-1400
! Version: 6.1.0 (November 10, 2004 21:15)
! Copyright (c) 1999-2004 Juniper Networks, Inc. All rights reserved.
!
! Commands displayed are limited to those available at privilege level 15
!
! NOTE: This script represents only a subset of the full system configuration.
! The category displayed is: aaa local-authentication users
!
hostname host1
aaa new-model
aaa local username cksmith database default
password yourPassword1
operational-virtual-router boston2
ip-address-pool addressPoolA
!
aaa local username btjones database westfordLocal40
secret 5 }9s7-4N<WK2)2=)^!6~#
operational-virtual-router boston2
ip-address-pool addressPoolA
!
aaa local username maryrdavis database westfordLocal40
secret 5 E@A:nDXJJ<irb\`mF#[j
operational-virtual-router boston1
ip-address 192.168.20.106
```

Example 5 This example uses the **users include-defaults** keywords to show the configured users and their parameters, including the default parameters **no-ip-address** and **no ip-address-pool**.

```
host1#show configuration category aaa local-authentication users include-defaults
! Configuration script being generated on TUE NOV 09 2004 13:09:03 UTC
! Juniper Edge Routing Switch ERX-1400
! Version: 6.1.0 (November 8, 2004 18:31)
! Copyright (c) 1999-2004 Juniper Networks, Inc. All rights reserved.
!
! Commands displayed are limited to those available at privilege level 15
!
! NOTE: This script represents only a subset of the full system configuration.
! The category displayed is: aaa local-authentication users
!
hostname host1
aaa new-model
aaa local username cksmith database default
    password yourPassword1
    operational-virtual-router boston2
    no ip-address
    ip-address-pool addressPoolA
!
aaa local username btjones database westfordLocal40
    secret 5 }9s7-4N<WK2)2=)^!6~#
    operational-virtual-router boston2
    no ip-address
    ip-address-pool addressPoolA
!
aaa local username maryrdavis database westfordLocal40
    secret 5 E@A:nDXJJ<irb\`mF#[j
    operational-virtual-router boston1
    ip-address 192.168.20.106
    no ip-address-pool
```

Example 6 This example uses the **virtual-router** keyword with the **default** specification to show the local user database that is used by the default virtual router.

```
host1#show configuration category aaa local-authentication virtual-router default
! Configuration script being generated on TUE NOV 09 2004 13:09:45 UTC
! Juniper Edge Routing Switch ERX-1400
! Version: 6.1.0 (November 8, 2004 18:31)
! Copyright (c) 1999-2004 Juniper Networks, Inc. All rights reserved.
!
! Commands displayed are limited to those available at privilege level 15
!
! NOTE: This script represents only a subset of the full system configuration.
! The category displayed is: aaa local-authentication
!
virtual-router default
aaa local select database westfordLocal40
```

Example 7 This example uses the **virtual-router** keyword with a named virtual router. The **include-defaults** keyword shows the default configuration, including the line showing that there is no named local user database selected.

```
host1#show configuration category aaa local-authentication virtual-router cleveland include-defaults
! Configuration script being generated on TUE NOV 09 2004 13:09:25 UTC
! Juniper Edge Routing Switch ERX-1400
! Version: 6.1.0 (November 8, 2004 18:31)
! Copyright (c) 1999-2004 Juniper Networks, Inc. All rights reserved.
!
! Commands displayed are limited to those available at privilege level 15
!
! NOTE: This script represents only a subset of the full system configuration.
! The category displayed is: aaa local-authentication
!
virtual-router cleveland
no aaa local select
```

Configuring Name Server Addresses

You can assign IP or IPv6 addresses for DNS and IP addresses for WINS name servers.

During setup negotiations between the router and remote PC clients using PPP (Internet Protocol Control Protocol [IPCP] specifically), the remote client may request the DNS and WINS server IP addresses. If the IP addresses passed to the router by the remote PC client are different from the ones configured on your router, the router returns the values that you configured as the correct values to the remote PC client. This behavior is controlled by the **ppp peer dns** and **ppp peer wins** interface commands.

If a PPP client request contains address values of 0.0.0.0 for the name servers, the router considers that the remote PC client is not configured and returns the configured values as the correct values to the remote PC client.

The DNS and WINS addresses are considered as part of the PPP user information. These addresses are provided to the PPP client as part of the IPCP negotiations between PPP peers. For details, see [RFC 1877—PPP Internet Protocol Control Protocol Extensions for Name Server Addresses \(December 1995\)](#).



NOTE: All name server address parameters are defined in the context of a virtual router.

Configuration Tasks

This section contains procedures for configuring the DNS and WINS primary and secondary name server addresses.

DNS Primary and Secondary NMS Configuration

To configure the DNS primary and secondary name server addresses:

1. Specify the IP address of the DNS primary name server.

```
host1(config)#aaa dns primary 10.10.10.5
```

or, for IPv6,

```
host1(config)#aaa ipv6-dns primary 2001:db8::8001
```

2. Specify the IP address of the DNS secondary name server.

```
host1(config)#aaa dns secondary 10.10.10.6
```

or, for IPv6,

```
host1(config)#aaa ipv6-dns secondary 2001:db8::8002
```



NOTE: The router uses name server addresses exclusively for PPP clients and not for domain name server resolution.

aaa dns primary

- Use to specify the IP address of the DNS primary name server.
- Example

```
host1(config)#aaa dns primary 10.10.10.5
```
- Use the **no** version to set the corresponding address to 0.0.0.0.

aaa dns secondary

- Use to specify the IP address of the DNS secondary name server.
- Example

```
host1(config)#aaa dns secondary 10.10.10.6
```
- Use the **no** version to set the corresponding address to 0.0.0.0.

aaa ipv6-dns primary

- Use to specify the IPv6 address of the DNS primary name server.
- Example

```
host1(config)#aaa ipv6-dns primary 2001:db8::8001
```
- Use the **no** version to set the corresponding address to 0 (or ::).

aaa ipv6-dns secondary

- Use to specify the IPv6 address of the DNS secondary name server.
- Example

```
host1(config)#aaa ipv6-dns secondary 2001:db8::8002
```
- Use the **no** version to set the corresponding address to 0 (or ::).

WINS Primary and Secondary NMS Configuration

To configure the WINS primary and secondary name server addresses:

1. Specify the IP address of the WINS primary name server.

```
host1(config)#aaa wins primary 192.168.10.05
```

2. Specify the IP address of the WINS secondary name server.

```
host1(config)#aaa wins secondary 192.168.10.40
```



NOTE: The router uses name server addresses exclusively for PPP clients and not for domain name server resolution.

aaa wins primary

- Use to specify the IP address of the WINS primary name server.
- Example

```
host1(config)#aaa wins primary 192.168.10.05
```
- Use the **no** version to set the corresponding address to 0.0.0.0.

aaa wins secondary

- Use to specify the IP address of the WINS secondary name server.
- Example

```
host1(config)#aaa wins secondary 192.168.10.40
```
- Use the **no** version to set the corresponding address to 0.0.0.0.

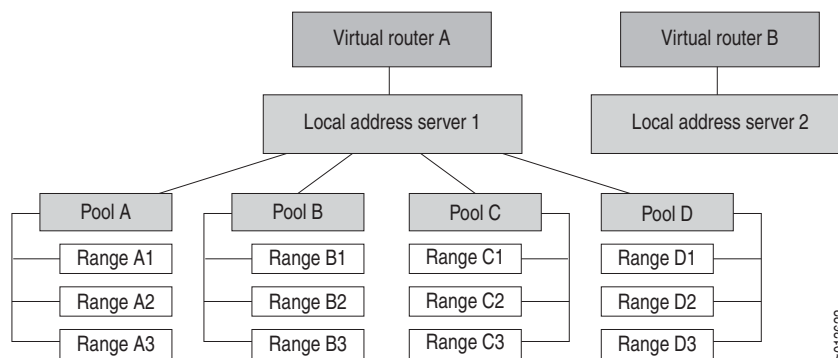
Configuring Local Address Servers

The local address server allocates IP addresses from a pool of addresses stored locally on the router. You can optionally configure shared local address pools to obtain addresses from a DHCP local address pool that is in the same virtual router. Addresses are provided automatically to client sessions requiring an IP address from a virtual router that is configured to use a local address pool.

A local address server is defined in the context of a virtual router. You create a local address server when you configure the first local pool. Local address servers exist as long as the virtual router exists or until you remove them by deleting all configured pools.

Figure 1 illustrates the local address pool hierarchy. Multiple local address server instances, one per virtual router, can exist. Each local address server can have one or more local address pools. Each pool can contain a number of IP addresses that are available for allocation and used by clients, such as PPP sessions.

Figure 1: Local Address Pool Hierarchy



Local Address Pool Ranges

As shown in Figure 1, each local address pool is named and contains ranges of sequentially ordered IP addresses. These addresses are allocated when the AAA server makes a request for an IP address.

If a local address pool range is exhausted, the next range of addresses is used. If all pool ranges are exhausted, you can configure a new range to extend or supplement the existing range of addresses, or you can create a new pool. The newly created pool range is then used for future address allocation. If addresses allocated from the first pool range are released, then subsequent requests for addresses are taken from the first pool range.

Addresses are assigned sequentially from a range within a pool. If a range has no addresses available, the next range within that pool is used. If a pool has no addresses available, the next configured pool is used, unless a specific pool is indicated.

Local Address Pool Aliases

An alias is an alternate name for an existing local address pool. It comprises an alias name and a pool name.

When the AAA server requests an IP address from a specific local address pool, the local address server first verifies whether an alias exists for the requested pool. If an alias exists, the IP address is allocated from the pool specified by the alias. If no alias exists, the IP address is allocated from the pool originally specified in the request.

The use of aliases simplifies management of subscribers. For example, you can use an alias to migrate subscribers from one local address pool to another. Instead of having to modify countless subscriber records on the AAA server, you create an alias to make the configuration change.

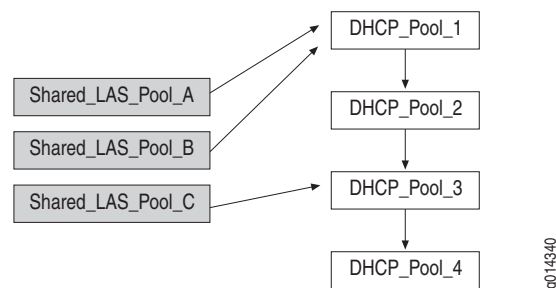
Shared Local Address Pools

Typically, the local address server allocates IP addresses from a pool of addresses that is stored locally on the router. However, *shared* local address pools enable a local address server to hand out addresses that are allocated from DHCP local server address pools within the same virtual router. The addresses are configured and managed within DHCP. Therefore, thresholds are not configured on the shared pool, but are instead managed by the referenced DHCP local server pool.

A shared local address pool references one DHCP address pool. The shared local address pool can then obtain addresses from the referenced DHCP address pool and from any DHCP address pools that are linked to the referenced DHCP address pool.

Figure 2 illustrates a shared local address pool environment that includes four linked DHCP address pools. In the figure, both Shared_LAS_Pool_A and Shared_LAS_Pool_B reference DHCP_Pool_1, and can therefore obtain addresses from all four DHCP address pools. Shared_LAS_Pool_C references DHCP_Pool_3 and can get addresses from DHCP_Pool_3 and DHCP_Pool_4.

Figure 2: Shared Local Address Pools



When the local address server requests an address from a shared address pool, the address is returned from the referenced DHCP pool or a subsequent linked pool. If no address is available, DHCP notifies the local address server and the search is ended.

Keep the following guidelines in mind when using shared local address pools:

- The DHCP attributes do not apply to shared local address pools; for example, the lease time for shared local address pools is infinite.
- When you delete the referenced DHCP address pool, DHCP notifies the local address server and logs out all subscribers that are using addresses from the deleted pool.
- When you delete a shared local address pool, the local address server logs out the subscribers that are using addresses from the deleted pool, then notifies DHCP and releases the addresses.
- If the chain of linked DHCP address pools is broken, no action is taken and the existing subscribers retain their address. However, the DHCP local address pools that are no longer part of the chain are now unable to provide any new addresses.

Example This following commands create the shared address pools in [Figure 2 on page 51](#):

```
host1(config)#ip local shared-pool Shared_LAS_Pool_A DHCP_Pool_1
host1(config)#ip local shared-pool Shared_LAS_Pool_B DHCP_Pool_1
host1(config)#ip local shared-pool Shared_LAS_Pool_C DHCP_Pool_3
```

SNMP Thresholds

An address pool has SNMP thresholds associated with it that enable 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.

Configuring a Local Address Server

You can create, modify, and delete address pools. You can display address pool information or status with the **show ip local pool** command described in [Monitoring Remote Access](#) on page 88. The following are examples of tasks you can configure:

- Specify an addressing scheme.

```
host1(config)#ip address-pool local
```

- Map an address pool name to a range of local addresses. You can also use this command to add additional ranges to a pool.

```
host1(config)#ip local pool addrpool_10 192.168.56.10 192.168.56.15
```

- Map an address pool name to a domain name.

```
host1(config)#aaa domain-map westford.com
host1(config-domain-map)#address-pool-name poolA
```

- Delete an address pool.

```
host1(config)#no ip local pool addrpool_10
```



NOTE: If a pool or range is deleted and addresses are outstanding, the AAA server logs out the clients using the addresses.

- Create a shared local address pool.

```
host1(config)#ip local shared-pool Shared_LAS_Pool_A DHCP_Pool_1
```

- Delete a shared local address pool.

```
host1(config)#no ip local shared-pool Shared_LAS_Pool_C
```

- Set SNMP variables by specifying an existing pool name and values.

```
host1(config)#ip local pool addrpool_10 warning 90 80
```

address-pool-name

- Use to specify the name of the local address pool from which the router allocates addresses for the domain that you are configuring.
- If the authentication server does not return an address, the router allocates an address from this pool. The authentication server may override this pool name using RADIUS attributes such as Framed-Pool.
- Example

```
host1(config)#aaa domain-map westford.com
host1(config-domain-map)#address-pool-name poolA
```
- Use the **no** version to remove the address pool name.

ip address-pool

- Use to specify the addressing scheme: **dhcp**, **local**, or **none**.
- The addressing scheme **none** returns a special indicator to AAA that enables the remote PPP client to assign its own address.
- Example

```
host1(config)#ip address-pool dhcp
```
- Use the **no** version to specify the default, local.

ip local alias

- Use to create an alias for an existing local address pool. The IP address is allocated from the pool specified by the alias rather than from the pool specified in the IP address request.
- An alias name may contain up to 16 characters.
- You can configure a maximum of 32 aliases per virtual router.
- A local address pool can have multiple aliases.
- You can set the name of the alias to match the name of a local address pool; however, the two names used in the alias cannot be the same.
- You can modify an existing alias with a different local address pool name.
- When a local address pool is deleted, all aliases with the matching pool name are also deleted.
- Example

```
host1(config)#ip local alias groupB pool-name addrpool_10
```
- Use the **no** version to remove the alias name.

ip local pool

- Use to map an address pool name to a range of local addresses.
- You can create a pool with no address ranges configured for it.
- A name may contain up to 16 characters.
- Example

```
host1(config)#ip local pool addrpool_10 192.168.56.10 192.168.56.15
```
- Use the **no** version to remove the local pool (all ranges), or the specified range.

ip local pool snmpTrap

- Use to enable SNMP pool utilization traps.
- Example

```
host 1(config)#ip local pool addr_test snmpTrap
```
- Use the **no** version to disable SNMP pool utilization traps.

ip local pool warning

- Use to set SNMP utilization warning threshold values.
- Example

```
host1(config)#ip local pool addr_test warning 90 80
```
- Use the **no** version to reset the attributes to their default values; high threshold 85, abated threshold 75.

ip local shared-pool

- Use to create a local shared address pool and to specify the DHCP address pool that provides the addresses.
- You can reference a DHCP address pool that has not yet been configured.
- Example

```
host1(config)#ip local shared-pool sharedPool11 dhcpPool6
```
- Use the **no** version to delete a specific local shared address pool.

Configuring DHCP Features

DHCP provides a mechanism through which computers using Transmission Control Protocol/IP (TCP/IP) can obtain an IP address and protocol configuration parameters automatically from a DHCP server on the network.

The E-series router provides support for the following DHCP features:

- DHCP proxy client
- DHCP relay agent
- DHCP relay proxy
- DHCP local server
- DHCP external server

For more information about DHCP, see [Chapter 8, Configuring DHCP](#).

Creating an IP Interface

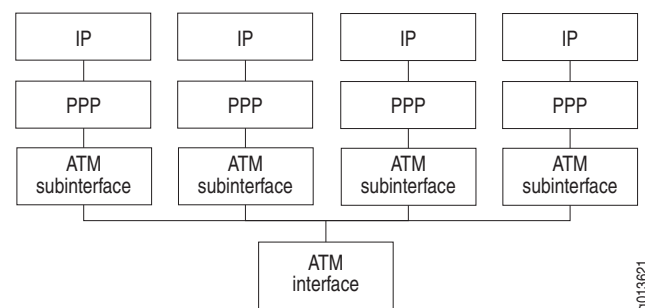
You can configure IP interfaces that support the following configurations:

- A single PPP client per ATM or Frame Relay subinterface
- Multiple PPP clients per ATM subinterface

Single Clients per ATM Subinterface

[Figure 3](#) shows a conceptual view of the configuration of a single PPP client per ATM subinterface.

Figure 3: Single PPP Clients per ATM Subinterface



Configure an ATM interface by entering Configuration mode and performing the following tasks. For more information about configuring ATM interfaces, see [JUNOS Link Layer Configuration Guide, Chapter 1, Configuring ATM](#).

1. Configure a physical interface.

```
host1(config)#interface atm 0/1
```

2. Configure the subinterface.

```
host1(config-if)#interface atm 0/1.20
```

3. Configure a permanent virtual circuit (PVC) by specifying the *vcd* (virtual circuit descriptor), the *vci* (virtual channel identifier), the *vpi* (virtual path identifier), and the encapsulation type.

```
host1(config-if)#atm pvc 10 22 100 aal5snap
```

4. Configure PPP encapsulation.

```
host1(config-if)#encapsulation ppp
```

5. Configure PAP or CHAP authentication.

```
host1((config-if))#ppp authentication chap
```

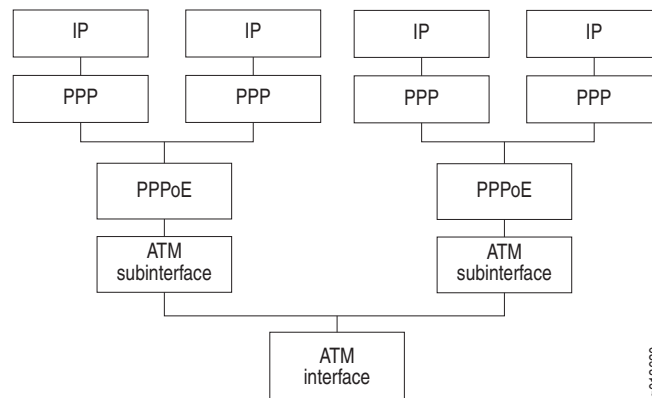
6. Assign a profile to the PPP interface.

```
host1(config-subif)#profile foo
```

Multiple Clients per ATM Subinterface

Figure 4 shows how PPPoE supports multiplexing of multiple PPP sessions per ATM subinterface.

Figure 4: Multiple PPP Clients per ATM Subinterface



Configure an ATM interface by entering Configuration mode and performing the following tasks. For more information about configuring ATM interfaces, see [JUNOS Link Layer Configuration Guide, Chapter 1, Configuring ATM](#).

1. Configure a physical interface.

```
host1(config)#interface atm 0/1
```

2. Configure the subinterface.

```
host1(config-if)#interface atm 0/1.20
```


3. Configure a PVC by specifying the *vcd* (virtual circuit descriptor), the *vci* (virtual channel identifier), the *vpi* (virtual path identifier), and the encapsulation type.

```
host1(config-if)#atm pvc 10 22 100 aal5snap
```

4. Configure PPPoE encapsulation.

```
host1(config-if)#encapsulation pppoe
```

5. Configure the subinterface for one PPP client.

```
host1(config-if)#interface atm 0/1.20.1
```

6. Configure PPP encapsulation.

```
host1(config-if)#encapsulation ppp
```

7. Configure PAP or CHAP authentication.

```
host1((config-if))#ppp authentication chap
```

8. Apply the profile to the PPP interface.

```
host1(config-subif)#profile foo2
```

9. Configure the subinterface for a second PPP client.

```
host1(config-if)#interface atm 0/1.20.2
```

10. Configure PPP encapsulation.

```
host1(config-if)#encapsulation ppp
```

11. Configure PAP or CHAP authentication.

```
host1((config-if))#ppp authentication chap
```

12. Apply the profile to the PPP interface.

```
host1(config-subif)#profile foo2
```

Configuring AAA Profiles

An AAA profile is a set of characteristics that act as a pattern that you can assign to domain names. Once you create an AAA profile, you can map it between a PPP client's domain name and certain AAA services on given interfaces. Using AAA profiles, you can:

- Allow or deny a domain name access to AAA authentication
- Map the original domain name to the mapped domain name for domain name lookup
- Use domain name aliases

- Force tunneling whenever a domain map contains tunnel attributes
- Manually set the NAS-Port-Type attribute (RADIUS attribute 61) for ATM and Ethernet interfaces
- Set the Service-Description attribute (RADIUS attribute 26-53)

An AAA profile contains a set of commands to control access for the incoming PPP subscriber. If no AAA profile is used, AAA continues as normal. The user's name and domain name are not changed as a result of an AAA profile mapping.



NOTE: There are two domain names with special meaning. The domain name **none** indicates that there is no domain name present in the subscriber's name. For more information about **none**, see the section [Mapping User Requests Without a Valid Domain Name](#) on page 7. The domain name **default** indicates that no other match occurs. For more information about **default**, see the section [Mapping User Requests Without a Configured Domain Name](#) on page 7.

Allowing or Denying Domain Names

You can control a PPP subscriber's access to certain domains on given interfaces. As the administrator, you can use the **deny** command to prevent PPP subscribers from using unauthorized domain names. Using the **allow** command, you can allow PPP subscribers to use authorized domain names.

Configuration Example

In this example, the administrator wants to restrict access of a PPP interface to the specific domain **abc.com**.

1. Create an AAA profile.

```
host1(config)#aaa profile restrictToABC
```

2. Specify the domain name you want to allow.

```
host1(config-aaa-profile)#allow abc.com
```

3. Specify the domain name you want to restrict.

```
host1(config-aaa-profile)#deny default
```

4. Associate the AAA profile to the designated PPP interface.

```
host1(config-if)#ppp aaa-profile restrictToABC
```

When configured as such, the following is a likely scenario:

- PPP passes the AAA profile **restrictToABC** to AAA in the authentication request.
- AAA performs the following:
 - Receives the authentication request from PPP with the subscriber's name **will@xyz.com**.

- Parses the domain name **xyz.com** and examines the specified AAA profile **restrictToABC**.
- Determines that the AAA profile **restrictToABC** is valid.
- Searches **restrictToABC** for a match on the PPP subscriber's domain name and finds no match.
- Searches **restrictToABC** for a match on the domain name **default**.
- Finds a match and denies the user access.

Using Domain Name Aliases

You can translate an original domain name to a new domain name via the **translate** command. The command allows you to create domain name aliases; that is, the grouping of multiple domain names into a single domain name. You can partition PPP subscribers with the same domain into separate domains, based on the PPP interface.



NOTE: Partitioning subscribers does not cause modification of a user's name or domain.

When you use aliases, you greatly simplify the configuration process. When there are a large number of domains and you use aliases, it reduces the configuration volume, thus requiring less NVS and memory usage.

Example 1 In this example, an administrator wants to associate all subscribers of a PPP interface with a specific domain name.

1. Create an AAA profile.

```
host1(config)#aaa profile forwardToXyz
```

2. Map the original domain name to the mapped domain name for domain map lookup.

```
host1(config-aaa-profile)#translate default xyz.com
```

3. Associate the AAA profile with the designated PPP interface.

```
host1(config-if)#ppp aaa-profile forwardToXyz
```

When configured as such, the following scenario is typical:

- PPP passes the AAA profile **forwardToXyz** to AAA in the authentication request.
- AAA performs the following tasks:
 - Receives the authentication request from PPP with the subscriber's name **morris@abc.com**.
 - Parses the domain name **abc.com** and examines the specified AAA profile **forwardToXyz**.

- Determines that the AAA profile **forwardToXyz** is valid.
- Searches **forwardToXyz** for a match on the PPP subscriber's domain name and finds no match.
- Searches **forwardToXyz** for a match on the domain name **default**.
- Finds a match and continues as normal using the domain name **xyz.com**.



NOTE: If there is no matching entry in the AAA profile for the user's domain name or for the domain name **default**, then AAA continues processing as if there were no AAA profile.

If the user's name does not contain a domain name, then AAA attempts to match to the domain name **none** in the AAA profile. If there is no entry for **none**, then AAA attempts to match for the domain name **default** in the AAA profile. If there is no entry for either **none** or **default**, then AAA continues processing as if there were no AAA profile.

Example 2 In this example, an administrator wants to use aliases; that is, to associate multiple domain names with a specific domain name and not allow other domain names.

1. Create an AAA profile.

```
host1(config)#aaa profile toAbc
```

2. Map the original domain name to the mapped domain name for domain map lookup.

```
host1(config-aaa-profile)#translate abc1.com abc.com
host1(config-aaa-profile)#translate abc2.com abc.com
host1(config-aaa-profile)#translate abc3.com abc.com
```

3. Specify the domain name you want to restrict.

```
host1(config-aaa-profile)#deny default
```

4. Associate the AAA profile with the designated PPP interface.

```
host1(config-if)#ppp aaa-profile toAbc
```

When configured as such, the following scenario is typical:

- PPP passes the AAA profile **toAbc** to AAA in the authentication request.
- AAA:
 - Receives the authentication request from PPP with the subscriber's name **jane@abc1.com**
 - Parses the domain name **abc1.com** and examines the specified AAA profile **toAbc**
 - Determines that the AAA profile **toAbc** is valid

- Searches **toAbc** for a match on the PPP subscriber's domain name and finds a match
- Continues as normal using the domain name **abc.com**



NOTE: If there is no matching entry in the AAA profile for the user's domain name or for the domain name **default**, then AAA continues processing as if there were no AAA profile.

If the user's name does not contain a domain name, then AAA attempts to match to the domain name **none** in the AAA profile. If there is no entry for **none**, then AAA attempts to match for the domain name **default** in the AAA profile. If there is no entry for either **none** or **default**, then AAA continues processing as if there were no AAA profile.

aaa profile

- Use to configure a new AAA profile.
- Example
host1(config)#**aaa profile boston123**
- Use the **no** version to delete the AAA profile.

allow

- Use to specify the domain name(s) that you want to be allowed access to AAA authentication.
- This command does not indicate that the user will be granted access; it is simply the first access point to AAA authentication.
- Using this command does not implicitly deny all other domains.
- Example
host1(config-aaa-profile)#**allow xyz.com**
- Use the **no** version to negate the command.

deny

- Use to specify the domain name(s) that you want to be denied access to AAA authentication.
- Example
host1(config-aaa-profile)#**deny xyz.com**
- Use the **no** version to negate the command.

ppp aaa-profile

- Use to assign an AAA profile to static and dynamic, multilink and nonmultilink PPP interfaces.
- The PPP application associates the AAA profile with the interface and passes the AAA profile to AAA for authentication.
- If an AAA profile is deleted after it has been assigned to an interface, AAA will deny the authentication and log a message.
- When you remove an AAA profile, it does not remove any corresponding bindings between PPP interfaces or interface profiles and the AAA profile. If an AAA profile with the same name is added, the interface cannot authenticate until the AAA profile is reassigned.



NOTE: Although an AAA profile and an interface profile have similar functionality, they are not related and should be treated differently.

- Example
host1(config-if)#**ppp aaa-profile westford24**
- Use the **no** version to remove the AAA profile assignment.

translate

- Use to map the original domain name to the mapped domain name for domain map lookup.
- This command allows you to group multiple domain names into a single domain name (that is, to use aliases).
- You can use this command to partition PPP subscribers with the same domain into separate domains, based on the PPP interface. By doing this, you do not cause modification of the user's name or domain.
- Example
host1(config-aaa-profile)#**translate abc.com xyz.com**
- Use the **no** version to negate the command.

Manually Setting NAS-Port-Type Attribute

You can manually configure the NAS-Port-Type RADIUS attribute (attribute 61) in AAA profiles for ATM and Ethernet interfaces. Doing so allows AAA profiles to determine the NAS port type for a given connection.

To set the NAS-Port-Type attribute for ATM or Ethernet interfaces:

1. Create an AAA profile.

```
host1(config)#aaa profile nasPortType
```

2. (Optional) Set the NAS-Port-Type attribute for ATM interfaces.

```
host1(config-aaa-profile)#nas-port-type atm wireless-80211
```

3. (Optional) Set the NAS-Port-Type attribute for Ethernet interfaces.

```
host1(config-aaa-profile)#nas-port-type ethernet wireless-cable
```

aaa profile

- Use to create and configure a AAA profile.
- Example

```
host1(config)#aaa profile nasPortType
```
- Use the **no** version to delete the AAA profile.

nas-port-type atm

- Use to specify the RADIUS NAS-Port-Type attribute (61) for ATM interfaces. You can set the attribute to:
 - *value*—Number in the range 0–65535
 - **adsl-cap**—Asymmetric DSL, carrierless amplitude phase (CAP) modulation
 - **adsl-dmt**—Asymmetric DSL, discrete multitone (DMT)
 - **cable**
 - **iapp**—Inter Access Point Protocol (IAPP)
 - **idsl**—ISDN DSL
 - **sdsl**—Symmetric DSL
 - **wireless-1x-ev**—Wireless 1xEV
 - **wireless-80211**—Wireless 802.11
 - **wireless-cdma**—Wireless code division multiple access (CDMA)
 - **wireless-other**
 - **wireless-umts**—Wireless universal mobile telecommunications system (UMTS)
 - **xdsl**—DSL of unknown type

- Example
`host1(config-aaa-profile)#nas-port-type atm wireless-80211`
- Use the **no** version to remove the NAS-Port-Type setting for ATM interfaces.

nas-port-type ethernet

- Use to specify the RADIUS NAS-Port-Type attribute (61) for Ethernet interfaces. You can set the attribute to:
 - *value*—Number in the range 0–65535
 - **cable**
 - **iapp**—IAPP
 - **wireless-1x-ev**—Wireless 1xEV
 - **wireless-80211**—Wireless 802.11
 - **wireless-cdma**—Wireless CDMA
 - **wireless-other**
 - **wireless-umts**—Wireless UMTS
- Example
`host1(config-aaa-profile)#nas-port-type ethernet wireless-80211`
- Use the **no** version to remove the NAS-Port-Type setting for Ethernet interfaces.

Service-Description Attribute

You can specify a service description that will be associated with an AAA profile. The description can then be exported through RADIUS by the Service-Description attribute (RADIUS attribute 26-53) in AAA profiles.

To set the Service-Description attribute:

1. Create the AAA profile.

```
host1(config)#aaa profile xyzCorpPro2
```

2. Set the Service-Description attribute.

```
host1(config-aaa-profile)#service-description bos-xyzcorp
```

aaa profile

- Use to create and configure a AAA profile.
- Example
`host1(config)#aaa profile xyzCorpPro2`
- Use the **no** version to delete the AAA profile.

service-description

- Use to specify a description that is associated with the AAA profile. The description can be transmitted to RADIUS in the Service-Description attribute (26-53)
- The service description can be a maximum of 64 characters.
- Example
`host1(config-aaa-profile)#service-description service11`
- Use the **no** version to remove the service description for the profile.

Using RADIUS Route-Download Server to Distribute Routes

The JUNOSe RADIUS route-download server provides periodic automatic distribution of IPv4 static access routes, which enables preconfiguration and preadvertising of access routes before they are assigned to clients. Using the route-download server helps eliminate routing protocol storms and other delays in client service activation that can be caused by protocol convergence or a large number of simultaneous customer activations.

The RADIUS route-download server periodically sends a RADIUS Access-Request message to the RADIUS server to request that routes be downloaded. The RADIUS server then responds with an Access-Accept message and downloads the configured routes. When the download operation is complete, the route-download server installs the access routes in the routing table.

JUNOSe software supports the creation of one RADIUS route-download server per chassis.

Format of Downloaded Routes

The RADIUS server sends the downloaded routes to the RADIUS route-download server in the following format:

```
[ { vir | virtual-router } virtualRouterName ] [ vrf vrfName ] prefix-mask [ { null0 | null 0 }
[ cost ] ] [ tag tagValue ]
```

The route-download server accepts downloaded routes in either the Framed-Route attribute (RADIUS attribute 22) or the Cisco-AVpair attribute (Cisco VSA 26-1).

Downloaded Route Format Examples

Framed-Route (RADIUS attribute 22)

```
NAS-1 Password = "14raddlsvr" User-Service-Type = Outbound-User
Framed-Route = "192.168.3.0 255.255.255.0 null0"
Framed-Route = "vrf vrfboston 192.168.1.0/24 null 0 0 tag 6"
Framed-Route = "vir host1 vrf vrf sunny 192.168.0.0/16 null0 0 tag 8"
```

Cisco-AVPair (Cisco VSA 26-1)

```
NAS-1 Password = "14raddlsvr" User-Service-Type = Outbound-User
cisco-avpair = "ip:route = 192.168.3.0 255.255.255.0 null0"
cisco-avpair = "ip:route = vrf vrfboston 192.168.1.0/24 null 0 0 tag 6"
cisco-avpair = "ip:route = vir host1 vrf vrf sunny 192.168.0.0/16 null0 0 tag 8"
```



NOTE: The prefix-mask entry in downloaded routes can be in the form of prefix length, prefix mask, or prefix. If prefix is used, the mask is determined by the IP address class of the prefix.

How the Route-Download Server Downloads Routes

The route-download server starts the initial route-download operation (for example, after a system reboot or the first time the route-download server is enabled) as soon as IP is established in the virtual router in which the download is performed. After the initial route-download process is established, the router repeats the route download operation based on either the default download schedule or the schedule you specify. You can also initiate an immediate route download at any time.

The RADIUS route-download server downloads routes in two stages—first, all routes are downloaded from the RADIUS server to the router's download database and examined for errors. Next, the router updates the routing table with the new routes, using the following guidelines:

- Adds all downloaded routes that are not already installed in the routing table
- Does not add downloaded routes that are already installed in the routing table
- Deletes routes from the routing table that do not appear in the newly downloaded group

Configuring the Route-Download Server to Download Routes

When you configure the E-series router as a route-download server, you specify the RADIUS server that you want to download the routes to your router. You can also modify the route-download server's default configuration parameters, such as when to start the download process each day, how often to download routes, and how long to wait after a download error before retrying the process.

To configure a RADIUS route-download server:

1. Specify the IP address and the key of the RADIUS server that you want to download routes.

```
host1(config)#radius route-download server 192.168.1.17
host1(config-radius)#key 35radsrv92
```

2. (Optional) Specify the UDP port used for RADIUS route-download server requests.

```
host1(config-radius)#udp-port 1812
host1(config-radius)#exit
host1(config)#
```

3. Enable the route-download feature and optionally modify default parameters as needed.

```
host1(config)#aaa route-download 1200 retry-interval 25 password dl1456atl
synchronization 03:45:00
```

4. (Optional) Verify your route-download configuration:

```

host1(config)#exit
host1#show aaa route-download

AAA Route Downloader:      configured in virtual router default
Download Interval:         1200 minutes
Retry Interval:            25 minutes
Default Cost:              2
Default Tag:               0
Base User Name:            <HOSTNAME>
Password:                  d11456at1
Synchronization:          03:45:00

Status:                    downloading
Last Download Attempt:     TUE FEB 9 22:07:30 2007
Last Download Success:     <NEVER>
Last Regular Download:     not complete
Next Download Scheduled:   <DOWNLOAD ACTIVE>
Next Regular Download:     WED FEB 9 22:27:00 2007

```

aaa route-download

- Use to enable the RADIUS route-download server on the router and to configure parameters for the server. You can configure the following parameters:
 - **download interval**—The amount of time the route-download server waits between route download operations. The newly created server downloads routes as soon as the IP protocol is active on the virtual router that performs the route download operation, and then repeats the download operation every 720 minutes by default. You can set a download interval in the range 1–1440 minutes.
 - **retry-interval**—The amount of time the server waits after a download failure before attempting another route download. You can set the retry interval in the range 1–60 minutes. The default interval is 10 minutes.



NOTE: If the download interval is less than the retry interval, the server ignores the retry interval setting.

- **cost**—The cost of a downloaded route. You can specify a cost in the range 1–254. The default cost is 2.
- **tag**—The tag assigned to a downloaded route. You can specify a tag in the range 1–4294967295. The default tag is 0.
- **base-user-name**—The virtual router that is used for route-download requests. The default name is the router hostname.
- **password**—The password used in RADIUS Access-Request messages for route-download requests. You can specify from 1 through 32 alphanumeric characters. The default password is juniper.
- **synchronization**—The time that the server starts the route download operation each day. You specify the time in 24-hour format, for example 03:45:00.

- Example

```
host1(config)#aaa route-download 1200 retry-interval 25 password dl1456atl
synchronization 03:45:00
```

- Use the **no** version to disable the route-download server.

aaa route-download now

- Use to specify that the RADIUS route-download server immediately restart the route download operation.
- If a download is currently in progress when you issue this command without the **force** keyword, the in-progress download continues until complete. No additional download is started.
- Use the **force** keyword to start an immediate download; a currently running download is interrupted. The download is not retried if it fails.
- Use the **adjust-scheduler** keyword to restart the configured download interval from the time of this download. However, if the download fails, the download interval is not changed and the download is not retried.
- Example

```
host1#aaa route-download now force adjust-scheduler
```
- There is no **no** version.

aaa route-download suspend

- Use to temporarily suspend the RADIUS route-download server operation.
- Example

```
host1#aaa route-download suspend
```
- Use the **no** version to restore the route download operation.

clear ip routes download

- Use to synchronize downloaded access routes and the routes that are installed in the routing tables of virtual routers.
- Use the following options to synchronize downloaded routes for a specific virtual router:
 - Specify a particular VRF whose downloaded routes you want synchronized. If you do not specify an optional VRF, the current virtual router is used.
 - Specify the IP address and IP mask that identifies the subset of downloaded routes that you want cleared in the routing table of the current virtual router or in the specified VRF.
 - Use the wildcard character (*) to clear all downloaded routes in the routing table of the current virtual router or in the specified VRF.

- Use the following keywords to perform global clearing operations:
 - **all**—Clears all downloaded routes from all virtual routers and VRFs.
 - **reload**—Initiates a download of routes and then clear the routes from the routing table of all virtual routers and VRFs.



NOTE: Clear commands fail if the route-download server is in the process of downloading routes from the RADIUS server.

- Example 1—Clear all downloaded routes from the current virtual router
`host1#clear ip routes download *`
- Example 2—Clear a subset of routes from a specific VRF
`host1#clear ip routes download vrf NY12 192.168.50.102 255.255.0.0`
- Example 3—Clear all downloaded routes from all virtual routers and VRFs
`host1#clear ip routes download all`
- There is no **no** version.

radius route-download server

- Use to configure a RADIUS route-download server and enter RADIUS Configuration mode. Specify the IP address of the RADIUS server that you want to download access routes.



NOTE: When the RADIUS route-download server is enabled, the router ignores the **radius rollover-on-reject enable** command—the **radius rollover-on-reject enable** command has no effect for a RADIUS route-download server.

- You can configure a single instance of the route downloader on the router.
- Example

```
host1(config)#radius route-download server 10.10.5.10
host1(config-radius)#
```
- Use the **no** version to delete the instance of the RADIUS route-download server.

Using the AAA Logical Line Identifier to Track Subscribers

You can configure the router to support the AAA logical line identification feature. This feature enables service providers to track subscribers on the basis of a virtual port known as the logical line ID (LLID).

The LLID is an alphanumeric string that logically identifies a subscriber line. The service provider maps each subscriber to an LLID based on the user name and circuit ID from which the customer's calls originate. When a subscriber moves to a new physical line, the service provider's customer profile database is updated to map to the same LLID.

Because a subscriber's LLID remains the same regardless of the subscriber's physical location, using the LLID gives service providers a more secure mechanism for tracking subscribers and maintaining the customer database.

How the Router Obtains and Uses the LLID

To obtain an LLID for a subscriber, the router must issue two RADIUS access requests: a preauthentication request to obtain the LLID, followed by an authentication request encoded with the LLID returned in response to the preauthentication request.

To configure this feature, you:

1. Create an AAA profile that supports preauthentication (by using the **pre-authenticate** command in AAA Profile Configuration mode).
2. Specify the IP address of a RADIUS preauthentication server (by using the **radius pre-authentication server** command in Global Configuration mode) and of an authentication server (by using the **radius authentication server** command in Global Configuration mode).

The following steps describe how the router uses RADIUS to obtain and use the LLID. It is assumed that you have already configured an AAA profile for preauthentication and have defined both a RADIUS preauthentication server and a RADIUS authentication server. Typically, the preauthentication server and the authentication server reside in the same virtual router context in which the PPP subscriber is authenticated.

The router obtains and uses the LLID as follows:

1. A PPP subscriber requests authentication through RADIUS.
2. The router sends an Access-Request message to the RADIUS preauthentication server to obtain an LLID for the subscriber.

This step is referred to as the preauthentication request because it occurs before user authentication and authorization.

3. The preauthentication server returns the LLID to the router in the Calling-Station-Id (RADIUS attribute 31) of an Access-Accept message.

The router ignores any RADIUS attributes other than the Calling-Station-Id that are returned in the preauthentication Access-Accept message.

4. The router encodes the LLID in the RADIUS Calling-Station-Id and sends an Access-Request message to the RADIUS authentication server.

This step is referred to as the authentication request.

5. The RADIUS authentication server returns an Access-Accept message to the router that includes the tunnel attributes for the subscriber session.
6. For tunneled PPP subscribers, the router, acting as an L2TP access concentrator (LAC), encodes the LLID into L2TP Calling Number AVP 22 and sends this to the L2TP network server (LNS) in an incoming-call request (ICRQ) packet.

After a successful preauthentication request, the router always encodes the LLID in Calling Number AVP 22. The use of **aaa** commands such as **aaa tunnel calling-number-format** to control or change the inclusion of the LLID in Calling Number AVP 22 has no effect.

RADIUS Attributes in Preauthentication Request

Table 5 describes the RADIUS IETF attributes that are always included in a preauthentication request to obtain the LLID. The attributes are listed in ascending order by standard number.

Table 5: RADIUS IETF Attributes in Preauthentication Request

Attribute Number	Attribute Name	Description
[1]	User-Name	Name of the user associated with the LLID, in the format: NAS-Port: < NAS-IP-Address > : < Nas-Port-Id > For example, nas-port:172.28.30.117:atm 4/1.104:2.104
[2]	User-Password	Password of the user to be authenticated; always set to “juniper”
[4]	NAS-IP-Address	IP address of the network access server (NAS) that is requesting authentication of the user; for example, 172.28.30.117
[5]	NAS-Port	Physical port number of the NAS that is authenticating the user; this is always interpreted as a bit field
[6]	Service-Type	Type of service the user has requested or the type of service to be provided; for example, framed
[61]	NAS-Port-Type	Type of physical port the NAS is using to authenticate the user
[77]	Connect-Info	Actual user name; for example, jdoe@xyzcorp.east.com
[87]	NAS-Port-Id	Text string that identifies the physical interface of the NAS that is authenticating the user; for example, atm 4/1.104:2.104

The use of **radius** commands such as **radius calling-station-format** or **radius override calling-station-id** to control or change the inclusion of these attributes in the preauthentication request has no effect.

For more information about these attributes, see *Appendix A, RADIUS Attribute Descriptions*.

Considerations for Using the LLID

The following considerations apply when you configure the router for subscriber preauthentication:

- Only PPP subscribers authenticating through RADIUS can use the AAA LLID feature on the router. PPP subscribers tunneled through domain maps cannot take advantage of this feature.
- The Calling-Station-Id [31] attribute is typically sent in RADIUS Access-Request messages, not in Access-Accept messages as is the case for this feature. As a result, your RADIUS server might require special configuration procedures to enable the Calling-Station-Id attribute to be returned in Access-Accept messages. See the documentation that came with your RADIUS server for information.
- The router ignores any RADIUS attributes other than the Calling-Station-Id that are returned in the preauthentication Access-Accept message.
- If a preauthentication request fails due to misconfiguration of the preauthentication server, timeout of the preauthentication server, or rejection of the preauthentication request by the preauthentication server, the authentication process continues normally and the preauthentication request is ignored.
- The router preserves the LLID value for established subscribers after a stateful SRP switchover.
- The **radius rollover-on-reject enable** command has no effect for a RADIUS preauthentication server. That is, you cannot use the **radius rollover-on-reject enable** command to configure the router to roll over to the next RADIUS preauthentication server when the router receives an Access-Reject message for the user it is authenticating. For information, see [radius rollover-on-reject](#) on page 29.

Configuring the Router to Obtain the LLID for a Subscriber

To configure the router to obtain the LLID for a subscriber:

1. Create an AAA profile that supports subscriber preauthentication.

```
host1(config)#aaa profile preAuthLlid
host1(config-aaa-profile)#pre-authenticate
host1(config-aaa-profile)#exit
```

2. Define a RADIUS preauthentication server.

```
host1(config)#radius pre-authentication server 10.10.10.1
host1(config-radius)#key abc123
host1(config-radius)#exit
```

3. Associate the AAA profile with the designated PPP interface.

```
host1(config)#interface atm 4/3.101
host1(config-subif)#ppp aaa-profile preAuthLlid
```


- (Optional) Verify that preauthentication support is configured for the AAA profile.

```
host1(config-subif)#run show aaa profile name PreAuthL1id
preAuthL1id:
  atm nas-port-type: ADSL-CAP
  ethernet nas-port-type: Cable
  profile-service-description: xyzService
  pre-authenticate
  allow xyz.com
  deny default
  translate xyz1.com abc.com
```

For information, see [show aaa profile](#) on page 93.

- (Optional) Verify configuration of the RADIUS preauthentication server.

```
host1(config-subif)#run show radius pre-authentication servers
```

RADIUS Pre-Authentication Configuration						
IP Address	Udp Port	Retry Count	Timeout	Maximum Sessions	Dead Time	Secret
10.10.10.1	1812	3	3	255	0	radius

You can also display configuration information for preauthentication servers by using the **show radius servers** command. For information, see [show radius servers](#) on page 109.

- (Optional) Display statistics for the RADIUS preauthentication server.

To display preauthentication statistics, use the **show radius pre-authentication statistics** command. For information, see [show radius statistics](#) on page 110.

To display a count of preauthentication requests and responses, use the **show aaa statistics** command. For information, see [show aaa statistics](#) on page 97.

aaa profile

- Use to configure a new AAA profile.
- Example
host1(config)#aaa profile boston123
- Use the **no** version to delete the AAA profile.

key

- Use from RADIUS Configuration mode to configure the secret for a RADIUS preauthentication server.
- The server secret is a text string used by RADIUS to encrypt the client and server authenticator field during exchanges between the router and a RADIUS preauthentication server. The router encrypts PPP PAP passwords using this text string.
- The default behavior is no server secret.

- Example
host1(config-radius)#**key gismo**
- Use the **no** version to remove the secret.



NOTE: The preauthentication request fails if you do not specify a key for the preauthentication server.

ppp aaa-profile

- Use to assign an AAA profile to static and dynamic, multilink and nonmultilink PPP interfaces.
- For more information about how to use this command, see [ppp aaa-profile](#) on page 62.
- Example
host1(config-if)#**ppp aaa-profile preAuth**
- Use the **no** version to remove the AAA profile assignment.

pre-authenticate

- Use to configure an AAA profile to support RADIUS preauthentication.
- During preauthentication, the router sends an Access-Request message to a RADIUS preauthentication server to obtain an LLID for a subscriber. In response, the preauthentication server returns the LLID in the RADIUS Calling-Station-Id [31] attribute of an Access-Accept message.
- Example
host1(config-aaa-profile)#**pre-authenticate**
- Use the **no** version to remove preauthentication support from the AAA profile.

radius pre-authentication server

- Use to specify the IP address of a RADIUS preauthentication server.
- This command accesses RADIUS Configuration mode, from which you can configure additional parameters for the RADIUS preauthentication server.
- Example
host1(config)#**radius pre-authentication server 10.10.10.2**
- Use the **no** version to delete the instance of the RADIUS preauthentication server.

Troubleshooting Subscriber Preauthentication

You can configure the router to send traps to SNMP when a RADIUS preauthentication server fails to respond to messages. To do so, you use the same procedure and commands as you do to configure SNMP traps for a RADIUS authentication server.

For example, to enable SNMP traps when a particular RADIUS preauthentication server fails to respond to Access-Request messages, use the **radius trap auth-server-not-responding enable** command.

For more information, see [Configuring SNMP Traps](#) on page 34.

Using VSAs for Dynamic IP Interfaces

[Table 6](#) describes the VSAs that apply to dynamic IP interfaces and are supported on a per-user basis from RADIUS. For details, see [JUNOS Link Layer Configuration Guide, Chapter 13, Configuring Dynamic Interfaces Using Bulk Configuration](#).

Table 6: VSAs That Apply to Dynamic IP Interfaces

VSA	Description	Type	Length	Subtype	Subtype Length	Value
Ingress-Policy-Name	Specifies the name of the input (ingress) policy	26	len	10	sublen	string: <i>input-policy-name</i>
Egress-Policy-Name	Specifies the name of the output (egress) policy	26	len	11	sublen	string: <i>output-policy-name</i>
Ingress-Statistics	Indicates whether statistics are collected on input	26	12	12	6	integer: 0 – disable, 1 – enable
Egress-Statistics	Indicates whether statistics are collected on output	26	12	13	6	integer: 0 – disable, 1 – enable
QoS-Profile-Name	Specifies the name of the QoS profile to attach to the interface	26	len	26	sublen	string: <i>qos-profile-name</i>

To use the VSAs shown in [Table 6](#):

- Specify the policy, or one or more QoS VSAs in the desired RADIUS user entries.
- Create the ingress or egress policy, or the QoS profile. Policies minimally consist of one or more policy commands and may include classifier control lists and rate limit profiles. See the [JUNOS Policy Management Configuration Guide](#) for more information about policies and policy routing. See the [JUNOS Quality of Service Configuration Guide](#) for information about creating QoS profiles.

When a dynamic interface is created according to a profile, the router checks with RADIUS to determine whether an input or output policy or a QoS profile must be applied to the interface. The VSA, if present, provides the name, enabling policy or QoS profile lookup. If found, the policy or QoS profile is applied to the dynamic interface.

The router also determines whether the creation profile specifies any policies to be applied to the interface. Policies specified by the RADIUS VSA supersede any specified by the profile, as described in the following example:

The RADIUS user entry includes an Ingress-Policy-Name VSA that specifies the policy input5. The profile specifies two policies, input7 and output1. In this case, the RADIUS-specified input policy (input5) and the profile-specified output policy (output1) are applied to the dynamic interface.

For information about assigning policies via profiles, see the [JUNOS Policy Management Configuration Guide](#). Only attributes assigned by RADIUS appear in RADIUS Acct-Start messages. RADIUS attributes specified by a profile for dynamic interfaces do not appear in RADIUS Acct-Start messages because the profile is not active when the Acct-Start message is generated. These attributes appear in RADIUS Acct-Stop messages for a profile that is active when the session is terminated.

Traffic Shaping for PPP over ATM Interfaces

The router supports the configuration of traffic shaping parameters for PPP over ATM (PPPoA) via domain-based profiles and RADIUS. In connection with this feature, [Table 7](#) describes VSAs that apply to dynamic IP interfaces and are supported on a per-user basis from RADIUS.

Table 7: Traffic-Shaping VSAs That Apply to Dynamic IP Interfaces

VSA	Description	Type	Length	Subtype	Subtype Length	Value
Service-Category	Specifies the type of service	26	12	14	6	integer: 1 – UBR 2 – UBR PCR 3 – NRT VBR 4 – CBR 5 – RT VBR
PCR	Specifies the value for the peak cell rate (PCR)	26	12	15	6	integer
SCR	Specifies the value for the sustained cell rate (SCR)	26	12	16	6	integer
MBS	Specifies the maximum burst size (MBS)	26	12	17	6	integer

To configure traffic-shaping parameters for PPPoA via domain maps, use the **atm** command in Domain Map Configuration mode.

atm

- Use to configure traffic-shaping parameters for PPPoA.
- Use one of the following keywords to select the traffic category to configure:
 - **ubr**—Unspecified bit rate
 - **ubrpqr**—Unspecified bit rate with peak cell rate
 - **nrtvbr**—Non-real time variable bit rate
 - **rtvbr**—Real time variable bit rate
 - **cbr**—Constant bit rate

- Example

```
host1(config)#aaa domain-map atmTraffic
host1(config-domain-map)#atm rtvbr 3897832145 3597861230 4294967295
```

- Use the **no** version to remove the traffic-shaping configuration.

Mapping Application Terminate Reasons to RADIUS Terminate Codes

The JUNOS software uses a default configuration that maps terminate reasons to RADIUS Acct-Terminate-Cause attributes. You can optionally create customized mappings between a terminate reason and a RADIUS Acct-Terminate-Cause attribute—these mappings enable you to provide different information about the cause of a termination.

When a subscriber's L2TP or PPP session is terminated, the router logs a message for the internal terminate reason and logs another message for the RADIUS Acct-Terminate-Cause attribute (RADIUS attribute 49). RADIUS attribute 49 is also included in RADIUS Acct-Off and Acct-Stop messages. You can use the logged information to help monitor and troubleshoot terminated sessions.

Use the **show terminate-code** command to display information about the mappings between application terminate reasons and RADIUS Acct-Terminate-Cause attributes.

[Table 8](#) lists the IETF RADIUS Acct-Terminate-Cause codes that you can use to map application terminate reasons. In addition, you can also configure and use proprietary codes for values beyond 22.

Table 8: Supported RADIUS Acct-Terminate-Cause Codes

Code	Name	Description
1	User Request	User initiated the disconnect (log out)
2	Lost Carrier	DCD was dropped on the port
3	Lost Service	Service can no longer be provided; for example, the user's connection to a host was interrupted
4	Idle Timeout	Idle timer expired
5	Session Timeout	Subscriber reached the maximum continuous time allowed for the service or session
6	Admin Reset	System administrator reset the port or session
7	Admin Reboot	System administrator terminated the session on the NAS; for example, prior to rebooting the NAS
8	Port Error	NAS detected an error on the port that required ending the session
9	NAS Error	NAS detected an error (other than on the port) that required ending the session
10	NAS Request	NAS ended the session for a non-error reason
11	NAS Reboot	NAS ended the session due to a non-administrative reboot
12	Port Unneeded	NAS ended the session because the resource usage fell below the low threshold; for example, the bandwidth-on-demand algorithm determined that the port was no longer needed

Table 8: Supported RADIUS Acct-Terminate-Cause Codes (continued)

Code	Name	Description
13	Port Preempted	NAS ended the session to allocate the port to a higher-priority use
14	Port Suspended	NAS ended the session to suspend a virtual session
15	Service Unavailable	NAS was unable to provide the requested service
16	Callback	NAS is terminating the current session in order to perform callback for a new session
17	User Error	An error in the user input caused the session to be terminated
18	Host Request	The login host terminated the session normally
19	Supplicant Restart	Supplicant state machine was reinitialized
20	Reauthentication Failure	A previously authenticated supplicant failed to reauthenticate successfully following expiration of the reauthentication timer or explicit reauthentication request by management action
21	Port Reinitialized	The port's MAC has been reinitialized
22	Port Administratively Disabled	The port has been administratively disabled

Configuration Example

This example describes a sample configuration procedure that creates custom mappings for PPP terminate reasons.

1. Configure the router to include the Acct-Terminate-Cause attribute in RADIUS Acct-Off messages.

```
host1(config)#radius include acct-terminate-cause acct-off enable
```

2. (Optional) Display the current PPP terminate-cause mappings.

```
host1(config)#run show terminate-code ppp
```

Apps	Terminate Reason	Description	Radius Code
-----	-----	-----	-----
ppp	authenticate-authenticator-timeout	authenticate authenticator timeout	17
ppp	authenticate-challenge-timeout	authenticate challenge timeout	10
ppp	authenticate-chap-no-resources	authenticate chap no resources	10
ppp	authenticate-chap-peer-authenticator-timeout	authenticate chap peer authenticator timeout	17
ppp	authenticate-deny-by-peer	authenticate deny by peer	17
ppp	authenticate-inactivity-timeout	authenticate inactivity timeout	4
--More--			

3. (Optional) Display all PPP terminate reasons.

```
host1(config)#terminate-code ppp ?
  authenticate-authenticator-timeout      Configure authenticate
                                           authenticator timeout
                                           translation
  authenticate-challenge-timeout          Configure authenticate
                                           challenge timeout translation
  authenticate-chap-no-resources           Configure authenticate chap no
                                           resources translation
  authenticate-chap-peer-authenticator-timeout Configure authenticate chap
                                           peer authenticator timeout
                                           translation
  authenticate-deny-by-peer               Configure authenticate deny by
                                           peer translation
--More--
```

4. Configure your customized PPP terminate-cause to RADIUS
Acct-Terminate-Cause code mappings.

```
host1(config)#terminate-code ppp authenticate-authenticator-timeout radius 3
host1(config)#terminate-code ppp authenticate-challenge-timeout radius 4
```

5. Verify the new terminate-cause mappings.

```
host1(config)#run show terminate-code ppp
```

Apps	Terminate Reason	Description	Radius Code
ppp	authenticate-authenticator-timeout	authenticate authenticator timeout	3
ppp	authenticate-challenge-timeout	authenticate challenge timeout	4
ppp	authenticate-chap-no-resources	authenticate chap no resources	10
ppp	authenticate-chap-peer-authenticator-timeout	authenticate chap peer authenticator timeout	17
ppp	authenticate-deny-by-peer	authenticate deny by peer	17
ppp	authenticate-inactivity-timeout	authenticate inactivity timeout	4
ppp	authenticate-max-requests	authenticate max requests	10

--More--

radius include acct-terminate-cause

- Use to include the Acct-Terminate-Cause attribute (RADIUS attribute 49) in RADIUS Acct-Off messages.
- You control inclusion of the Acct-Terminate-Cause attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include acct-terminate-cause acct-off disable
```

- Use the **no** version to restore the default, enable.

terminate-code

- Use to configure a customized mapping relationship between an application's terminate reason and a RADIUS Acct-Terminate-Cause code (RADIUS attribute 49).
- To set up the mapping, specify the following variables with this command:
 1. Specify the application where the terminate event occurs. You can specify **aaa**, **l2tp**, **ppp**, or **radius-client**.
 2. Specify the application's terminate reason that you want to map.
 - Use the question mark character (?) to display a list of the application's terminate reasons. For example:


```
host1(config)#terminate-code l2tp ?
```
 - See *Appendix C, Application Terminate Reasons* for a list of the default terminate reasons for the AAA, L2TP, PPP, and RADIUS client applications.
 3. Specify RADIUS as the translation application that is used for mapping. Then, specify the RADIUS Acct-Terminate-Cause code that you want to map to the application's terminate reason. See [Table 8 on page 77](#) for a list of supported RADIUS codes.
- Example


```
host1(config)#terminate-code ppp authenticate-challenge-timeout radius 4
```
- Use the **no** version to restore a default mapping, which are listed in *Appendix C, Application Terminate Reasons*. For example:


```
host1(config)#no terminate-code aaa deny-address-allocation-failure radius
```

Configuring Timeout

You can configure an idle or a session timeout. The values you set are the default values for PPP B-RAS users. Attributes returned by RADIUS override these default settings on a per-user basis.

aaa timeout

- Use to set either an idle or a session timeout.
- The range in seconds for an idle timeout is 300–7200.
- The range in seconds for a session timeout is a minimum of 1 minute (60 seconds) through a maximum of 366 days (31622400 seconds).
- These values can also be set by RADIUS, where the range is not enforceable. PPP and L2TP will round the timeout values from RADIUS as follows:
 - If the session timeout is less than the minimum (60 seconds), that value is used.
 - If the idle timeout is less than the minimum (300 seconds), it is rounded up to the minimum.

- If either timeout is greater than the maximum, it is rounded down to the maximum.
- All other timeouts are rounded to the nearest minute.
- Example 1
host1(config)#**aaa timeout idle 1200**
- Example 2
host1(config)#**aaa timeout session 3600**
- For a session timeout, the router interprets the default value (indicated by **0**) to mean that the PPP or L2TP user session should be forced to the maximum session timeout, 366 days. This means that the duration of a PPP or an L2TP user session cannot exceed 366 days; once the maximum session timeout is reached, the router terminates the user session.
- Use the **no** version to restore the idle or session timeout to its default value, 0 (seconds).

Limiting Active Subscribers

You can limit the number of active subscribers on a port or virtual router.

aaa subscriber limit per-port

- Use to limit the number of active subscribers permitted on a port.
- Example
host1(config)#**aaa subscriber limit per-port 2/0 20**
- Use the **no** version to return to the default value, 0 (zero).

aaa subscriber limit per-vr

- Use to limit the number of active subscribers permitted on a virtual router.
- Because profiles are applied to subscribers after the PPP authentication phase, subscribers that have their VR context specified by profiles are not denied access. Instead, when IP notifies AAA of the subscribers VR context, AAA checks limits. If the subscriber exceeds the VR limit, AAA revokes the subscriber's access and logs out the subscriber.
- Example
host1:vr17(config)#**aaa subscriber limit per-vr 20**
- Use the **no** version to return to the default value, 0 (zero).

Notifying RADIUS of AAA Failure

If a user passes RADIUS authentication, but fails AAA authentication, the RADIUS server may still allocate an address for the user from its internal address pool. To indicate to the RADIUS server to free the address, you can set up the router to send an Acct-Stop message if a user fails AAA.

aaa accounting acct-stop on-aaa-failure

- Use to cause the router to send an Acct-Stop message if a user fails AAA, but RADIUS grants access.
- Example

```
host1:vr17(config)#aaa accounting acct-stop on-aaa-failure disable
```
- Use the **no** version to return to the default value, enabled.

aaa accounting acct-stop on-access-deney

- Use to cause the router to issue an Acct-Stop message if RADIUS denies access.
- Example

```
host1:vr17(config)#aaa accounting acct-stop on-access-deney enable
```
- Use the **no** version to return to the default value, disabled.

Configuring the SDX Client

The JUNOS software has an embedded client that interacts with the Juniper Networks SDX application, enabling the SDX application to manage the router's policy and QoS configuration.

The connection between the router and the SDX application uses the Common Open Policy Service (COPS) protocol and is fully compliant with the COPS usage for policy provisioning (COPS-PR) specification. The router's SDX client functions as the COPS client, or policy enforcement point (PEP). The SDX application functions as the COPS server, or policy decision point (PDP).

[Table 9](#) provides common terms used in the COPS environment.

Table 9: SDX Client and COPS Terminology

Term	Description
COPS	Common Open Policy Service; query-and-response protocol used to exchange policy information between a policy server and its clients.
COPS-PR	COPS usage for policy provisioning; the PEP requests policy provisioning when the operational state of interface and DHCP addresses changes.
PDP	Policy decision point; the COPS server, which makes policy decisions for itself and for clients that request decisions. The SDX application is the PDP.
PEP	Policy enforcement point; the COPS client, which enforces policy decisions. The JUNOS COPS interface is a PEP.
PIB	Policy Information Base; a collection of sets of attributes that represent configuration information for a device.

Table 9: SDX Client and COPS Terminology (continued)

Term	Description
SDX	Service Deployment System; functions as a COPS PDP.
XDR	External Data Representation Standard; a standard for the description and encoding of data. XDR can be used to transfer data between computers.

The JUNOS software's COPS-PR implementation uses the outsourcing model that is described in RFC 3084. In this model, the PEP delegates responsibility to the PDP to make provisioning decisions on the PEP's behalf.

The provisioning is event-driven and is based on policy requests rather than on an action taken by an administrator—the provisioning is initiated when the PDP receives external requests and PEP events. Provisioning can be performed in bulk (for example, an entire QoS configuration) or in smaller segments (for example, updating a marking filter). The following list shows the interaction between the PEP and the PDP during the COPS-PR operation.

1. Initial connection
 - a. PEP starts the COPS-PR connection with the PDP.
 - b. PDP requests synchronization.
 - c. PEP sends all currently provisioned policies to PDP.
2. Change of interface state
 - a. PEP requests provisioning of an interface from the PDP.
 - b. PDP determines policies and sends provisioning data to the PEP.
 - c. PEP provisions the policies.
3. PDP requests policy provisioning
 - a. PDP determines new policies and sends provisioning data to the PEP.
 - b. PEP provisions the policies.

The information exchange between the PDP and PEP consists of data that is modeled in Policy Information Bases (PIBs) and is encoded using the standard ASN.1 basic encoding rules (BERs). The JUNOS software's COPS-PR support uses a proprietary PIB. The proprietary PIB consists of a series of tables designed to replicate and enhance the XDR functionality that is supported in previous JUNOS software releases, including the proprietary accounting and address assignment mechanisms. The XDR-encoded commands for the SDX application continue to be supported.

The proprietary PIB provides the Policy Manager and QoS Manager functionality shown in the following lists.

- Policy Manager
 - Committed access rate
 - Packet filtering
 - Policy routing
 - QoS classification and marking
 - Rate limiting
 - Traffic class
- QoS Manager
 - Queues
 - Schedulers
 - Traffic classes

You can configure SDX clients on a per-virtual-router basis. To configure the SDX client:

1. Enable the SDX client. With the CLI **sscc enable** command you can specify either BER-encoded information exchange for COPS-PR or XDR exchange for COPS.

```
host1(config)#sscc enable cops-pr
```

2. Specify the IP addresses of up to three SDX servers (primary, secondary, and tertiary). You can optionally specify the port on which the servers listen for activity.

```
host1(config)#sscc primary address
host1(config)#sscc secondary address 192.168.12.1 port 3288
```

3. (Optional) Enable policy and QoS configuration support for IPv6 interfaces.

```
host1(config)#sscc protocol ipv6
```

4. (Optional) Specify on which router the TCP/COPS connection is to be established.

```
host1(config)#sscc transportRouter chicago
```

5. (Optional) Specify a fixed source address for the TCP/COPS connection created for an SDX client session.

```
host1(config)#sscc sourceAddress 10.9.123.8
```

6. (Optional) Specify a fixed source interface for the TCP/COPS connection.

```
host1(config)#sscc sourceInterface atm 3/0
```

7. (Optional) Specify the delay period during which the SDX client waits for a response from the SDX server.

```
host1(config)#sscc retryTimer 120
```

sscc address

- Use to configure the SDX client with the IP addresses of the SDX servers and the ports on which the servers listen for activity.
- You can specify primary, secondary, and tertiary servers, and the port numbers on which each listens for activity. By default, the server listens on port 3288.

- Example

```
host1(config)#sscc primary address 192.168.128.10 port 3288
```

- Use the **no** version to remove a specific SDX server (primary, secondary, or tertiary) from the list of servers.

sscc enable

- Use to enable the SDX client's COPS support in the router.
- Use with the **cops-pr** keyword to enable COPS-PR support; omit the **cops-pr** keyword to enable XDR-based COPS support.

- Example

```
host1(config)#sscc enable cops-pr
```

- Use the **no** version to disable the feature.

sscc protocol ipv6

- Use to configure IPv6 support on the SDX client. IPv6 support enables policy and QoS configuration on IPv6 interfaces. The IPv6 support is in addition to the default IPv4 support.
- The SDX client does not support IPv6 policy and QoS configuration when in the XDR mode.

- Example

```
host1(config)#sscc protocol ipv6
```

- Use the **no** version to disable IPv6 support on the SDX client.

sscc retryTimer

- Use to specify the delay period (in the range 5–300 seconds) during which the SDX client waits for a response from the SDX server.
- If only a primary server is configured, the client resends the request to the primary server.

- The client attempts to connect to a tertiary server only if both the primary and secondary SDX server are unavailable. For example, if the client is connected to the SDX secondary server when the delay period expires, the client first tries to connect to the primary server before trying the tertiary server. The client waits for the length of the delay period before each attempt.
- Example
`host1(config)#sscc retryTimer 90`
- Use the **no** version to restore the default value, 90 seconds.

sscc sourceAddress

- Use to specify a fixed source address for the TCP/COPS connection created for an SDX client session. This is the local address.
- If you do not specify a source address, the TCP/COPS connection is not bound to a specific source (that is, local) address.
- Example
`host1(config)#sscc sourceAddress 10.9.123.8`
- Use the **no** version to remove the specified address.

sscc sourceInterface

- Use to specify a fixed source interface for the TCP/COPS connection created for an SDX client session. This is a local interface.
- You may need to set a source interface in cases where a firewall, access control list, or policy configuration exists; and it is important to know what the interface is, or you need to set the interface independently from other protocols that have conflicting requirements.
- If you do not specify a source interface, the TCP/COPS connection is not bound to a specific source (that is, local) interface.
- Example
`host1(config)#sscc sourceInterface atm 3/0`
- Use the **no** version to remove the source interface.

sscc transportRouter

- Use to specify on which router the TCP/COPS connection is to be established.
- The router can be the same as or different from the router the SDX client session is created in and associated with.
- If you do not specify the transport router for an SDX client session, the transport router defaults to the router associated with the session.
- Example
`host1(config)#sscc transportRouter chicago`
- Use the **no** version to remove the specified SDX client transport router.

Setting Baselines

You can set baseline statistics using the **baseline** commands. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline when you retrieve baseline-relative statistics.

baseline aaa

- Use to set a baseline for AAA statistics.
- Use the **delta** keyword with the **show aaa statistics** command to show baselined statistics.
- There is no **no** version.

baseline aaa route-download

- Use to set a baseline for route downloads.
- Example
host1#**baseline aaa route-download**
- There is no **no** version.

baseline cops

- Use to set a baseline for COPS statistics.
- Use the **delta** keyword with the **show cops statistics** command to show baselined statistics.
- There is no **no** version.

baseline local pool

- Use to set a baseline for local address pool statistics.
- Use the **delta** keyword with the **show local pool statistics** command to show baselined statistics.
- There is no **no** version.

baseline radius

- Use to set a baseline for RADIUS statistics.
- Use the **delta** keyword with the **show radius statistics** command to show baselined statistics.
- There is no **no** version.

baseline sssc

- Use to set a baseline for SDX statistics.
- Use the **delta** keyword with the **show sssc statistics** command to show baselined statistics.
- There is no **no** version.

Monitoring Remote Access

Use the commands in this section to monitor remote access. These commands provide information about:

- AAA configuration
- AAA profiles
- AAA statistics
- Address pools
- COPS protocol layer
- Domain name delimiters
- Name servers
- RADIUS servers
- RADIUS SNMP traps
- RADIUS statistics
- SDX client connections
- Subscribers
- User domain mapping

Use the following commands to monitor PPP interfaces:

- **show ppp interface summary**
- **show ppp interface** *< selective control >*

For details on the **show ppp** commands, see [JUNOS Link Layer Configuration Guide, Chapter 4, Configuring Point-to-Point Protocol](#).

You can use the output filtering feature of the **show** command to include or exclude lines of output based on a text string you specify. For details, see [JUNOS System Basics Configuration Guide, Chapter 2, Command-Line Interface](#).



NOTE: AAA and RADIUS statistics are not preserved across a warm restart when stateful SRP Switchover is enabled.

show aaa accounting

- Use to display the AAA accounting configuration.
- Field descriptions
 - Accounting duplication—Name of the virtual router to which duplicate accounting records are sent to the accounting server
 - Broadcast accounting—Name of the virtual router groups to which broadcast accounting records are sent to the accounting server
 - send acct-stop on AAA access deny—Enabled, disabled
 - send acct-stop on authentication server access deny—Enabled, disabled
 - acct-interval (for PPP Clients)—Number of minutes between accounting update operations
 - send immediate-update—On receipt of response to Acct-Start message; enabled, disabled

■ Example

```
host1:vrXyz7#show aaa accounting
```

```
Accounting duplication set to router vrXyz25
Broadcast accounting uses group groupXyzCompany20
send acct-stop on AAA access deny is enabled
send acct-stop on authentication server access deny is disabled
acct-interval (for PPP Clients) 0
send immediate-update is enabled
```

show aaa accounting default

- Use to display the AAA accounting default method for a subscriber type. You can view the method used for ATM 1483, IPSec, PPP, RADIUS relay server, and tunnel subscribers, and IP subscriber management interfaces.

■ Example

```
host1#show aaa accounting tunnel default
radius
```

show aaa accounting interval

- Use to display the accounting interval.
- Example

```
host1#show aaa accounting interval
acct-interval (for PPP Clients) 10
```

show aaa accounting vr-group

- Use to display the names of a specific virtual router group or of all virtual router groups configured on the router and the virtual routers making up the groups.
- Field descriptions
 - vr-group—Name of the virtual router group.
 - virtual-router—Index entry and name of virtual routers in the group.
- Example

```
host1#show aaa accounting vr-group
```

```
vr-group groupXyzCompany10:
  virtual-router 1 vrXyzA
  virtual-router 2 vrXyzB
  virtual-router 3 vrXyzC
  virtual-router 4 vrXyzD
vr-group groupXyzCompany20:
  virtual-router 1 vrXyzP
  virtual-router 2 vrXyzQ
  virtual-router 3 vrXyzR
  virtual-router 4 vrXyzS
```

show aaa authentication default

- Use to display the default AAA authentication method list for a subscriber type. You can view the method list used for ATM 1483 subscribers, IPSec subscribers, IP subscriber management interfaces, PPP subscribers, RADIUS relay subscribers, and tunnel subscribers. For example, you can verify that the local authentication method is configured for PPP subscribers.
- Example

```
host1#show aaa authentication ppp default
local none
```

show aaa delimiters

- Use to display the domain and realm name delimiters, parse order, and parse direction configured on the router.
- Example

```
host1#show aaa delimiters
domain delimiters "@"
realm delimiters "/"
parse order is realm-first
domain parse direction is right-to-left
realm parse direction is left-to-right
```

show aaa domain-map

- Use to display the mapping between user domains and virtual routers.
- The following keywords have significance when used as user domains:
 - **none**—All client requests with no user domain name are associated with the virtual router mapped to the **none** entry
 - **default**—All client requests with a domain present that have no map are associated with the virtual router mapped to the **default** entry

- Field descriptions—The actual fields displayed depend on your configuration
 - Domain—Name of the domain
 - router-name—Virtual router to which user domain name is mapped
 - tunnel-group—Name of the tunnel group assigned to the domain map
 - ipv6-router-name—IPv6 virtual router to which user domain name is mapped
 - local-interface—Interface information to use on the local (E-series) side of the subscriber's interface
 - ipv6-local-interface—IPv6 interface information to use on the local (E-series) side of the subscriber's interface
 - poolname—Local address pool from which the router allocates addresses for this domain
 - IP hint—IP hint is enabled
 - strip-domain—Strip domain is enabled
 - override-username—Single username used for all users from a domain in place of the values received from the remote client
 - override-password—Single password used for all users from a domain in place of the values received from the remote client
 - Tunnel Tag—Tag that identifies the tunnel
 - Tunnel Peer—Destination address of the tunnel
 - Tunnel Source—Source address of the tunnel
 - Tunnel Type—L2TP
 - Tunnel Medium—Type of medium for the tunnel; only IPv4 is supported
 - Tunnel Password—Password for the tunnel
 - Tunnel Id—ID of the tunnel
 - Tunnel Client Name—Host name that the LAC sends to the LNS when communicating to the LNS about the tunnel
 - Tunnel Server Name—Host name expected from the peer (the LNS) when during tunnel startup
 - Tunnel Preference—Preference level for the tunnel
 - Tunnel Max Sessions—Maximum number of sessions allowed on a tunnel
 - Tunnel RWS—L2TP receive window size (RWS) for a tunnel on the LAC; displays either the configured value or the default behavior, which is indicated by **system chooses**
 - Tunnel Virtual Router—Name of the virtual router to map to the user domain name
 - Tunnel Failover Resync—L2TP peer resynchronization method
 - Tunnel Switch Profile—Name of the L2TP tunnel switch profile
 - Tunnel Tx Speed Method—Method that the router uses to calculate the transmit connect speed of the subscriber's access interface: static layer2, dynamic layer2, qos, actual, not set

- Example

```
host1#show aaa domain-map
```

```
Domain: lac-tunnel; router-name: lac; ipv6-router-name: default
```

Tunnel Tag	Tunnel Peer	Tunnel Source	Tunnel Type	Tunnel Medium	Tunnel Password	Tunnel Id
5	192.168.1.1	<null>	l2tp	ipv4	welcome	lac-tunnel

Tunnel Tag	Tunnel Client Name	Tunnel Server Name	Tunnel Preference	Tunnel Max Sessions	Tunnel RWS
5	lac	boston	5	0	4

Tunnel Tag	Tunnel Virtual Router	Tunnel Failover Resync	Tunnel Switch Profile	Tunnel Tx Speed Method
5	<null>	silent failover	denver	qos

show aaa duplicate-address-check

- Use to display whether the routing table address lookup or duplicate address check is enabled or disabled.
- Example

```
host1#show aaa duplicate-address-check
enabled
```

show aaa model

- Use to display the AAA model.
- Example

```
host1#show aaa model
aaa model: old model
```

show aaa name-servers

- Use to display the IP addresses of the primary and secondary DNS and WINS name servers.
- Example

```
host1#show aaa name-servers
Name Server Addresses (for PPP Clients):
primary DNS Addr          10.2.3.4
secondary DNS Addr        10.6.7.8
primary NBNS (WINS) Addr  10.22.33.44
secondary NBNS (WINS) Addr 10.66.77.88
```

show aaa profile

- Use to display the configuration of all AAA profiles or of a specific profile.
- Field descriptions
 - atm nas-port-type—Configuration of NAS-Port-Type attribute for ATM interfaces
 - ethernet nas-port-type—Configuration of NAS-Port-Type attribute for Ethernet interfaces
 - profile-service-description—Description configured in the Service-Description attribute
 - pre-authenticate—Indicates that subscriber preauthentication is configured for the profile
 - allow—One or more domain names that are allowed access to AAA authentication
 - deny—One or more domain names that are denied access to AAA authentication
 - translate—Original domain name and the name to which it is mapped for domain map lookup

■ Example

```
host1#show aaa profile name PreAuth1
preAuth1:
  atm nas-port-type: ADSL-CAP
  ethernet nas-port-type: Cable
  profile-service-description: xyzService
  pre-authenticate
  allow xyz.com
  deny default
  translate xyz1.com abc.com
```

show aaa route-download

- Use to display statistics about the RADIUS route-download server configuration.
- Use the optional **statistics** keyword to display information about the RADIUS route download server operation.
- Use the optional **delta** keyword to show baselined statistics.
- Field descriptions
 - AAA Route Downloader—Virtual router where the RADIUS route-download server is configured
 - Download Interval—Number of minutes between route downloads
 - Retry Interval—Number of minutes before retry after a download failure
 - Default Cost—Default cost of downloaded routes
 - Default Tag—Default tag for downloaded routes
 - Base User Name—Virtual router used for route-download requests; either <HOSTNAME> or the configured name
 - Password—Password for route-download requests or <DEFAULT>
 - Synchronization—Either <NOT SET> or the time that the server starts the route download operation each day

- Status—Current status of route-download server; waiting for base router, waiting for IP warmstart, idle, downloading, updating ip, downloading and updating ip, or suspended
- Last Download Attempt—Either < NEVER > or the day, date, and time of attempt
- Last Download Success—Either < NEVER > or the day, date, and time of success
- Last Regular Download—Status of last regular download; either complete or not complete
- Next Download Scheduled—< DOWNLOAD ACTIVE > , < NOT SCHEDULED > , or the day, date, and time of next download
- Next Regular Download—Day, date, and time
- Total Download Attempts—Number of downloads attempted
- Successful Downloads—Number of successful download operations
- Downloaded Fragments—Number of downloaded fragments
- Downloaded Routes—Number of downloaded routes
- IP Updates—Number of IP updates
- Updated Routes—Number of updated routes
- Cleared Route Intervals—Number of cleared route intervals

■ Example 1

```
host1#show aaa route-download
```

```
AAA Route Downloader:    configured in virtual router default
Download Interval:       720 minutes
Retry Interval:          10 minutes
Default Cost:            2
Default Tag:              0
Base User Name:          <HOSTNAME>
Password:                <DEFAULT>
Synchronization:        <NOT SET>
```

```
Status:                  idle
Last Download Attempt:    TUE DEC 19 22:46:47 2006
Last Download Success:    TUE DEC 19 22:46:47 2006
Last Regular Download:    complete
Next Download Scheduled:  WED DEC 20 10:46:47 2006
Next Regular Download:    WED DEC 20 10:46:47 2006
```

■ Example 2

```
host1#show aaa route-download statistics
```

```
Total Download Attempts: 2
Successful Downloads:    2
Downloaded Fragments:    3756
Downloaded Routes:        192000
IP Updates:               1
Updated Routes:           96000
Cleared Route Intervals:  0
```

show aaa route-download routes

- Use to display information about the routes that are downloaded by the RADIUS route-download server.
- Use the optional **detail** keyword to display more detailed information about the downloaded routes.
- Field descriptions
 - downloaded routes—Number of current downloaded routes
 - Prefix/Length—IP address prefix and mask information for downloaded routes
 - Type—Type of downloaded routes; Access-P indicates routes downloaded from the RADIUS route-download server
 - NextHop—IP address of the next hop
 - Dst/Met—Administrative distance and number of hops for the route
 - Tag—Tag assigned to downloaded routes
 - Intf—Interface type and specifier
- Example 1

```
host1#show aaa route-download routes
96000 downloaded routes
```

- Example 2

```
host1#show aaa route-download routes detail
Prefix/Length      Type      NextHop      Dst/Met  Intf  Tag
-----
192.168.1.1/32     Access-P  255.255.255.255  254/2    null0  0
192.168.1.5/32     Access-P  255.255.255.255  254/2    null0  0
192.168.1.9/32     Access-P  255.255.255.255  254/2    null0  0
192.168.1.13/32    Access-P  255.255.255.255  254/2    null0  0
192.168.1.17/32    Access-P  255.255.255.255  254/2    null0  0
192.168.1.21/32    Access-P  255.255.255.255  254/2    null0  0
```

show aaa route-download routes global

- Use to display chassis-wide information about routes that are downloaded by RADIUS route-download servers.
- Use the optional **detail** keyword to display more detailed information about the downloaded routes.
- Use the optional **start** keyword to specify the first router context that you want to display in the output. For example, aaa:a2 specifies that the display shows a list of router contexts starting with VRF a2 in virtual router aaa.
- Field descriptions
 - Virtual Router—Name of the virtual router used to download the routes
 - VRF—Name of the VRF used to download the routes
 - Present—Routes have been downloaded; y (yes) or n (no) indicates if the router context has been created.
 - Number of Routes—Number of current downloaded routes
 - Prefix/Length—IP address prefix and mask information for downloaded routes

- Type—Type of downloaded routes; Access-P indicates routes downloaded from the RADIUS route-download server
- NextHop—IP address of the next hop
- Dst/Met—Administrative distance and number of hops for the route
- Tag—Tag assigned to downloaded routes
- Intf—Interface type and specifier

■ Example 1

```
host1#show aaa route-download routes global
```

Virtual Router	VRF	Present	Number of Routes
aaa		n	4
aaa	a1	n	4
default		y	4
default	d1	n	4

■ Example 2

```
host1#show aaa route-download routes global detail
```

Virtual Router	VRF	Present	Prefix/Length	Type	NextHop	Dst/Met	Intf	Tag
aaa		n	192.168.1.1/32	Access-P	255.255.255.255	0/2	null0	0
aaa		n	192.168.1.2/32	Access-P	255.255.255.255	0/2	null0	0
aaa		n	192.168.3.1/32	Access-P	255.255.255.255	0/2	null0	0
aaa		n	192.168.4.1/32	Access-P	255.255.255.255	0/2	null0	0
aaa	a1	n	192.168.5.3/32	Access-P	255.255.255.255	0/2	null0	0
aaa	a1	n	192.168.7.1/32	Access-P	255.255.255.255	0/2	null0	0
aaa	a1	n	192.168.7.5/32	Access-P	255.255.255.255	0/2	null0	0
aaa	a1	n	192.168.9.1/32	Access-P	255.255.255.255	0/2	null0	0
default		y	192.168.22.1/32	Access-P	255.255.255.255	0/2	null0	0
default		y	192.168.23.1/32	Access-P	255.255.255.255	0/2	null0	0
default		y	192.168.24.1/32	Access-P	255.255.255.255	0/2	null0	0
default		y	192.168.25.1/32	Access-P	255.255.255.255	0/2	null0	0
default	d1	n	192.168.40.6/32	Access-P	255.255.255.255	0/2	null0	0
default	d1	n	192.168.40.7/32	Access-P	255.255.255.255	0/2	null0	0
default	d1	n	192.168.40.8/32	Access-P	255.255.255.255	0/2	null0	0
default	d1	n	192.168.40.9/32	Access-P	255.255.255.255	0/2	null0	0

■ Example 3

```
host1#show aaa route-download routes global start aaa:a2
```

Virtual Router	VRF	Present	Number of Routes
default		y	4
default	d1	n	4

show aaa statistics

- Use to display authentication, authorization, and accounting statistics.
- Use the optional **delta** keyword to specify that baselined statistics are to be shown.
- Field descriptions
 - incoming initiate requests—Number of incoming AAA requests (from other E-series applications) for user connect services
 - incoming disconnect requests—Number of incoming AAA requests (from other E-series applications) for user disconnect services
 - outgoing grant (tunnel) responses—Number of outgoing tunnel grant responses to AAA requests
 - outgoing grant responses—Number of outgoing grant responses to AAA requests
 - outgoing deny responses—Number of outgoing deny responses to AAA requests
 - outgoing error responses—Number of outgoing error responses to AAA requests
 - outgoing Authentication requests—Number of authentication requests from AAA to the authentication task
 - incoming Authentication responses—Number of authentication responses from the authentication task to AAA
 - outgoing Re-Authentication requests—Number of reauthentication requests from AAA to the authentication task
 - incoming Re-Authentication responses—Number of reauthentication responses from the authentication task to AAA
 - outgoing Pre-Authentication requests—Number of preauthentication requests from AAA to the preauthentication task
 - incoming Pre-Authentication responses—Number of preauthentication responses from the preauthentication task to AAA
 - outgoing Accounting requests—Number of accounting requests (starts, updates, stops) from AAA to the accounting task
 - incoming Accounting responses—Number of accounting responses (starts, updates, stops) from the accounting task to AAA
 - outgoing Duplicate Acct requests—Number of duplicate accounting requests (starts, updates, stops) from AAA to the accounting task
 - incoming Duplicate Acct responses—Number of duplicate accounting responses (starts, updates, stops) from the accounting task to AAA
 - outgoing Broadcast Acct requests—Number of broadcast accounting requests (starts, updates, stops) from AAA to the accounting task
 - incoming Broadcast Acct responses—Number of broadcast accounting responses (starts, updates, stops) from the accounting task to AAA

- outgoing Address requests—Number of address allocation/release requests from AAA to address allocation task
- incoming Address responses—Number of address allocation/release responses from the address allocation task to AAA
- Example

```
host1#show aaa statistics
```

AAA Statistics	
Statistic	Count
incoming initiate requests	109
incoming disconnect requests	7
outgoing grant (tunnel) responses	3
outgoing grant responses	6
outgoing deny responses	0
outgoing error responses	0
outgoing Authentication requests	9
incoming Authentication responses	9
outgoing Re-Authentication requests	0
incoming Re-Authentication responses	0
outgoing Pre-Authentication requests	1
incoming Pre-Authentication responses	1
outgoing Accounting requests	120
incoming Accounting responses	120
outgoing Duplicate Acct requests	18
incoming Duplicate Acct responses	18
outgoing Broadcast Acct requests	32
incoming Broadcast Acct responses	32
outgoing Address requests	0
incoming Address responses	0

show aaa subscriber per-port-limit

- Use to display the maximum number of active subscribers configured per port.
- Example

```
host1#show aaa subscriber per-port-limit
```

Subscriber Port Limits	
Port	Limit
0/2	5
0/3	2
3/2	2

show aaa subscriber per-vr-limit

- Use to display the maximum number of active subscribers configured per virtual router.
- Example

```
host1#show aaa subscriber per-vr-limit
subscriber limit is 0
```

show aaa timeout

- Use to display idle and session timeouts.
- Example


```
host1#show aaa timeout
idle timeout (for PPP Clients) 0 seconds
session timeout (for PPP Clients) 31622400 seconds
```

show configuration category aaa global-attributes

- Use to display the virtual router groups that are configured for AAA broadcast accounting.
- For additional information about the **show configuration** command, see [Customizing the Configuration Output](#) in *JUNOS System Basics Configuration Guide, Chapter 5, Managing the System*.
- Field descriptions
 - aaa accounting vr-group—Name of virtual router groups
 - aaa virtual-router—Name and index number of the virtual routers that are members of the virtual router group
- Example

```
host1#show configuration category aaa global-attributes
! Configuration script being generated on MON JAN 10 2005 15:19:19 UTC
! Juniper Edge Routing Switch ERX-1440
! Version: 9.9.9 development-4.0 (January 7, 2005 17:26)
! Copyright (c) 1999-2004 Juniper Networks, Inc. All rights reserved.
!
! Commands displayed are limited to those available at privilege level 15
!
! NOTE: This script represents only a subset of the full system configuration.
! The category displayed is: aaa global-attributes
!
aaa accounting vr-group groupXyzCompany10
aaa virtual-router 1 vrXyzA
aaa virtual-router 2 vrXyzB
aaa virtual-router 3 vrXyzC
aaa virtual-router 4 vrXyzD

aaa accounting vr-group groupXyzCompany20
aaa virtual-router 1 vrXyzP
aaa virtual-router 2 vrXyzQ
aaa virtual-router 3 vrXyzR
aaa virtual-router 4 vrXyzS
!
hostname "host1"
```

show configuration category aaa local-authentication

- Use to display the configuration information for AAA local authentication. You can display information for the following keywords:
 - **databases**—Local user databases configured on the router
 - **users**—Users configured in the local user databases
 - **virtual-router**—Local user database selected by the specified virtual router for local authentication

- For additional information about the **show configuration** command, see [Customizing the Configuration Output](#) in *JUNOS System Basics Configuration Guide, Chapter 5, Managing the System*.
- Field descriptions for all keywords
 - aaa local database—Name of the local user database; the name **default** specifies the default local user database
 - aaa local select database—Local user database that the virtual router uses for local authentication
 - aaa local username—Unique user entry in the local user database
 - database—Name of the local user database for the specified username
 - hostname—Name of the host router
 - ip-address—IP address parameter for the user entry
 - ip-address-pool—IP address pool parameter for the user entry
 - operational virtual-router—Virtual router parameter for the user entry
 - password—Password used to authenticate the subscriber
 - secret—Secret used to authenticate the subscriber
 - virtual-router—Name of virtual router
- Example (see [Local Authentication Example](#) on page 44 for additional examples with the **users** and **virtual-router** keywords).

```

host1#show configuration category aaa local-authentication databases
! Configuration script being generated on TUE NOV 09 2004 12:50:18 UTC
! Juniper Edge Routing Switch ERX-1400
! Version: 6.1.0 (November 8, 2004 18:31)
! Copyright (c) 1999-2004 Juniper Networks, Inc. All rights reserved.
!
! Commands displayed are limited to those available at privilege level 15
!
! NOTE: This script represents only a subset of the full system configuration.
! The category displayed is: aaa local-authentication databases
!
hostname host1
aaa new-model
aaa local database default
aaa local database svaleldb10

```

show configuration category aaa server-attributes include-defaults

- Use to display status of the attributes on the AAA server, including AAA accounting duplication and broadcast.
- For additional information about the **show configuration** command, see [Customizing the Configuration Output](#) in *JUNOS System Basics Configuration Guide, Chapter 5, Managing the System*.
- Field descriptions
 - virtual router—Name of the virtual router
 - aaa accounting duplication—Virtual router used for duplicate accounting
 - aaa accounting broadcast—Virtual router group used for broadcast accounting

- aaa duplicate-address-check—Enabled, disabled
- aaa accounting acct-stop on-aaa-failure—Enabled, disabled
- aaa accounting acct-stop on-access-deny—Enabled, disabled
- aaa subscriber limit per-vr—Enabled, disabled
- aaa intf-desc-format include sub-intf—Enabled, disabled
- aaa intf-desc-format include adapter—Enabled, disabled
- aaa accounting immediate-update—Enabled, disabled

■ Example

```

host1#show configuration category aaa server-attributes include-defaults
! Configuration script being generated on MON JAN 10 2005 15:12:02 UTC
! Juniper Edge Routing Switch ERX-1440
! Version: 9.9.9 development-4.0 (January 7, 2005 17:26)
! Copyright (c) 1999-2004 Juniper Networks, Inc. All rights reserved.
!
! Commands displayed are limited to those available at privilege level 15
!
! NOTE: This script represents only a subset of the full system configuration.
! The category displayed is: aaa server-attributes
!
virtual-router default
aaa accounting duplication lac
aaa accounting broadcast group1
aaa duplicate-address-check enable
aaa accounting acct-stop on-aaa-failure enable
aaa accounting acct-stop on-access-deny disable
aaa subscriber limit per-vr 0
aaa intf-desc-format include sub-intf enable
aaa intf-desc-format include adapter enable
aaa accounting immediate-update disable
!
! =====
!
virtual-router lac
no aaa accounting duplication
no aaa accounting broadcast
aaa duplicate-address-check enable
aaa accounting acct-stop on-aaa-failure enable
aaa accounting acct-stop on-access-deny disable
aaa subscriber limit per-vr 0
aaa intf-desc-format include sub-intf enable
aaa intf-desc-format include adapter enable
aaa accounting immediate-update disable
!
! =====
!
virtual-router isp
no aaa accounting duplication
no aaa accounting broadcast
aaa duplicate-address-check enable
aaa accounting acct-stop on-aaa-failure enable
aaa accounting acct-stop on-access-deny disable
aaa subscriber limit per-vr 0
aaa intf-desc-format include sub-intf enable
aaa intf-desc-format include adapter enable
aaa accounting immediate-update disable

```

show cops info

- Use to display information about the COPS layer over which the SDX connection is made.
- Field descriptions
 - General COPS Information:
 - Session Created—Number of COPS sessions created
 - Sessions Deleted—Number of COPS sessions deleted
 - Current Sessions—Number of current COPS sessions
 - Bytes Received—Number of bytes received on all COPS sessions
 - Packets Received—Number of packets received on all COPS sessions
 - Bytes Sent—Number of bytes transmitted on all COPS sessions
 - Packets Sent—Number of packets transmitted on all COPS sessions
 - Keep Alive Received—Number of COPS keepalive messages received
 - Keep Alive Sent—Number of COPS keepalive messages *sent*
 - Session Information:
 - Remote IP Address—IP address of the remote peer
 - Remote TCP Port—TCP port number of the remote peer
 - Client Type—Type of client for the session. For this release the client type must be 16640 (SDX client).
 - Bytes Received—Number of bytes received for this COPS session
 - Packets Received—Number of packets received for this COPS session
 - Bytes Sent—Number of bytes sent on this COPS session
 - Packets Sent—Number of packets sent on this COPS session
 - REQ Sent—Number of Request packets sent on this COPS session
 - DEC Rcv—Number of Decision packets received on this COPS session
 - RPT Sent—Number of Report packets sent on this COPS session
 - DRQ Sent—Number of Delete Requests sent on this COPS session
 - SSQ Rcv—Number of Synch Requests received on this COPS session
 - OPN Sent—Number of Open messages sent on this COPS session
 - CAT Rcv—Number of Client Accepts packets received on this COPS session
 - CC Sent—Number of Client Closes packets sent on this COPS session
 - CC Rcv—Number of Client Closes packets received on this COPS session
 - SSC Sent—Number of Sync Complete packets sent on this COPS session

- Example

```
host1#show cops info
```

```
General Cops Information:
```

```
Sessions Created: 1
Sessions Deleted: 0
Current Sessions: 1
Bytes Received: 680
Packets Received: 17
Bytes Sent: 692
Packets Sent: 21
Keep Alive Received: 12
Keep Alive Sent: 12
```

```
Session Information
```

```
Remote Ip Address: 10.10.0.223
Remote TCP Port: 4001
Client Type: 16384
Bytes Received: 2224
Packets Received: 5
Bytes Sent: 596
Packets Sent: 9
REQ Sent: 4
DEC Rcv: 4
RPT Sent: 4
DRQ Sent: 0
SSQ Rcv: 0
OPN Sent: 1
CAT Rcv: 1
CC Sent: 0
CC Rcv: 0
SSC Sent: 0
```

show cops statistics

- Use to display statistics about the COPS layer over which the SDX connection is made.
- Field descriptions
 - General COPS Information:
 - Session Created—Number of COPS sessions created
 - Sessions Deleted—Number of COPS sessions deleted
 - Current Sessions—Number of current COPS sessions
 - Bytes Received—Number of bytes received on all COPS sessions
 - Packets Received—Number of packets received on all COPS sessions
 - Bytes Sent—Number of bytes transmitted on all COPS sessions
 - Packets Sent—Number of packets transmitted on all COPS sessions
 - Keep Alive Received—Number of COPS keepalive messages received
 - Keep Alive Sent—Number of COPS keepalive messages *sent*

- Session Information:
 - Client Type—Type of client for the session.
 - Bytes Received—Number of bytes received for this COPS session
 - Packets Received—Number of packets received for this COPS session
 - Bytes Sent—Number of bytes sent on this COPS session
 - Packets Sent—Number of packets sent on this COPS session
 - REQ Sent—Number of Request packets sent on this COPS session
 - DEC Rcv—Number of Decision packets received on this COPS session
 - RPT Sent—Number of Report packets sent on this COPS session
 - DRQ Sent—Number of Delete Requests sent on this COPS session
 - SSQ Rcv—Number of Synch Requests received on this COPS session
 - OPN Sent—Number of Open messages sent on this COPS session
 - CAT Rcv—Number of Client Accepts packets received on this COPS session
 - CC Sent—Number of Client Closes packets sent on this COPS session
 - CC Rcv—Number of Client Closes packets received on this COPS session
 - SSC Sent—Number of Sync Complete packets sent on this COPS session

■ Example

```

host1#show cops statistics
General Cops Information:
  Sessions Created: 0
  Sessions Deleted: 0
  Current Sessions: 0
  Bytes Received: 1108
  Packets Received: 12
  Bytes Sent: 1572
  Packets Sent: 18
  Keep Alive Received: 2
  Keep Alive Sent: 2
Session Information:
  Client Type: 24754
  Bytes Received: 2539032
  Packets Received: 20388
  Bytes Sent: 4386648
  Packets Sent: 51337
  REQ Sent: 21203
  DEC Rcv: 20388
  RPT Sent: 20391
  DRQ Sent: 9743
  SSQ Rcv: 0
  OPN Sent: 0
  CAT Rcv: 0
  CC Sent: 0
  CC Rcv: 0
  SSC Sent: 0

```


show ip local alias

- Use to display information about aliases for the local address pools configured on your router.
- If you do not specify an alias, the router displays all aliases.
- Field descriptions
 - Alias—Name of alias for the local address pool
 - Pool—Name of the local address pool
- Example

```
host1#show ip local alias
```

Alias	Pool
-----	-----
alias1	poolA
alias2	poolB
alias3	poolC
poolA	poolD
poolB	poolD
poolC	poolD

show ip local pool

- Use to display information about the local address pools configured on your router.
- If you do not specify the name of a local address pool, the router displays all local address pools.
- Field descriptions
 - Pool—User-specified name of the address pool
 - High Thresh—High utilization threshold value
 - Abated Thresh—Abated utilization threshold value
 - Trap—Enable SNMP pool utilization traps: Y (yes) or N (no)
 - Aliases—Aliases for the local address pool
 - Begin—Starting IP address
 - End—Ending IP address
 - Free—Number of addresses available for use
 - In Use—Number of addresses currently in use

■ Example

```
host1#show ip local pool
```

Pool	High Thresh	Abated Thresh	Trap	Group
poolA	85	75	N	

```
Aliases
```

alias1			In Use
Begin	End	Free	
10.1.1.1	10.1.1.10	10	0
10.1.2.1	10.1.2.10	10	0
10.1.3.1	10.1.3.10	10	0

Pool	High Thresh	Abated Thresh	Trap	Group
poolB	85	75	N	

```
Aliases
```

alias2			In Use
Begin	End	Free	
10.2.1.1	10.2.1.10	10	0
10.2.2.1	10.2.2.10	10	0

Pool	High Thresh	Abated Thresh	Trap	Group
poolC	85	75	N	

```
Aliases
```

alias3			In Use
Begin	End	Free	
10.3.1.1	10.3.1.10	10	0

Pool	High Thresh	Abated Thresh	Trap	Group
poolD	85	75	N	

```
Aliases
```

poolA poolB poolC			In Use
Begin	End	Free	
10.4.1.1	10.4.1.255	255	0

show ip local pool statistics

- Use to display local address pool statistics.
- Use the optional **delta** keyword to specify that baselined statistics are to be shown.
- Example

```
host1#show ip local pool statistics
Local Address Pool Statistics
```

Statistic	Values
Requests denied (pool exhaustion)	0

show ip local shared-pool

- Use to display the shared local address pool configurations.
- Field descriptions
 - Shared Pool—Name of the shared local address pool
 - In Use—Number of addresses allocated
 - Dhcp Pool—Name of the DHCP address pool
- Example

```
host1#show ip local shared-pool
```

Shared Pool	In Use	Dhcp Pool
shared_poolA	253	dhcp_pool_25
shared_poolB	83	dhcp_pool_25
shared_poolC	99	dhcp_pool_17

show ip route

- Use to display the current state of the routing table, including routes not used for forwarding.
- An Access-P entry in the Type column of the output indicates routes that are downloaded by the RADIUS route-download server.
- Refer to the description of the **show ip route** command in [JUNOS IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP](#) for additional information about the **show ip route** command.

```
host1#show ip route
```

Protocol/Route type codes:

I1- ISIS level 1, I2- ISIS level2,
 I- route type intra, IA- route type inter, E- route type external,
 i- metric type internal, e- metric type external,
 P- periodic download, O- OSPF, E1- external type 1, E2- external type2,
 N1- NSSA external type1, N2- NSSA external type2
 L- MPLS label, V- VRF, *- via indirect next-hop

Prefix/Length	Type	Next Hop	Dst/Met	Interface
0.0.0.0/0	Static	10.13.10.1	1/0	FastEthernet6/0/0
192.168.10.0/23	Connect	10.13.10.187	0/0	FastEthernet6/0/0
192.168.21.21/32	Access-P	255.255.255.255	254/2	null0
192.168.22.22/32	Access-P	255.255.255.255	254/2	null0
192.168.23.23/32	Access-P	255.255.255.255	254/2	null0
192.168.24.24/32	Access-P	255.255.255.255	254/2	null0

show license b-ras

- Use to display the B-RAS license.
- Example

```
host1#show license b-ras
K4bZ16Lr
```

show radius algorithm

- Use to display information about the currently configured RADIUS server algorithm.
- Example

```
host1#show radius algorithm
direct
```

show radius override

- Use to display the current RADIUS override settings.
- Field descriptions
 - nas-ip-addr—Either the NAS-IP-Address [4] attribute is used, or it is overridden with the Tunnel-Client-Endpoint [66] attribute.
 - nas-info—Either the NAS-IP-Address [4] and NAS-Identifier [32] attributes of the virtual router generating the accounting information are used, or they are overridden with the respective attributes of the authentication virtual router.
- Example

```
host1:vrXyz7#show radius override
nas-ip-addr: nas-ip-addr
nas-info:    from authentication virtual router
```

show radius rollover-on-reject

- Use to display the configuration of the RADIUS rollover feature.
- Example

```
host1#show radius rollover-on-reject
rollover-on-reject enabled
```

show radius servers

- Use to display RADIUS server information.
- Use with the optional **accounting**, **authentication**, **dynamic-request**, **route-download**, or **pre-authentication** keywords to limit output to the specific type of server.
- Field descriptions
 - IP Address—IP address of RADIUS server
 - Udp Port—Number of the UDP of the RADIUS server
 - Retry Count—Maximum number of times that the router retransmits a RADIUS packet to the RADIUS server
 - Timeout—Interval (in seconds) before the router retransmits a RADIUS packet to the RADIUS server
 - Maximum Sessions—Number of outstanding requests to the RADIUS server
 - Dead Time—Amount of time to remove the authentication server or accounting server from the available list when a timeout occurs
 - Secret—Configured authentication server or accounting server secret
- Example

```
host1#show radius servers
```

RADIUS Authentication Configuration

IP Address	Udp Port	Retry Count	Timeout	Maximum Sessions	Dead Time	Secret
-----	-----	-----	-----	-----	-----	-----
172.28.30.117	1812	3	3	255	0	radius

RADIUS Accounting Configuration

IP Address	Udp Port	Retry Count	Timeout	Maximum Sessions	Dead Time	Secret
-----	-----	-----	-----	-----	-----	-----
172.28.30.117	1813	3	3	255	0	radius

RADIUS Pre-Authentication Configuration

IP Address	Udp Port	Retry Count	Timeout	Maximum Sessions	Dead Time	Secret
-----	-----	-----	-----	-----	-----	-----
172.28.30.117	1812	3	3	255	0	radius

RADIUS Route-Download Configuration

IP Address	Udp Port	Retry Count	Timeout	Maximum Sessions	Dead Time	Secret
-----	-----	-----	-----	-----	-----	-----
192.168.30.16	1812	3	3	255	0	radius

show radius statistics

- Use to display statistics on RADIUS services.
- Use with the optional **accounting**, **authentication**, **dynamic-request**, **route-download**, or **pre-authentication** keywords to limit output to the specific type of statistics.
- Use the optional **delta** keyword to specify that baselined statistics are to be shown.
- Field descriptions



NOTE: All descriptions apply to the primary, secondary, and tertiary RADIUS authentication and accounting servers.

- UDP Port—Number of the UDP of a RADIUS server
- Round Trip Time—Hundreds of seconds from request to response
- Access Requests—Number of access requests sent to server
- Rollover Requests—Number of requests coming into server as a result of the previous server timing out
- Retransmissions—Number of retransmissions
- Access Accepts—Number of Access-Accepts received from the server
- Access Rejects—Number of Access-Rejects received from the server
- Access Challenges—Number of access challenges received from the server
- Malformed Responses—Number of responses with attributes having an invalid length or unexpected attributes (such as two attributes when the response is required to have at most one)
- Bad Authenticators—Number of responses in which the authenticator is incorrect for the matching request. This can occur if the RADIUS secret for the client and server does not match.
- Requests Pending—Number of requests waiting for a response
- Request Timeouts—Number of requests that timed out
- Unknown Responses—Number of unknown responses. The RADIUS response type in the header is invalid or unsupported.
- Packets Dropped—Number of packets dropped either because they are too short or the E-series router receives a response for which there is no corresponding request. For example, if the router sends a request and the request times out, the router removes the request from the list and sends a new request. If the server is slow and sends a response to the first request after the router removes the request, the packet is dropped.
- Requests—Total number of accounting requests received from the server
- Start Requests—Number of accounting start requests sent; includes Acct-On, Acct-Start, Acct-Link-State, and Acct-Tunnel-Start requests
- Interim Requests—Number of interim accounting requests
- Stop Requests—Number of accounting stop requests sent; includes Acct-Off, Acct-Stop, Acct-Link-Stop, and Acct-Tunnel-Stop requests

- Reject Requests—Number of accounting reject requests sent; includes Acct-Link-Reject and Acct-Tunnel-Reject requests
 - Responses—Number of accounting responses received from the server
 - Start Responses—Number of accounting start responses received; includes Acct-On, Acct-Start, Acct-Link-Start, and Acct-Tunnel-Start responses
 - Interim Responses—Number of interim accounting responses
 - Stop Responses—Number of accounting stop responses received; includes Acct-Off, Acct-Stop, Acct-Link-Stop, and Acct-Tunnel-Stop responses
 - Reject Responses—Number of accounting reject responses received; includes Acct-Link-Reject and Acct-Tunnel-Reject responses
- Example 1

```
host1#show radius statistics
RADIUS Authentication Statistics
```

Statistic	10.10.121.128
UDP Port	1812
Round Trip Time	0
Access Requests	0
Rollover Requests	0
Retransmissions	0
Access Accepts	0
Access Rejects	0
Access Challenges	0
Malformed Responses	0
Bad Authenticators	0
Requests Pending	0
Request Timeouts	0
Unknown Responses	0
Packets Dropped	0

RADIUS Accounting Statistics

Statistic	10.10.121.128
UDP Port	1646
Round Trip Time	2
Requests	1
Start Requests	1
Interim Requests	0
Stop Requests	0
Reject Requests	0
Rollover Requests	0
Retransmissions	3
Responses	1
Start Responses	1
Interim Responses	0
Stop Responses	0
Reject Responses	0
Malformed Responses	0
Bad Authenticators	0
Requests Pending	0
Request Timeouts	3
Unknown Responses	0
Packets Dropped	0

- Example 2

```
host1#show radius pre-authentication statistics
```

RADIUS Pre-Authentication Statistics

Statistic	172.28.30.117
UDP Port	1812
Round Trip Time	0
Access Requests	2809
Rollover Requests	0
Retransmissions	56
Access Accepts	2809
Access Rejects	0
Access Challenges	0
Malformed Responses	0
Bad Authenticators	0
Requests Pending	0
Request Timeouts	72
Unknown Responses	0
Packets Dropped	2

- Example 3

```
host1#show radius route-download statistics
```

RADIUS Route-Download Statistics

Statistic	192.168.30.16
UDP Port	1812
Round Trip Time	0
Access Requests	1613
Rollover Requests	0
Retransmissions	6
Access Accepts	1612
Access Rejects	1
Access Challenges	0
Malformed Responses	0
Bad Authenticators	0
Requests Pending	0
Request Timeouts	6
Unknown Responses	0
Packets Dropped	5

show radius trap

- Use to display the configuration of RADIUS SNMP traps.

- Example

```
host1#show radius trap
```

```
trap for auth-server-not-responding enabled
trap for no-auth-server-responding disabled
trap for auth-server-responding enabled
trap for acct-server-not-responding enabled
trap for no-acct-server-responding disabled
trap for acct-server-responding disabled
```


show radius tunnel-accounting

- Use to display information about RADIUS accounting for L2TP tunnels.

- Example

```
host1#show radius tunnel-accounting
disabled
```

show radius udp-checksum

- Use to display information about UDP checksums.

- Example

```
host1#show radius udp-checksum
enabled
```

show radius update-source-addr

- Use to display the IP address of the RADIUS servers.

- Example

```
host1#show radius update-source-address
192.168.1.228
```

show ssc info

- Use to display the current status of the SDX client connection to the SDX servers. The command output refers to the SDX client by its former name, SSC client.
- Field descriptions
 - The SSC client configured servers—IP addresses of the primary, secondary, and tertiary SDX client servers
 - Local Source—Fixed source interface for the TCP/COPS connection
 - Local Source Address—Fixed source address for the TCP/COPS connection
 - The configured transport router is—Router on which is TCP/COPS connection is established
 - The configured retry timer is (seconds)—Delay period the client waits for a response from the SDX server before submitting request again
 - The connection state is—Current state of the TCP/COPS connection
 - SSC Client Statistics—Statistics about the connection between the SDX client and SDX server
 - Policy Commands received—Number of policy commands received on the SDX client connection
 - Policy Commands(List)—Number of Policy Commands with subtype List
 - Policy Commands(Acct)—Number of Policy Commands with subtype Accounting
 - Bad Policy Cmds received—Number of Policy Commands received with bad policies
 - Error Policy Cmds received—Number of Policy Commands received with errors

- ❑ Policy Reports sent—Number of Policy Reports sent
- ❑ Connection Open requests—Number of connections the SDX client has tried to open with a remote SDX server
- ❑ Connection Open completed—Number of connections successfully open to the SDX server
- ❑ Connection Closed sent—Number of connections the SDX client has closed
- ❑ Connection Closed remotely—Number of connections that were closed by the remote SDX server
- ❑ Create Interfaces sent—Number of create interface indications sent to the SDX server
- ❑ Delete Interfaces sent—Number of delete interface indications sent to the SDX server
- ❑ Active IP Interfaces—Current number of active IP interfaces the SDX client is aware of
- ❑ IP Interface Transitions—Number of IP interface transitions logged by the SDX client
- ❑ Synchronizes received—Number of synchronization requests the SDX client received from the SDX server
- ❑ Synchronize Complete sent—Number of synchronization complete indications sent
- ❑ Internal Errors—Number of internal errors
- ❑ Communication Errors—Number of errors with lower-layer communications (such as socket errors)

■ Example

```
host1#show sssc info
```

```
The SSC Client is currently unconnected
```

```
The SSC Client configured servers are:
```

```
Primary: 10.10.2.2:3
```

```
Secondary: 0.0.0.0:0
```

```
Tertiary: 0.0.0.0:0
```

```
Local Source: FastEthernet 0/0, Local Source Address: 10.13.5.61
```

```
The configured transport router is: default
```

```
The configured retry timer is (seconds): 90
```

```
The connection state is: NoConnection
```

```
SSC Client Statistics:
```

```
Policy Commands received    0
Policy Commands(List)      0
Policy Commands(Acct)      0
Bad Policy Cmds received    0
Error Policy Cmds received  0
Policy Reports sent         0
Connection Open requests    0
Connection Open completed   0
Connection Closed sent      0
Connection Closed remotely  0
Create Interfaces sent      0
Delete Interfaces sent      0
Active IP Interfaces        2
IP Interface Transitions    0
Synchronizes received       0
```

```

Synchronize Complete sent 0
Internal Errors            0
Communication Errors       0
Tokens Seen               0
Active Tokens              0
Token Transitions          0
Token Creates Sent         0
Token Deletes Sent         0
Active Addresses           0
Address Transitions        0
Create Addresses Sent      0
Delete Addresses Sent      0
Authentication Successes   0
Authentication Failures    0

```

show ssc statistics

- Use to display statistics about connection between the SDX client and SDX server. The command output refers to the SDX client by its former name, SSC client.
- Field descriptions
 - Policy Commands received—Number of policy commands received on the SDX client connection
 - Policy Commands(List)—Number of Policy Commands with subtype List
 - Policy Commands(Acct)—Number of Policy Commands with subtype Accounting
 - Bad Policy Cmds received—Number of Policy Commands received with bad policies
 - Error Policy Cmds received—Number of Policy Commands received with errors
 - Policy Reports sent—Number of Policy Reports sent
 - Connection Open requests—Number of connections the SDX client has tried to open with a remote SDX server
 - Connection Open completed—Number of connections successfully open to the SDX server
 - Connection Closed sent—Number of connections the SDX client has closed
 - Connection Closed remotely—Number of connections that were closed by the remote SDX server
 - Create Interfaces sent—Number of create interface indications sent to the SDX server
 - Delete Interfaces sent—Number of delete interface indications sent to the SDX server
 - Active IP Interfaces—Current number of active IP interfaces the SDX client is aware of
 - IP Interface Transitions—Number of IP interface transitions logged by the SDX client
 - Synchronizes received—Number of synchronization requests the SDX client received from the SDX server

- Synchronize Complete sent—Number of synchronization complete indications sent
- Internal Errors—Number of internal errors
- Communication Errors—Number of errors with lower-layer communications (such as socket errors)

■ Example

```
host1#show sssc statistics
```

```
SSC Client Statistics:
```

```
Policy Commands received 0
Policy Commands(List)    0
Policy Commands(Acct)    0
Bad Policy Cmds received 0
Error Policy Cmds received 0
Policy Reports sent      3
Connection attempts      7
Connection Open requests 7
Connection Open completed 0
Connection Closed sent   0
Connection Closed remotely 5
Create Interfaces sent    0
Delete Interfaces sent    3
Active IP Interfaces      3282
IP Interface Transitions 3281
Synchronizes received    0
Synchronizes rcvd & dropped 0
Synchronize Complete sent 2
Internal Errors           0
Communication Errors      0
Discovers Seen            15263
Active Discovers          4911
Discover Transitions      20704
Discover Creates Sent     15263
Discover Deletes Sent     10352
Active Addresses          3274
Address Transitions       3280
Create Addresses Sent     3277
Delete Addresses Sent     3
```

show sssc version

- Use to display the SDX client (formerly SSC client) version number.

■ Example

```
host1#show sssc version
```

```
The SSC Client version is: 4.0
```

show subscribers

- Use to display the active subscribers on the router.
- If you specify a username, the router displays only the users that match.
- When you issue the command in the default VR, all users are displayed. When you issue the command in a nondefault VR, only those users attached to that VR are displayed.
- You can use the **domain**, **interface**, **port**, **slot**, **username**, or **virtual-router** keywords on all routers to filter the results. If you do not use a keyword, all active users are displayed.

- When you use the **interface** keyword to display detailed subscriber information by interface, you must also specify either the **atm** or **ethernet** keyword, an interface specifier, and optionally a subinterface specifier.
- The output displayed in the interface field depends on the configuration of two commands at the time the subscriber logs in: **aaa intf-desc-format include sub-intf** and **aaa intf-desc-format include adapter** (for the E120 and E320 routers).

When the **aaa intf-desc-format include sub-intf disable** command has been issued, the subinterface is stripped from the subscriber's interface field at login and is not displayed in the output. In the default state, or when the **aaa intf-desc-format include sub-intf enable** command has been issued, the subinterface is included in the subscriber's interface field at login, and is displayed in the output.

When the **aaa intf-desc-format include adapter disable** command has been issued, the adapter is stripped from the subscriber's interface field at login and is not displayed in the output. In the default state, or when the **aaa intf-desc-format include adapter enable** command has been issued, the adapter is included in the subscriber's interface field at login and is displayed in the output.

Even when the subinterface has been stripped from the subscriber's interface field, you can still include the subinterface specifier in the **show subscribers interface** command. Even though the subinterface itself is not displayed, only subscribers on the specified subinterface are displayed.

These considerations do not apply when you issue the **summary** keyword. The output displayed in the Interface field of summary versions is not affected by the state of either the **aaa intf-desc-format include sub-intf** command or the **aaa intf-desc-format include adapter** command when the subscriber logs in.

- You can use the **ipv6** keyword to display all IPv6 subscribers or include the IPv6 prefix to limit the display to only IPv6 subscribers on a specific network.
- You can use the **summary** keyword to display only summary information about active subscribers.
- Field descriptions
 - User Name—Name of the subscriber
 - Type—Type of subscriber: atm, ip, ipsec, ppp, tnl (tunnel), tst (test)
 - Addr | Endpt—IP or IPv6 address and source of the address: l2tp, local, dhcp, radius, user. For local, dhcp, radius, and user endpoints, the address is that of the user. When the endpoint is l2tp, the address is that of the LNS.
 - Virtual Router—Name of the virtual router context
 - Interface—Interface specifier over which the subscriber is connected
 - Login Time—Date, in YY/MM/DD format, and time the subscriber logged in
 - Circuit Id—User circuit ID value specified by PPPoE
 - Remote Id—User remote ID value specified by PPPoE
 - Total Subscribers—Number of active subscribers, chassis-wide

- Peak Subscribers—Maximum value of the Total Subscriber field during the time the router has been active, chassis-wide
- Subscribers—Number of subscribers; the sum of the Ppp and Ip fields
- Ppp—Number of PPPoA and PPPoE users, combined
- Ip—Number of DHCP and IP subscriber manager users, combined
- Tnl—Number of users tunneled to an LNS
- Total—Total number of users per virtual router; the sum of the Ppp, Ip, and Tnl fields
- Domain Name—Domain name used by the subscriber
- Count—Number of subscribers
- Slot—Number of slot in the chassis

■ Example 1

host1#show subscribers

Subscriber List			
User Name	Type	Addr Endpt	Virtual Router
fred	tst	10.10.65.86/radius	default
bert	tst	192.168.10.3/user	default
User Name	Interface		
fred	atm 2/1.42:100.104		
bert	FastEthernet 5/2.4		
User Name	Login Time	Circuit Id	
fred	06/05/12 10:58:42	atm 5/1.3	
bert	06/05/12 10:59:08		
User Name	Remote Id		
fred			
bert	(800) 555-1212		

- Example 2—Shows detailed information for subscribers on the specified interface

host1#show subscribers interface ethernet 5/2

Subscriber List					
User Name	Type	Addr Endpt	Virtual Router		
bert	tst	192.168.10.3/user	default		
User Name	Interface				
bert	FastEthernet 5/2.4				
User Name	Login Time	Circuit Id			
bert	06/05/12 10:59:08				
User Name	Remote Id				
bert	(800) 555-0000				

- Example 3—Shows detailed information for subscribers on the specified slot

host1#show subscribers slot 5

```

Subscriber List
-----
User Name      Type      Addr|Endpt      Virtual
-----
fred           tst       10.10.65.86/radius default
User Name      Interface
-----
fred           atm 5/1.42:100.104
User Name      Login Time      Circuit Id
-----
fred           06/05/12 10:58:42 atm 5/1.3
User Name      Remote Id
-----
fred

```

- Example 4—Shows the number of subscribers on each virtual router, as well as the total and peak subscribers for the chassis

host1#show subscribers summary

```

Virtual
Router      Subscribers      Ppp      Ip      Tnl      Total
-----
default      1              1        0        0        1
Total Subscribers : 10 (chassis-wide total)
Peak Subscribers : 15 (chassis-wide total)

```

- Example 5—Shows the number of subscribers on each port

host1#show subscribers summary port

```

Interface      Count
-----
3/1             5
2/1             5
Total Subscribers : 10 (chassis-wide total)
Peak Subscribers : 15 (chassis-wide total)

```

- Example 6—Shows the number of subscribers by domain name

host1#show subscribers summary domain

```

Domain Name      Count
-----
abc.com           5
iii.com           5
Total Subscribers : 10 (chassis-wide total)
Peak Subscribers : 15 (chassis-wide total)

```

- Example 7—Shows the number of subscribers by interface

host1#show subscribers summary interface

```

Interface      Count
-----
ATM 3/2.1      1
ETHERNET 5/2.1 2
Total Subscribers : 3 (chassis-wide total)
Peak Subscribers : 6 (chassis-wide total)

```

- Example 8—Shows the number of subscribers by slot

```
host1#show subscribers summary slot
  Slot      Count
  -----
  3          1
  5          4
Total Subscribers : 5 (chassis-wide total)
Peak Subscribers : 8 (chassis-wide total)
```

show terminate-code

- Use to display information about the mappings for application terminate reasons.
- Field descriptions
 - Apps—The application generating the terminate reason; AAA, L2TP, PPP, or RADIUS client
 - Terminate Reason—The application's terminate reason
 - Description—The terminate reason
 - Radius Code—The RADIUS Acct-Terminate-Cause code to which the application's terminate reason is mapped
- Example 1—Specifies the **radius** keyword to display all current terminate reasons mapped to RADIUS Acct-Terminate-Cause codes. This command lists all PPP mappings, followed by L2TP mappings, and then AAA mappings.

```
host1(config)#run show terminate-code radius
```

Apps	Terminate Reason	Description	Radius Code
ppp	authenticate-authenticator-timeout	authenticate authenticator timeout	17
ppp	authenticate-challenge-timeout	authenticate challenge timeout	10
ppp	authenticate-chap-no-resources	authenticate chap no resources	10
ppp	authenticate-chap-peer-authenticator-timeout	authenticate chap peer authenticator timeout	17
ppp	authenticate-deny-by-peer	authenticate deny by peer	17
ppp	authenticate-inactivity-timeout	authenticate inactivity timeout	4
ppp	authenticate-max-requests	authenticate max requests	10
--More--			

- Example 2—Specifies the **radius** keyword and a RADIUS Acct-Terminate-Cause code to display all terminate reasons mapped to the specified terminate code. The following example uses **radius 4** as the terminate code.

```
host1(config)#run show terminate-code radius 4
```

Apps	Terminate Reason	Description	Radius Code
ppp	authenticate-inactivity-timeout	authenticate inactivity timeout	4
l2tp	session-timeout-inactivity	session timeout inactivity	4

- Example 3—Specifies an application to show all current mappings for the particular application's terminate reasons. This example uses **aaa** as the application.

```
host1(config)#run show terminate-code aaa
```

Apps	Terminate Reason	Description	Radius Code
aaa	deny-server-not-available	deny server not available	17
aaa	deny-server-request-timeout	deny server request timed out	17
aaa	deny-authentication-failure	deny authentication failure from server	17
aaa	deny-address-assignment-failure	deny address assignment failure	17
aaa	deny-address-allocation-failure	deny address allocation failure	17
aaa	deny-no-address-allocation-resources	deny insufficient resources for address allocation	17
aaa	deny-unknown-subscriber	deny no such server entry	17
aaa	deny-no-resources	deny no resources available	10
--More--			

- Example 4—Specifies an application and terminate reason to show the mapping for a specific terminate reason. This example uses **l2tp** as the application and **session-access-interface-down** as the terminate reason.

```
host1(config)#run show terminate-code l2tp session-access-interface-down
```

Terminate Reason	Description	Radius Code
session access interface down		8

Chapter 2

Configuring RADIUS Attributes

This chapter identifies the Remote Authentication Dial-In User Service (RADIUS) attributes that JUNOS software supports and describes the RADIUS attributes you can configure with the command-line interface (CLI). RADIUS attributes are discussed in the following sections:

- [Overview](#) on page 123
- [Platform Considerations](#) on page 125
- [References](#) on page 125
- [Subscriber AAA Access Messages](#) on page 125
- [Subscriber AAA Accounting Messages](#) on page 131
- [DSL Forum VSAs in AAA Access and Accounting Messages](#) on page 136
- [CLI AAA Messages](#) on page 137
- [CLI Commands Used to Modify RADIUS Attributes](#) on page 138

Overview

RADIUS is a distributed client/server that protects networks against unauthorized access. RADIUS clients running on a E-series router send authentication requests to a central RADIUS server.

You can access the RADIUS server through either a subscriber line or the CLI.



NOTE: For CLI/telnet users only—For CLI security, the router supports the RADIUS Access-Challenge message. The RADIUS server uses this message to send the user a challenge requiring a response. The router then displays the single reply message and attempts to authenticate the user with the new response as the password.

The central RADIUS server stores all the required user authentication and network access information. RADIUS informs the router of the privilege levels for which RADIUS-authenticated users have enable access. The router permits or denies enable access accordingly.

The RADIUS server is configured and managed by a RADIUS administrator. See your RADIUS server documentation for information about configuring and managing a RADIUS server.

The E-series RADIUS client uses the IP address in the router ID unless you explicitly set an IP address by using the **radius update-source-addr** command. See *Configuring RADIUS Authentication and Accounting Servers* in *Chapter 1, Configuring Remote Access*.

To explicitly set the source address, perform the following tasks:

- Configure the RADIUS update-source address.
- Set this address on the RADIUS server if required.



NOTE: For additional RADIUS information about topics such as restricting user access, vty line authentication, or SSH, see *JUNOS System Basics Configuration Guide, Chapter 8, Passwords and Security*.

RADIUS Services

RADIUS provides three distinct services:

- Authentication—Determines whether or not a user is allowed to access a specific service or resource.
- Authorization—Associates connection attributes or characteristics with a specific user.
- Accounting—Tracks service use by subscribers.

RADIUS Attributes

JUNOS software supports the RADIUS attributes and vendor-specific attributes (VSAs) listed in this chapter. These attributes define specific authentication, authorization, and accounting elements in a user's profile. The profile is stored on the RADIUS server. RADIUS messages contain RADIUS attributes to communicate information between an E-series router and the RADIUS server.

Note these guidelines about RADIUS attribute numbers:

- The number, such as [1], that appears in brackets before each attribute is the attribute's standard number.
- Any attribute number beginning with 26, such as [26-1], identifies a vendor-specific attribute.

For a complete list of RADIUS attributes supported by JUNOS software, see *Appendix A, RADIUS Attribute Descriptions*.

Platform Considerations

RADIUS is supported on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

References

For more information about RADIUS, consult the following resources:

- [RFC 2865—Remote Authentication Dial In User Service \(RADIUS\) \(June 2000\)](#)
- [RFC 2866—RADIUS Accounting \(June 2000\)](#)
- [RFC 2867—RADIUS Accounting Modifications for Tunnel Protocol Support \(June 2000\)](#)
- [RFC 2868—RADIUS Attributes for Tunnel Protocol Support \(June 2000\)](#)
- [RFC 2869—RADIUS Extensions \(June 2000\)](#)
- [DSL Forum Vendor-Specific RADIUS Attributes—draft-mammoliti-radius-dsl-vsa-02.txt \(September 2006 expiration\)](#)



NOTE: IETF drafts are valid for only 6 months from the date of issuance. They must be considered as works in progress. Please refer to the IETF Web site at <http://www.ietf.org> for the latest drafts.

Subscriber AAA Access Messages

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

The router supports the following types of authentication and authorization messages:

- Access-Request—Requests client authentication. RADIUS responds to a client authentication request with either an Access-Accept, an Access-Reject, or an Access-Challenge message. An Access-Request message can contain a number of RADIUS attributes.

- Access-Accept—Grants the client's access request and can provide specific configuration information necessary to begin delivery of service to the user.
- Access-Reject—Sent if any value of the received attributes is not acceptable.
- Access-Challenge—Sent to the client, requesting additional authentication information.
- Change-of-Authorization-Request (CoA-Request)—Dynamically modifies session attributes, such as data filters.
- Disconnect-Request—Immediately terminates a user session.

Supported RADIUS IETF Attributes

Table 10 lists the Access-Request, Access-Accept, Access-Reject, Access-Challenge, CoA, and Disconnect-Request attributes supported by JUNOS software. The following notes are referenced in Table 10:

1. Attribute is used by Access-Request messages when terminating a PPP connection at the LNS or the initiating LAC.
2. Attribute is used to support pass-through exchange of EAP messages.
3. Attribute is used by Access-Challenge messages to set the PPP retransmission timeout used for EAP request packets.

Table 10 lists the RADIUS IETF attributes supported for Access-Request, Access-Accept, Access-Reject, CoA-Request, and Disconnect-Request messages.

Table 10: AAA Access Message RADIUS IETF Attributes Supported

Attribute Number	Attribute Name	Access-Request	Access-Accept	Access-Reject	Access-Challenge	CoA-Request	Disconnect-Request
[1]	User-Name	✓	✓	–	–	✓	✓
[2]	User-Password	✓	–	–	–	–	–
[3]	CHAP-Password	✓	–	–	–	–	–
[4]	NAS-IP-Address	✓	–	–	–	–	–
[5]	NAS-Port	✓	–	–	–	–	–
[6]	Service-Type	✓	✓	–	–	–	–
[7]	Framed-Protocol	✓	✓	–	–	–	–
[8]	Framed-IP-Address	✓	✓	–	–	✓	–
[9]	Framed-IP-Netmask	–	✓	–	–	–	–
[11]	Filter-Id	–	✓	–	–	–	–
[12]	Framed-MTU (See Note 2 on page 126.)	✓	✓	–	–	–	–
[18]	Reply-Message (See Note 2 on page 126.)	–	✓	✓	✓	–	–

Table 10: AAA Access Message RADIUS IETF Attributes Supported (continued)

Attribute Number	Attribute Name	Access-Request	Access-Accept	Access-Reject	Access-Challenge	CoA-Request	Disconnect-Request
[22]	Framed-Route	–	✓	–	–	–	–
[24]	State (See Note 2 on page 126.)	–	–	–	✓	–	–
[25]	Class	–	✓	–	–	–	–
[27]	Session-Timeout (See Note 2 on page 126.) (See Note 3 on page 126.)	–	✓	✓	✓	–	–
[28]	Idle-Timeout	–	✓	–	–	–	–
[30]	Called-Station-Id	✓	–	–	–	–	–
[31]	Calling-Station-Id	✓	–	–	–	✓	–
[32]	NAS-Identifier	✓	–	–	–	–	–
[33]	Proxy-State	✓	–	–	–	–	–
[44]	Acct-Session-Id	✓	–	–	–	✓	–
[50]	Multilink-Session-Id	✓	–	–	–	–	✓
[60]	CHAP-Challenge	✓	–	–	–	–	–
[61]	NAS-Port-Type	✓	–	–	–	–	–
[62]	Port-Limit	–	✓	–	–	–	–
[64]	Tunnel-Type (See Note 1 on page 126.)	✓	✓	–	–	–	–
[65]	Tunnel-Medium-Type (See Note 1 on page 126.)	✓	✓	–	–	–	–
[66]	Tunnel-Client-Endpoint (See Note 1 on page 126.)	✓	✓	–	–	–	–
[67]	Tunnel-Server-Endpoint (See Note 1 on page 126.)	✓	✓	–	–	–	–
[68]	Acct-Tunnel-Connection (See Note 1 on page 126.)	✓	–	–	–	–	–
[69]	Tunnel-Password	–	✓	–	–	–	–
[77]	Connect-Info	✓	–	–	–	–	–
[79]	EAP-Message (See Note 2 on page 126.)	✓	✓	✓	✓	–	–
[80]	Message-Authenticator (See Note 2 on page 126.)	✓	✓	✓	✓	–	–
[82]	Tunnel-Assignment-Id	–	✓	–	–	–	–
[83]	Tunnel-Preference	–	✓	–	–	–	–
[85]	Acct-Interim-Interval	–	✓	–	–	–	–
[87]	NAS-Port-Id	✓	–	–	–	✓	–
[88]	Framed-Pool	–	✓	–	–	–	–

Table 10: AAA Access Message RADIUS IETF Attributes Supported (continued)

Attribute Number	Attribute Name	Access-Request	Access-Accept	Access-Reject	Access-Challenge	CoA-Request	Disconnect-Request
[90]	Tunnel-Client-Auth-Id (See Note 1 on page 126.)	✓	✓	–	–	–	–
[91]	Tunnel-Server-Auth-Id (See Note 1 on page 126.)	✓	✓	–	–	–	–
[96]	Framed-Interface-Id	–	✓	–	–	–	–
[97]	Framed-Ipv6-Prefix	–	✓	–	–	–	–
[99]	Framed-Ipv6-Route	–	✓	–	–	–	–
[101]	Error-Cause	–	–	–	–	✓	✓
[135]	Ascend-Primary-Dns	–	✓	–	–	–	–
[136]	Ascend-Secondary-Dns	–	✓	–	–	–	–
[188]	Ascend-Num-In-Multilink	✓	–	–	–	–	–
[242]	Ascend-Data-Filter	–	✓	–	–	–	–

Supported Juniper Networks VSAs

Table 11 lists the Juniper Networks (Vendor ID 4874) VSAs supported for Access-Request, Access-Accept, Access-Reject, CoA-Request, and Disconnect-Request messages.

Table 11: AAA Access Message Juniper Networks (Vendor ID 4874) VSAs Supported

Attribute Number	Attribute Name	Access-Request	Access-Accept	Access-Reject	CoA-Request	Disconnect-Request
[26-1]	Virtual-Router	–	✓	–	✓	–
[26-2]	Local-Address-Pool	–	✓	–	–	–
[26-3]	Local-Loopback-Interface	–	✓	–	–	–
[26-4]	Primary-DNS	–	✓	–	–	–
[26-5]	Secondary-DNS	–	✓	–	–	–
[26-6]	Primary-WINS (NBNS)	–	✓	–	–	–
[26-7]	Secondary-WINS (NBNS)	–	✓	–	–	–
[26-8]	Tunnel-Virtual-Router	–	✓	–	–	–
[26-9]	Tunnel-Password	–	✓	–	–	–
[26-10]	Ingress-Policy-Name	–	✓	–	–	–
[26-11]	Egress-Policy-Name	–	✓	–	–	–
[26-12]	Ingress-Statistics	–	✓	–	–	–
[26-13]	Egress-Statistics	–	✓	–	–	–
[26-14]	Service-Category	–	✓	–	–	–
[26-15]	PCR	–	✓	–	–	–

Table 11: AAA Access Message Juniper Networks (Vendor ID 4874) VSAs Supported (continued)

Attribute Number	Attribute Name	Access-Request	Access-Accept	Access-Reject	CoA-Request	Disconnect-Request
[26-16]	SCR	–	✓	–	–	–
[26-17]	Mbs	–	✓	–	–	–
[26-22]	Sa-Validate	–	✓	–	–	–
[26-23]	IGMP-Enable	–	✓	–	–	–
[26-24]	Pppoe-Description	✓	–	–	–	–
[26-25]	Redirect-Vrouter-Name	–	✓	–	–	–
[26-26]	Qos-Profile-Name	–	✓	–	–	–
[26-30]	Tunnel-Nas-Port-Method	–	✓	–	–	–
[26-31]	SSC-Service-Bundle-Name	–	✓	–	–	–
[26-33]	Tunnel-Max-Sessions	–	✓	–	–	–
[26-34]	Framed-IP-Route-Tag	–	✓	–	–	–
[26-44]	Tunnel-Interface-ID	✓	–	–	–	–
[26-45]	Ipv6-Virtual-Router	–	✓	–	–	–
[26-46]	Ipv6-Local-Interface	–	✓	–	–	–
[26-47]	Ipv6-Primary-DNS	–	✓	–	–	–
[26-48]	Ipv6-Secondary-DNS	–	✓	–	–	–
[26-52]	RADIUS-Client-Address	✓	–	–	–	–
[26-53]	Service-Description	✓	–	–	–	–
[26-54]	L2tp-Recv-Window-Size	–	✓	–	–	–
[26-55]	DHCP-Options	✓	–	–	–	–
[26-56]	DHCP-MAC-Address	✓	–	–	–	–
[26-57]	DHCP-GI-Address	✓	–	–	–	–
[26-58]	LI-Action	–	✓	–	✓	–
[26-59]	Med-Dev-Handle	–	✓	–	✓	–
[26-60]	Med-Ip-Address	–	✓	–	✓	–
[26-61]	Med-Port-Number	–	✓	–	✓	–
[26-62]	MLPPP-Bundle-Name	✓	–	–	–	–
[26-63]	Interface-Desc	✓	–	–	–	–
[26-64]	Tunnel-Group	–	✓	–	–	–
[26-65]	Activate-Service	–	✓	–	✓	–
[26-66]	Deactivate-Service	–	✓	–	✓	–

Table 11: AAA Access Message Juniper Networks (Vendor ID 4874) VSAs Supported (continued)

Attribute Number	Attribute Name	Access-Request	Access-Accept	Access-Reject	CoA-Request	Disconnect-Request
[26-67]	Service-Volume	–	✓	–	✓	–
[26-68]	Service-Timeout	–	✓	–	✓	–
[26-69]	Service-Stats	–	✓	–	✓	–
[26-70]	Ignore-DF-Bit	–	✓	–	–	–
[26-71]	IGMP-Access-Name	–	✓	–	–	–
[26-72]	IGMP-Access-Src-Name	–	✓	–	–	–
[26-73]	IGMP-OIF-Map-Name	–	✓	–	–	–
[26-74]	MLD-Access-Name	–	✓	–	–	–
[26-75]	MLD-Access-Src-Name	–	✓	–	–	–
[26-76]	MLD-OIF-Map-Name	–	✓	–	–	–
[26-77]	MLD-Version	–	✓	–	–	–
[26-78]	IGMP-Version	–	✓	–	–	–
[26-79]	IP-Mcast-Adm-Bw-Limit	–	✓	–	–	–
[26-80]	IPv6-Mcast-Adm-Bw-Limit	–	✓	–	–	–
[26-81]	L2c-Information	✓	–	–	–	–
[26-82]	QoS-Parameters	–	✓	–	–	–
[26-90]	L2TP-Resynch-Method	–	✓	–	–	–
[26-91]	Tunnel-Switch-Profile	–	✓	–	–	–
[26-92]	L2C-Up-Stream-Data	✓	–	–	–	–
[26-93]	L2C-Down-Stream-Data	✓	–	–	–	–
[26-94]	Tunnel-Tx-Speed-Method	–	✓	–	–	–
[26-95]	IGMP-Query-Interval	–	✓	–	–	–
[26-96]	IGMP-Max-Resp-Time	–	✓	–	–	–
[26-97]	IGMP-Immediate-Leave	–	✓	–	–	–
[26-98]	MLD-Query-Interval	–	✓	–	–	–
[26-99]	MLD-Max-Resp-Time	–	✓	–	–	–
[26-100]	MLD-Immediate-Leave	–	✓	–	–	–

Subscriber AAA Accounting Messages

Accounting messages identify service provisions and use on a per-user or per-tunnel basis. These messages keep track of when a particular service is initiated and terminated for a specific user.

JUNOS software supports the Acct-On message on startup or configuration of the first accounting server. Acct-Off messages are supported when the last RADIUS accounting server in a virtual router is removed, when the router is shut down, and when a virtual router that has configured RADIUS accounting servers is deleted.

The router supports the following types of accounting messages:

- Acct-Start
- Acct-Stop
- Interim-Acct
- Acct-On
- Acct-Off

Supported RADIUS IETF Attributes

[Table 12](#) lists the RADIUS IETF attributes supported for Acct-Start, Acct-Stop, Interim-Acct, Acct-On, and Acct-Off messages.

The following notes are referred to in [Table 12](#):

1. The attribute is used when terminating a PPP connection at the LNS or the initiating LAC.
2. The attribute is not included in Acct-Stop messages that are sent when a user session does not get established in one of the following situations.
 - The **aaa accounting acct-stop on-access-deny** command is enabled and the authentication server sends an Access-Reject (deny) message.
 - The **aaa accounting acct-stop on-aaa-failure** command is enabled and the authentication server issues an Access-Accept message (grant), but the AAA configuration denies access for the user. The **aaa accounting acct-stop on-aaa-failure** is enabled by default.
 - The **aaa accounting acct-stop on-aaa-failure** command is enabled and the user terminates before AAA receives the authentication response from the authentication server.

Table 12: AAA Accounting Message RADIUS IETF Attributes Supported

Attribute Number	Attribute Name	Acct-Start	Acct-Stop	Interim-Acct	Acct-On	Acct-Off
[1]	User-Name	✓	✓	✓	–	–
[4]	NAS-IP-Address	✓	✓	✓	✓	✓
[5]	NAS-Port	✓	✓	✓	–	–
[6]	Service-Type	✓	✓	✓	–	–
[7]	Framed-Protocol (See Note 2 on page 131.)	✓	✓	✓	–	–
[8]	Framed-IP-Address	✓	✓	✓	–	–
[9]	Framed-IP-Netmask	✓	✓	✓	–	–
[13]	Framed-Compression (See Note 2 on page 131.)	✓	✓	✓	–	–
[25]	Class	✓	✓	✓	–	–
[30]	Called-Station-Id	✓	✓	✓	–	–
[31]	Calling-Station-Id	✓	✓	✓	–	–
[32]	NAS-Identifier	✓	✓	✓	✓	✓
[40]	Acct-Status-Type	✓	✓	✓	✓	✓
[41]	Acct-Delay-Time	✓	✓	✓	✓	✓
[42]	Acct-Input-Octets	–	✓	✓	–	–
[43]	Acct-Output-Octets	–	✓	✓	–	–
[44]	Acct-Session-Id	✓	✓	✓	✓	✓
[45]	Acct-Authentic	✓	✓	✓	✓	✓
[46]	Acct-Session-Time	–	✓	✓	–	–
[47]	Acct-Input-Packets	–	✓	✓	–	–
[48]	Acct-Output-Packets	–	✓	✓	–	–
[49]	Acct-Terminate-Cause	–	✓	–	–	✓
[50]	Acct-Multi-Session-ID (See Note 2 on page 131.)	✓	✓	✓	–	–
[51]	Acct-Link-Count (See Note 2 on page 131.)	✓	✓	✓	–	–
[52]	Acct-Input-Gigawords	–	✓	✓	–	–
[53]	Acct-Output-Gigawords	–	✓	✓	–	–
[55]	Event-Timestamp	✓	✓	✓	✓	✓
[61]	NAS-Port-Type	✓	✓	✓	–	–

Table 12: AAA Accounting Message RADIUS IETF Attributes Supported (continued)

Attribute Number	Attribute Name	Acct-Start	Acct-Stop	Interim-Acct	Acct-On	Acct-Off
[64]	Tunnel-Type (See Note 1 on page 131 .)	✓	✓	✓	–	–
[65]	Tunnel-Medium-Type (See Note 1 on page 131 .)	✓	✓	✓	–	–
[66]	Tunnel-Client-Endpoint (See Note 1 on page 131 .)	✓	✓	✓	–	–
[67]	Tunnel-Server-Endpoint (See Note 1 on page 131 .)	✓	✓	✓	–	–
[68]	Acct-Tunnel-Connection (See Note 1 on page 131 .)	✓	✓	✓	–	–
[77]	Connect-Info	✓	✓	✓	–	–
[82]	Tunnel-Assignment-Id (LAC only) (See Note 1 on page 131 .)	✓	✓	✓	–	–
[83]	Tunnel-Preference (LAC only)	✓	✓	✓	–	–
[87]	NAS-Port-Id	✓	✓	✓	–	–
[90]	Tunnel-Client-Auth-Id (See Note 1 on page 131 .)	✓	✓	✓	–	–
[91]	Tunnel-Server-Auth-Id (See Note 1 on page 131 .)	✓	✓	✓	–	–
[188]	Ascend-Num-In-Multilink (See Note 2 on page 131 .)	✓	✓	✓	–	–

Supported Juniper Networks VSAs

Table 13 lists the Juniper Networks (Vendor ID 4874) VSAs supported for Acct-Start, Acct-Stop, Interim-Acct, Acct-On, and Acct-Off messages.

The following note is referred to in Table 13:

1. The attribute is not included in Acct-Stop messages that are sent when a user session does not get established in one of the following situations.
 - The **aaa accounting acct-stop on-access-deny** command is enabled and the authentication server sends an Access-Reject (deny) message.
 - The **aaa accounting acct-stop on-aaa-failure** command is enabled and the authentication server issues an Access-Accept message (grant), but the AAA configuration denies access for the user. The **aaa accounting acct-stop on-aaa-failure** is enabled by default.
 - The **aaa accounting acct-stop on-aaa-failure** command is enabled and the user terminates before AAA receives the authentication response from the authentication server.

Table 13: AAA Accounting Message Juniper Network (Vendor ID 4874) VSAs Supported

Attribute Number	Attribute Name	Acct-Start	Acct-Stop	Interim-Acct	Acct-On	Acct-Off
[26-10]	Ingress-Policy-Name	✓	✓	✓	–	–
[26-11]	Egress-Policy-Name	✓	✓	✓	–	–
[26-24]	Pppoe-Description (See Note 1 on page 134.)	✓	✓	✓	–	–
[26-42]	Acct-Input-Gigapackets	–	✓	✓	–	–
[26-43]	Acct-Output-Gigapackets	–	✓	✓	–	–
[26-44]	Tunnel-Interface-Id	✓	✓	✓	–	–
[26-51]	Disconnect-Cause	–	✓	–	–	–
[26-53]	Service-Description	✓	✓	–	–	–
[26-55]	DHCP-Options (See Note 1 on page 134.)	✓	✓	–	–	–
[26-56]	DHCP-MAC-Address (See Note 1 on page 134.)	✓	✓	–	–	–
[26-57]	DHCP-GI-Address (See Note 1 on page 134.)	✓	✓	–	–	–
[26-62]	MLPPP-Bundle-Name	✓	✓	✓	–	–
[26-63]	Interface-Description	✓	✓	✓	–	–
[26-92]	L2C-Up-Stream-Data	✓	✓	–	–	–
[26-93]	L2C-Down-Stream-Data	✓	✓	–	–	–

Tunnel Accounting Messages

Table 14 lists RADIUS attributes supported by the following tunnel-related accounting messages:

- Acct-Tunnel-Start
- Acct-Tunnel-Stop
- Acct-Tunnel-Reject
- Acct-Tunnel-Link-Start
- Acct-Tunnel-Link-Stop
- Acct-Tunnel-Link-Reject

Table 14: AAA Accounting Tunnel Message RADIUS Attributes Supported

Attribute Number	Attribute Name	Acct-Tunnel-Start	Acct-Tunnel-Stop	Acct-Tunnel-Reject	Acct-Tunnel-Link-Start	Acct-Tunnel-Link-Stop	Acct-Tunnel-Link-Reject
[1]	User-Name	–	–	–	✓	✓	–
[4]	NAS-IP-Address	✓	✓	✓	✓	✓	✓
[26-51]	Disconnect-Cause	–	–	–	–	✓	–
[32]	NAS-Identifier	✓	✓	✓	✓	✓	✓
[40]	Acct-Status-Type	✓	✓	✓	✓	✓	✓
[41]	Acct-Delay-Time	✓	✓	✓	✓	✓	✓
[44]	Acct-Session-Id	✓	✓	✓	✓	✓	✓
[46]	Acct-Session-Time	–	✓	–	–	✓	–
[49]	Acct-Terminate-Cause	–	✓	✓	–	✓	✓
[55]	Event-Timestamp	✓	✓	✓	✓	✓	✓
[64]	Tunnel-Type	✓	✓	✓	✓	✓	✓
[65]	Tunnel-Medium-Type	✓	✓	✓	✓	✓	✓
[66]	Tunnel-Client-Endpoint	✓	✓	✓	✓	✓	✓
[67]	Tunnel-Server-Endpoint	✓	✓	✓	✓	✓	✓
[68]	Acct-Tunnel-Connection	✓	✓	✓	✓	✓	✓
[82]	Tunnel-Assignment-Id (LAC only)	✓	✓	✓	✓	✓	✓
[83]	Tunnel-Preference (LAC only)	–	–	–	✓	✓	✓
[86]	Acct-Tunnel-Packets-Lost	–	–	–	–	✓	✓
[90]	Tunnel-Client-Auth-Id	✓	✓	✓	✓	✓	✓
[91]	Tunnel-Server-Auth-Id	✓	✓	✓	✓	✓	✓

DSL Forum VSAs in AAA Access and Accounting Messages

JUNOS software supports the inclusion of a set of DSL Forum vendor-specific attributes (VSAs) in the following AAA access and accounting messages:

- Access-Request
- Acct-Start
- Acct-Stop
- Interim-Acct (if Acct-Stop messages are specified)

The DSL Forum VSAs convey information about the subscriber associated with the digital subscriber line (DSL) and the data rate of the DSL. This information is not otherwise available in the standard set of RADIUS attributes or Juniper Networks VSAs. When you use the [radius include dsl-forum-attributes](#) command to enable inclusion of the DSL Forum VSAs in these AAA messages, the router includes all of the attributes listed in [Table 15](#) in the specified message, provided that the VSA is available in the information that the router receives from the digital subscriber line access multiplexer (DSLAM).

[Table 15](#) lists the DSL Forum VSAs supported by JUNOS software in Access-Request, Acct-Start, Acct-Stop, and (if Acct-Stop is specified) Interim-Acct messages. JUNOS software uses the vendor ID assigned to the DSL Forum (3561, or DE9 in hexadecimal format) by the Internet Assigned Numbers Authority (IANA).

For information about configuring inclusion of the DSL Forum VSAs, see [DSL Forum Vendor-Specific Attributes](#) on page 171. For a detailed description of the DSL Forum VSAs supported by JUNOS software, see [DSL Forum VSAs in Appendix A, RADIUS Attribute Descriptions](#).

Table 15: DSL Forum (Vendor ID 3561) VSAs Supported in AAA Access and Accounting Messages

Attribute Number	Attribute Name	Access-Request	Acct-Start	Acct-Stop	Interim-Acct
[26-1]	Agent-Circuit-Id	✓	✓	✓	✓
[26-2]	Agent-Remote-Id	✓	✓	✓	✓
[26-129]	Actual-Data-Rate-Upstream	✓	✓	✓	✓
[26-130]	Actual-Data-Rate-Downstream	✓	✓	✓	✓
[26-131]	Minimum-Data-Rate-Upstream	✓	✓	✓	✓
[26-132]	Minimum-Data-Rate-Downstream	✓	✓	✓	✓
[26-133]	Attainable-Data-Rate-Upstream	✓	✓	✓	✓
[26-134]	Attainable-Data-Rate-Downstream	✓	✓	✓	✓
[26-135]	Maximum-Data-Rate-Upstream	✓	✓	✓	✓
[26-136]	Maximum-Data-Rate-Downstream	✓	✓	✓	✓
[26-137]	Minimum-Data-Rate-Upstream-Low-Power	✓	✓	✓	✓
[26-138]	Minimum-Data-Rate-Downstream-Low-Power	✓	✓	✓	✓

Table 15: DSL Forum (Vendor ID 3561) VSAs Supported in AAA Access and Accounting Messages (continued)

Attribute Number	Attribute Name	Access-Request	Acct-Start	Acct-Stop	Interim-Acct
[26-139]	Maximum-Interleaving-Delay-Upstream	✓	✓	✓	✓
[26-140]	Actual-Interleaving-Delay-Upstream	✓	✓	✓	✓
[26-141]	Maximum-Interleaving-Delay-Downstream	✓	✓	✓	✓
[26-142]	Actual-Interleaving-Delay-Downstream	✓	✓	✓	✓
[26-144]	Access-Loop-Encapsulation	✓	✓	✓	✓
[26-254]	IWF-Session	✓	✓	✓	✓

CLI AAA Messages

There are four types of AAA messages used by CLI users to gain administrative access to the router. Access-Challenge attributes pertain only to CLI/telnet users.

- Access-Request
- Access-Accept
- Access-Challenge
- Access-Reject

Table 16 lists the RADIUS attributes supported for CLI AAA messages.

Table 16: CLI AAA Access Message RADIUS Attributes Supported

Attribute Number	Attribute Name	Access-Request	Access-Accept	Access-Challenge	Access-Reject
[1]	User-Name	✓	–	–	–
[2]	User Password	✓	–	–	–
[4]	NAS-IP-Address	✓	–	–	–
[6]	Service-Type	✓	✓	–	–
[18]	Reply-Message	–	–	✓	✓
[24]	State (Access-Request is only in response to an Access-Challenge)	✓	–	✓	–
[25]	Class	–	✓	–	–
[26-1]	Virtual-Router	–	✓	–	–
[26-18]	Init-CLI-Access-Level	–	✓	–	–
[26-19]	Allow-All-VR-Access	–	✓	–	–
[26-20]	Alt-CLI-Access-Level	–	✓	–	–
[26-21]	Alt-CLI-Virtual-Router-Name	–	✓	–	–
[26-25]	Redirect-Vrouter-Name	–	✓	–	–

CLI Commands Used to Modify RADIUS Attributes

This section discusses the RADIUS Internet Engineering Task Force (IETF) attributes and the Juniper Networks vendor-specific attributes that you can configure using CLI commands.

For many attributes, you can configure the router to include the attribute in RADIUS messages. To see a list of attributes that are included in or excluded from RADIUS messages, use the **show radius attributes-included** command, which is described in [Including or Excluding Attributes in RADIUS Messages](#) on page 172.

You can also configure the router to ignore many attributes that it receives in Access-Accept messages. To see a list of attributes that the router ignores, use the **show radius attributes-ignored** command, which is described in [Ignoring Attributes When Receiving Access-Accept Messages](#) on page 172.

For a complete list of RADIUS attributes supported by JUNOS software, see *Appendix A, RADIUS Attribute Descriptions*.

RADIUS IETF Attributes

This section describes the RADIUS IETF attributes that you can configure using CLI commands. The attributes are listed numerically—each attribute is followed by a list of the commands that you can use to manage the attribute and descriptions of each command.

[4] NAS-IP-Address

Use the following commands to configure, manage, and display information for the NAS-IP-Address RADIUS attribute.

- **radius override nas-ip-addr tunnel-client-endpoint**
- **radius override nas-info**
- **show radius override**

radius override nas-ip-addr tunnel-client-endpoint

- Use to configure the RADIUS client (LNS) to use the tunnel-client-endpoint (LAC) IP address for the NAS-IP-Address attribute.
- Example

```
host1(config)#radius override nas-ip-addr tunnel-client-endpoint
```
- Use the **no** version to restore the default address.

radius override nas-info

- Use in the correct virtual router context to override standard use of NAS-IP-Address and NAS-Identifier attributes for AAA broadcast accounting; specifies that the attributes for the authentication virtual router be included in accounting packets instead of the attributes for the virtual router that generates the accounting information.
- Example

```
host1(config)#virtual-router vrXyz1
host1:vrXyz1(config)#radius override nas-info
```
- Use the **no** version to restore standard use of the NAS-IP-Address and NAS-Identifier attributes.

show radius override

- Use to display the current setting for the NAS-IP-Address and the NAS-Identifier. These settings can be changed with the **radius override nas-ip-addr tunnel-client-endpoint** and **radius override nas-info** commands.
- Example

```
host1#show radius override
nas-ip-addr:      nas-ip-addr
nas-port-id:      nas-port-id
calling-station-id: calling-station-id
nas-info:         from current virtual router
```

[5] NAS-Port

Use the following commands to manage and display information for the NAS-Port RADIUS attribute:

- **radius include nas-port**
- **radius nas-port-format**
- **radius nas-port-format extended**
- **radius pppoe nas-port-format unique**
- **radius vlan nas-port-format stacked**
- **show radius nas-port-format**
- **show radius nas-port-format extended**
- **show radius pppoe nas-port-format**
- **show radius vlan nas-port-format**

radius include nas-port

- Use to include the NAS-Port attribute in Access-Request, Acct-Start, and Acct-Stop messages.
- You control inclusion of the attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include nas-port acct-start enable
```
- Use the **no** version to restore the default, enable.

radius nas-port-format

- Use to set the NAS-Port format attribute for ATM and Ethernet only to either *0ssssppp* or *ssss0ppp*.
- The format is a 4-octet integer. The remaining bits are not changed (8 bits VPI and 16 bits VCI; or 12 bits S-VLAN and 12 bits VLAN).
- The *s* indicates a bit used to represent the *slot*; the *p* indicates a bit used to represent the *port* from which the authentication request originates.
- Example: If the PPP user is received on a VC from the card in slot 7, port 2, then the bit pattern is either 00111010 (for *0ssssppp*) or 01110010 (for *ssss0ppp*).
`host1(config)#radius nas-port-format 0ssssppp`
- Use the **no** version to restore the default.

radius nas-port-format extended atm**radius nas-port-format extended ethernet**

- Use to set the NAS-Port format attribute for ATM, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces on the E120 and E320 routers only.
- The format attribute set using the **radius nas-port-format** command does not accommodate the number of bits required by the ATM interface specifier (*slot/adapter/port/vpi/vci*) or the Gigabit Ethernet and 10-Gigabit Ethernet interface specifier [*slot/adapter/port*] [*.vlanSubinterface*]. Issuing this command enables you to encode the interface information in the attribute by specifying the number of bits available for each field in the interface specifier.



NOTE: You must use this command with the **extended** keyword when you configure the NAS-Port format attribute on routers that have line modules that support more than seven physical ports.

- The default number of bits for each field in the interface specifier for ATM interfaces are:
 - Slot—5 bits
 - Adapter—0 bits
 - Port—3 bits
 - VPI—8 bits
 - VCI—16 bits
- The default number of bits for each field in the interface specifier for Gigabit Ethernet and 10-Gigabit Ethernet interfaces are:
 - Slot—5 bits
 - Adapter—0 bits
 - Port—3 bits
 - VLAN—12 bits
 - S-VLAN—12 bits
- To set valid S-VLAN widths on Gigabit Ethernet and 10-Gigabit Ethernet interfaces, you must include S-VLAN IDs in the NAS-Port attribute by issuing the **radius vlan nas-port-format stacked** command.

- The total number of bits for all fields cannot exceed 32. When the total number of bits is less than 32, the NAS-Port attribute is right-justified and the extra bits are set to 0. If you do not specify a value for a field, the number of bits is set to 0.
- Example 1—Sets the field widths for ATM interfaces

```
host1(config)#radius nas-port-format extended atm field-widths slot 4 adapter 1 vpi 7 vpi 17
```
- Example 2—Sets the field widths for Gigabit Ethernet and 10-Gigabit Ethernet interfaces

```
host1(config)#radius nas-port-format extended ethernet field-widths slot 4 adapter 1 port 3 vlan 12
```
- Use the **no** version to restore the default behavior of the **radius nas-port-format** command.

radius pppoe nas-port-format unique

- Use to set the NAS-Port attribute to a unique value for subscribers on PPPoE interface. This unique value is derived from the subscriber's profileHandle.
- Example

```
host1(config)#radius pppoe nas-port-format unique
```
- Use the **no** version to return to the default, in which the value is determined by the interface.

radius vlan nas-port-format stacked

- Use to include the S-VLAN ID, in addition to the VLAN ID, in the NAS-Port attribute for subscribers on Ethernet interfaces.
- The VLAN ID is always included whether the S-VLAN ID inclusion feature is enabled or disabled.
- The **radius pppoe nas-port-format unique** command overrides this command.
- Example

```
host1(config)#radius vlan nas-port-format stacked
```
- Use the **no** version to return to the default, in which the S-VLAN ID is not included.

show radius nas-port-format***show radius nas-port-format extended***

- Use to display the setting for the NAS-Port attribute.
- Example 1—Displays information about NAS-Port attribute

```
host1#show radius nas-port-format
0ssssppp
```
- Example 2—Displays information about the NAS-Port attribute on an ATM interface on an E320 router

```
host1#show radius nas-port-format extended atm
extended atm field-width slot 5 adapter 0 port 4 vpi 4 vci 12
```

show radius pppoe nas-port-format

- Use to display the status of NAS-Port attribute settings for PPPoE interfaces.
- Example

```
host1#show radius pppoe nas-port-format
unique
```

show radius vlan nas-port-format

- Use to display the status of the S-VLAN ID setting for the NAS-Port attribute for VLAN interfaces. The string **vlan stacked** indicates that the S-VLAN ID is included.
- Example

```
host1#show radius vlan nas-port-format
vlan stacked
```

[8] Framed-IP-Address

Use the following command to manage the Framed-IP-Addr RADIUS attribute.

- **radius include framed-ip-addr**

radius include framed-ip-addr

- Use to include the Framed-Ip-Address attribute in Acct-Start and Acct-Stop messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include framed-ip-addr acct-start enable
```
- Use the **no** version to restore the default, enable.

[9] Framed-Ip-Netmask

Use the following commands to manage the Framed-IP-Netmask RADIUS attribute.

- **radius include framed-ip-netmask**
- **radius ignore framed-ip-netmask**

radius include framed-ip-netmask

- Use to include the Framed-Ip-Netmask attribute in Acct-Start or Acct-Stop messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include framed-ip-netmask acct-start enable
```
- Use the **no** version to restore the default, enable.

radius ignore framed-ip-netmask

- Use to cause the Framed-Ip-Netmask attribute to be ignored in Access-Accept messages.
- You can control this behavior by enabling or disabling this command.
- If the subnet mask is specified by the Frame-Ip-Netmask attribute in the RADIUS user profile, the router passes the mask and IP address to the CPE during IPCP negotiations. When this command is enabled, the default subnet mask 255.255.255.255 is provided by AAA and used for IPCP negotiations.
- Enabling the command guards against any breaks in the negotiation.
- Example

```
host1(config)#radius ignore framed-ip-netmask disable
```
- Use the **no** version to restore the default, enable.

[13] Framed-Compression

Use the following command to manage the Framed-Compression RADIUS attribute.

- **radius include framed-compression**

radius include framed-compression

- Use to include the Framed-Compression attribute in Acct-Start or Acct-Stop messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include framed-compression acct-start disable
```
- Use the **no** version to restore the default, enable.

[25] Class

Use the following command to manage the Class RADIUS attribute.

- **radius include class**

radius include class

- Use to include the Class attribute in Acct-Start or Acct-Stop messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include class acct-start disable
```
- Use the **no** version to restore the default, enable.

[30] Called-Station-Id

Use the following command to manage the Called-Station-Id RADIUS attribute.

- **radius include called-station-id**

radius include called-station-id

- Use to include the Called-Station-Id attribute in Access-Request, Acct-Start, or Acct-Stop messages.
- You can control inclusion of the Called-Station-Id attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include called-station-id acct-start enable
```
- Use the **no** version to restore the default, enable.

[31] Calling-Station-Id

Use the following commands to manage and display information for the Calling-Station-Id RADIUS attribute.

- **radius calling-station-format**
- **radius calling-station-delimiter**
- **radius include calling-station-id**
- **radius override calling-station-id remote-circuit-id**
- **show radius calling-station-format**
- **show radius calling-station-delimiter**
- **show radius override**

radius calling-station-format

- Use to specify the format of the Calling-Station-Id [31] attribute on a virtual router.
- For each field in angle brackets (< >) in the Calling-Station-Id formats, the virtual router supplies the actual value for your configuration, unless otherwise specified.
- To specify that the RADIUS client use the delimited format when the PPP user is terminated at the non-LNS E-series router, use the **delimited** keyword.
 - Format for ATM interfaces:
 < delimiter > < system name > < delimiter > < interface > < delimiter >
 < VPI > < delimiter > < VCI > < delimiter >
 - Format for Ethernet interfaces:
 < delimiter > < system name > < delimiter > < interface > < delimiter >
 < VLAN >

Where < interface > is one of the following items:

- < port name > —The default setting
- < VP description > —Appears if you use the **atm vp-description** command to assign a text description to an individual VP on an ATM interface
- < VC description > —Appears if you use the **atm atm1483 description** command to assign a text description to VCs on an ATM 1483 subinterface and you use the **atm1483 export-subinterface-description** command to enable sending of VC interface descriptors to AAA
- To specify that the RADIUS client use a fixed format of up to 15 characters consisting of all ASCII fields, use the **fixed-format** keyword. The maximum number of characters for each field is shown in square brackets ([]).
 - Format for ATM interfaces:
 < system name [4] > < slot [2] > < port [1] > < VPI [3] > < VCI [5] >
 - Format for Ethernet interfaces:
 < system name [4] > < slot [2] > < port [1] > < VLAN [8] >
 - Format for serial interfaces:
 < system name [4] > < slot [2] > < port [1] > < 0 [8] >

Where the final 8-byte field is always 0 (zero).
- In the case of PPP terminated at the LNS, the Calling-Station-Id attribute is based on the received L2TP calling number AVP.
- To specify that the RADIUS client use a fixed format of up to 15 characters consisting of all ASCII fields with a 1-byte slot field, 1-byte adapter field, and 1-byte port field, use the **fixed-format-adapter-embedded** keyword. The maximum number of characters for each field is shown in square brackets ([]).
 - Format for ATM interfaces:
 < system name [4] > < slot [1] > < adapter [1] > < port [1] >
 < VPI [3] > < VCI [5] >
 - Format for Ethernet interfaces:
 < system name [4] > < slot [1] > < adapter [1] > < port [1] >
 < VLAN [8] >

- Format for serial interfaces:
`<system name [4]> <slot [1]> <adapter [1]> <port [1]> <0 [8]>`
 Where the final 8-byte field is always 0 (zero).
- For E120 and E320 routers, `<adapter>` is the number of the bay in which the I/O adapter (IOA) resides, either 0 (representing the right IOA bay on the E120 router or the upper IOA bay on the E320 router) or 1 (representing the left IOA bay on the E120 router or the lower IOA bay on the E320 router). For ERX-7xx models, ERX-14xx models, and ERX-310 routers, `<adapter>` is always shown as 0 (zero).
- Slot numbers 0 through 16 are shown as ASCII characters in the 1-byte slot field according to the following translation:

Slot Number	ASCII Character	Slot Number	ASCII Character
0	0	9	9
1	1	10	A
2	2	11	B
3	3	12	C
4	4	13	D
5	5	14	E
6	6	15	F
7	7	16	G
8	8	–	–

For example, slot 16 is shown as the ASCII character uppercase G.

- To specify that the RADIUS client use a fixed format of up to 17 characters consisting of all ASCII fields with a 2-byte slot field, 1-byte adapter field, and 2-byte port field, use the **fixed-format-adapter-new-field** keyword. The maximum number of characters for each field is shown in square brackets ([]).



NOTE: You must use this command with the **fixed-format-adapter-new-field** keyword when you configure the format of the Calling-Station-ID attribute on routers that have line modules that support more than seven physical ports.

- Format for ATM interfaces:
`<system name [4]> <slot [2]> <adapter [1]> <port [2]>
 <VPI [3]> <VCI [5]>`
- Format for Ethernet interfaces:
`<system name [4]> <slot [2]> <adapter [1]> <port [2]>
 <VLAN [8]>`
- Format for serial interfaces:
`<system name [4]> <slot [2]> <adapter [1]> <port [2]> <0 [8]>`
 Where the final 8-byte field is always 0 (zero).

- For E120 and E320 routers, <adapter> is the number of the bay in which the I/O adapter (IOA) resides, either 0 or 1. For ERX-7xx models, ERX-14xx models, and ERX-310 routers, <adapter> is always shown as 0 (zero).
- Slot numbers 0 through 16 are shown as integers in the 2-byte slot field.
- Attribute 31, Calling-Station-Id, is used with Attribute 30, Called-Station-Id, in a standard way when the router is the LNS and the LAC is a dial-up LAC (not an E-series router). When the LNS receives the Calling-Station-Id and Called-Station-Id AVPs, the router includes the values as they are, with no format changes in the RADIUS messages.

- Example 1

host1(config)#**radius calling-station-format fixed-format**

For example, when you configure this Calling-Station-Id format on an E320 router for an ATM interface on slot 14, adapter 1, port 2, VCI 3, and VPI 4, the virtual router displays the format in ASCII as '14' '2' '003' '00004'. The adapter number does not appear in this format.

- Example 2

host1(config)#**radius calling-station-format fixed-format-adapter-embedded**

For example, when you configure this Calling-Station-Id format on an E320 router for an ATM interface on slot 14, adapter 1, port 2, VCI 3, and VPI 4, the virtual router displays the format in ASCII as 'E' '1' '2' '003' '00004'.

- Example 3

host1(config)#**radius calling-station-format fixed-format-adapter-new-field**

For example, when you configure this Calling-Station-Id format on an E320 router for an ATM interface on slot 14, adapter 1, port 2, VCI 3, and VPI 4, the virtual router displays the format in ASCII as '14' '1' '02' '003' '00004'.

- Use the **no** version to restore the default Calling-Station-Id format, **delimited**.

radius calling-station-delimiter

- Use to specify the Calling-Station-Id attribute's delimiter for DSL PPP users.
- The delimiter is one special character you select to set off items in the Calling-Station-Id's definition (for example, # or %).

- Example

host1(config)#**radius calling-station-delimiter &**

- Use the **no** version to remove the delimiter.

radius include calling-station-id

- Use to include the Calling-Station-Id attribute in Access-Request, Acct-Start, or Acct-Stop messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include calling-station-id acct-start disable
```
- Use the **no** version to restore the default, enable.

radius override calling-station-id remote-circuit-id

- Use to configure RADIUS to override the standard use of the Calling-Station-Id attribute and instead use the remote circuit ID transmitted from a DSLAM device.
- Example

```
host1(config)#radius override calling-station-id remote-circuit-id
```
- Use the **no** version to restore the default Calling-Station-ID value, which is the telephone number from which the call originated.

show radius calling-station-format

- Use to display the format configured for the Calling-Station-Id [31] attribute.
- Example

```
host1#show radius calling-station-format
fixed-format-adapter-new-field
```

show radius calling-station-delimiter

- Use to display the delimiter used in the Calling-Station-Id for authenticated ATM PPP users.
- Example

```
host1#show radius calling-station-delimiter
&
```

show radius override

- Use to display the current override settings configured for NAS-IP-Address [4], NAS-Port-Id [87], Calling-Station-Id [31], and NAS-Identifier [32] RADIUS.
- You can use the **radius override calling-station-id remote-circuit-id** command to override the standard Calling-Station-Id attribute with the PPPoE remote circuit ID transmitted from the DSLAM.
- Example

```
host1#show radius override
nas-ip-addr:      nas-ip-addr
nas-port-id:      remote-circuit-id
calling-station-id: remote-circuit-id
nas-info:         from current virtual router
```

[32] NAS-Identifier

Use the following commands to manage and display information for the NAS-Identifier RADIUS attribute.

- **radius nas-identifier**
- **radius include nas-identifier**
- **radius override nas-info**
- **radius remote-circuit-id-format**
- **radius remote-circuit-id-delimiter**
- **show radius nas-identifier**
- **show radius override**
- **show radius remote-circuit-id-format**
- **show radius remote-circuit-id-delimiter**

radius nas-identifier

- Use to set a value for the NAS-Identifier attribute. This value is used in the NAS-Identifier attribute for authentication and accounting requests.
- Example

```
host1(config)#radius nas-identifier fox
```
- Use the **no** version to delete the NAS-Identifier.

radius include nas-identifier

- Use to include the NAS-Identifier attribute in Access-Request, Acct-Start, Acct-Stop, Acct-On, and Acct-Off messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include nas-identifier acct-start disable
```
- Use the **no** version to restore the default, enable.

radius override nas-info

- Use in the correct virtual router context to override the standard use of NAS-IP-Address and NAS-Identifier attributes for AAA broadcast accounting; specifies that the attributes for the authentication virtual router be included in accounting packets instead of the attributes for the virtual router that generates the accounting information.
- Example

```
host1(config)#virtual-router vrXyz1  
host1:vrXyz1(config)#radius override nas-info
```
- Use the **no** version to restore the standard use of the NAS-IP-Address and NAS-Identification attributes.

radius remote-circuit-id-format

- Use to configure the format of the PPPoE remote circuit ID value captured from a DSLAM.
- You can format the PPPoE remote circuit ID value to include either or both of the agent-circuit-ID (suboption 1) and agent-remote-id (suboption 2) suboptions of the DHCP relay agent information option (option 82) or the PPPoE intermediate agent tags.
- By default, the router formats the PPPoE remote circuit ID to include only the agent-circuit-id suboption.
- You can use this command to configure the following nondefault formats for the PPPoE remote circuit ID value:
 - Include either or both of the agent-circuit-id and agent-remote-id suboptions, with or without the NAS-Identifier [32] RADIUS attribute
 - Append the agent-circuit-id suboption value to an interface specifier that is consistent with the recommended format in the [DSL Forum Technical Report \(TR\)-101—Migration to Ethernet-Based DSL Aggregation \(April 2006\)](#).
- For more information about how to use this command, see [Using the PPPoE Remote Circuit ID to Identify Subscribers](#) and [Configuring PPPoE Remote Circuit ID Capture](#) in *JUNOS Link Layer Configuration Guide, Chapter 7, Configuring Point-to-Point Protocol over Ethernet*.
- Examples


```
host1(config)#radius remote-circuit-id-format nas-identifier agent-circuit-id
agent-remote-id

host1(config)#radius remote-circuit-id-format dsl-forum-1
```
- Use the **no** version to restore the default format, agent-circuit-id.

radius remote-circuit-id-delimiter

- Use to configure the delimiter character that the router uses to set off multiple components in the format of the PPPoE remote circuit ID value captured from a DSLAM.
- For information about how to use this command, see [Configuring PPPoE Remote Circuit ID Capture](#) in *JUNOS Link Layer Configuration Guide, Chapter 7, Configuring Point-to-Point Protocol over Ethernet*.
- Example


```
host1(config)#radius remote-circuit-id-delimiter !
```
- Use the **no** version to restore the default delimiter character, #.

show radius nas-identifier

- Use to display the NAS-Identifier value.
- Example


```
host1#show radius nas-identifier
fox
```

show radius override

- Use to display the current setting for both the NAS-IP-Address and the NAS-Identifier. This setting can be changed with the **radius override nas-info** command, which is used for AAA broadcast accounting.
- Example


```
host1#show radius override
nas-ip-addr: nas-ip-addr
nas-info:      from authentication virtual router
```

show radius remote-circuit-id-format

- Use to display the format configured for the PPPoE remote circuit ID value captured from a DSLAM.
- If the PPPoE remote circuit ID value is configured to include any or all of the agent-circuit-id, agent-remote-id, and nas-identifier components, the display lists the components included and the order in which they appear.
- If the PPPoE remote circuit ID value is configured to use the format for the **dsl-forum-1** keyword of the **radius remote-circuit-id-format** command, the display indicates that this format is in effect.
- The default format is agent-circuit-ID.
- Example


```
host1#show radius remote-circuit-id-format
nas-identifier agent-circuit-id agent-remote-id
```

show radius remote-circuit-id-delimiter

- Use to display the delimiter character configured to set off components in the PPPoE remote circuit ID value captured from a DSLAM.
- The default delimiter character is #.
- Example


```
host1#show radius remote-circuit-id-delimiter
!
```

[41] Acct-Delay-Time

Use the following commands to manage and display information for the Acct-Delay-Timer RADIUS attribute.

- **radius include acct-delay-time**

radius include acct-delay-time

- Use to include the Acct-Delay-Time attribute in Acct-On or Acct-Off messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example


```
host1(config)#radius include acct-delay-time acct-on enable
```
- Use the **no** version to restore the default, enable.

[44] Acct-Session-Id

Use the following commands to manage and display information for the Acct-Session-Id RADIUS attribute.

- **radius include acct-session-id**
- **radius acct-session-id-format**
- **show radius acct-session-id-format**

radius include acct-session-id

- Use to include the Acct-Session-Id attribute in Access-Request, Acct-On, or Acct-Off messages.
- You can control inclusion of the Acct-Session-Id attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include acct-session-id access-request disable
```
- Use the **no** version to restore the default, enable.

radius acct-session-id-format

- Use to set the Acct-Session-Id attribute format. Two formats are supported:
 - **description**—Configures RADIUS client to use the generic format: **erx < interface identifier > : < hex number > .** For example: **erx atm 12/1:0.3:0000ef1**
 - **decimal**—Configures the RADIUS client to use a decimal format. For example: **435264**
- Example

```
host1(config)#radius acct-session-id-format decimal
```
- Use the **no** version to negate the Acct-Session-Id format.

show radius acct-session-id-format

- Use to display the format used for the Acct-Session-Id attribute.
- Example

```
host1#show radius acct-session-id-format
decimal
```


[45] Acct-Authentic

Use the following command to manage the Acct-Authentic RADIUS attribute.

- **radius include acct-authentic**

radius include acct-authentic

- Use to include the Acct-Authentic attribute in Acct-On or Acct-Off messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example
host1(config)#**radius include acct-authentic acct-on enable**
- Use the **no** version to restore the default, enable.

[49] Acct-Terminate-Cause

Use the following command to manage the Acct-Terminate-Cause RADIUS attribute.

- **radius include acct-terminate-cause**

radius include acct-terminate-cause

- Use to include the Acct-Terminate-Cause attribute in Acct-Off messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example
host1(config)#**radius include acct-terminate-cause acct-off disable**
- Use the **no** version to restore the default, enable.

[50] Acct-Multi-Session-Id

Use the following command to manage the Acct-Multi-Session-Id RADIUS attribute.

- **radius include acct-multi-session-id**

radius include acct-multi-session-id

- Use to include the Acct-Multi-Session-Id attribute in Access-Request, Acct-Start, or Acct-Stop messages.
- You can control inclusion of the Acct-Multi-Session-Id attribute by enabling or disabling this command.
- Example
host1(config)#**radius include acct-multi-session-id acct-stop disable**
- Use the **no** version to restore the default, enable for accounting messages and disable for access requests.

[51] Acct-Link-Count

Use the following command to manage the Acct-Link-Count RADIUS attribute.

- **radius include acct-link-count**

radius include acct-link-count

- Use to include the Acct-Link-Count attribute in Acct-Start and Acct-Stop messages.
- You can control inclusion of the Acct-Input-Gigawords attribute by enabling or disabling this command.
- Example
host1(config)#**radius include acct-link-count acct-stop disable**
- Use the **no** version to restore the default, enable.

[52] Acct-Input-Gigawords

Use the following command to manage the Acct-Input-Gigawords RADIUS attribute.

- **radius include input-gigawords**

radius include input-gigawords

- Use to include the Acct-Input-Gigawords attribute in Acct-Stop messages.
- You can control inclusion of the Acct-Input-Gigawords attribute by enabling or disabling this command.
- Example
host1(config)#**radius include input-gigawords acct-stop disable**
- Use the **no** version to restore the default, enable.

[53] Output-Gigawords

Use the following command to manage the Acct-Output-Gigawords RADIUS attribute.

- **radius include output-gigawords**

radius include output-gigawords

- Use to include the Acct-Output-Gigawords attribute in Acct-Stop messages.
- You can control inclusion of the Acct-Output-Gigawords attribute by enabling or disabling this command.
- Example
host1(config)#**radius include output-gigawords acct-stop enable**
- Use the **no** version to restore the default, enable.

[55] Event-Timestamp

Use the following command to manage the Acct-Output-Gigawords RADIUS attribute.

- **radius include event-timestamp**

radius include event-timestamp

- Use to include the Event-Timestamp attribute in Acct-Start, Acct-Stop, Acct-On, or Acct-Off messages.
- You can control inclusion of the Event-Timestamp attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include event-timestamp acct-on enable
```
- Use the **no** version to restore the default, enable.

[61] NAS-Port-Type

Use the following commands to manage and display information for the NAS-Port-Type RADIUS attribute.

- **radius dsl-port-type**
- **radius ethernet-port-type**
- **radius include nas-port-type**
- **show radius dsl-port-type**
- **show radius ethernet-port-type**

radius dsl-port-type

- Use to configure the NAS-Port-Type attribute for the DSL port type.
- This attribute can have several values. If the interface (port) is DSL, then the attribute can have any value listed in the command and uses the value configured. If the interface (port) is Ethernet, then it sets the attribute to Ethernet and disregards the parameter set with this command. Options include:
 - **adsl-cap**—Asymmetric DSL, carrierless amplitude phase (CAP) modulation
 - **adsl-dmt**—Asymmetric DSL, discrete multitone (DMT)
 - **idsl**—ISDN DSL
 - **sdsl**—Symmetric DSL
 - **virtual**—Virtual
 - **xdsl**—DSL of unknown type
- Example

```
host1(config)#radius dsl-port-type xsdsl
```
- Use the **no** version to restore the default, xsdsl.

radius ethernet-port-type

- Use to set the NAS-Port-Type attribute for Ethernet interfaces to **ethernet** or **virtual**.
- Example
host1(config)#**radius ethernet-port-type virtual**
- Use the **no** version to restore the default, ethernet.

radius include nas-port-type

- Use to include the NAS-Port-Type attribute in Access-Request, Acct-Start, and Acct-Stop messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example
host1(config)#**radius include nas-port-type acct-start enable**
- Use the **no** version to restore the default, enable.

show radius dsl-port-type

- Use to display the DSL port type for NAS-Port-Type attribute for ATM users.
- Example
host1#**show radius dsl-port-type**
xds1

show radius ethernet-port-type

- Use to display the NAS-Port-Type attribute for Ethernet interfaces.
- Example
host1#**show radius ethernet-port-type**
virtual

[64] Tunnel-Type

Use the following command to manage the Tunnel-Type RADIUS attribute.

- **radius include tunnel-type**

radius include tunnel-type

- Use to include the Tunnel-Type attribute in Access-Request, Acct-Start, and Acct-Stop messages.
- You can control inclusion of the Tunnel-Type attribute by enabling or disabling this command.
- Example
host1(config)#**radius include tunnel-type access-request enable**
- Use the **no** version to restore the default, enable.

[65] Tunnel-Medium-Type

Use the following command to manage the Tunnel-Type-Medium RADIUS attribute.

- **radius include tunnel-medium-type**

radius include tunnel-medium-type

- Use to include the Tunnel-Medium-Type attribute in Access-Request, Acct-Start, and Acct-Stop messages.
- You can control inclusion of the Tunnel-Medium-Type attribute by enabling or disabling this command.
- Example
host1(config)#**radius include tunnel-medium-type acct-start enable**
- Use the **no** version to restore the default, enable.

[66] Tunnel-Client-Endpoint

Use the following command to manage the Tunnel-Client-Endpoint RADIUS attribute.

- **radius include tunnel-client-endpoint**

radius include tunnel-client-endpoint

- Use to include the Tunnel-Client-Endpoint attribute in Access-Request, Acct-Start, and Acct-Stop messages.
- You can control inclusion of the Tunnel-Client-Endpoint attribute by enabling or disabling this command.
- Example
host1(config)#**radius include tunnel-client-endpoint acct-start enable**
- Use the **no** version to restore the default, enable.

[67] Tunnel-Server-Endpoint

Use the following command to manage the Tunnel-Server-Endpoint RADIUS attribute.

- **radius include tunnel-server-endpoint**

radius include tunnel-server-endpoint

- Use to include the Tunnel-Server-Endpoint attribute in Access-Request, Acct-Start, and Acct-Stop messages.
- You can control inclusion of the Tunnel-Server-Endpoint attribute by enabling or disabling this command.
- Example
host1(config)#**radius include tunnel-server-endpoint acct-stop disable**
- Use the **no** version to restore the default, enable.

[68] Acct-Tunnel-Connection

Use the following command to manage the Acct-Tunnel-Connection RADIUS attribute.

- **radius include acct-tunnel-connection**

radius include acct-tunnel-connection

- Use to include the Acct-Tunnel-Connection attribute in Access-Request, Acct-Start, or Acct-Stop messages.
- You can control inclusion of the Acct-Tunnel-Connection attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include acct-tunnel-connection acct-stop enable
```
- Use the **no** version to restore the default, enable.

[77] Connect-Info

Use the following commands to manage and display information for the Connect-Info RADIUS attribute.

- **radius connect-info-format l2tp-connect-speed**
- **radius include connect-info**
- **show radius connect-info-format**

radius connect-info-format

- Use on the LNS to enable the generation of the RADIUS Connect-Info attribute and to specify the attribute's format. The attribute is based on the L2TP connect-speed AVPs for received (RX) speed (AVP 38) and transmit (TX) speed (AVP 24). See [Configuring the RX Speed on the LAC](#) on page 235 for information about generating the RX and TX speed AVPs.
- The Connect-Info attribute is a string in the following format; the attribute is generated whenever the TX speed is not zero.

```
tx-speed [ /rx-speed ]
```
- The TX speed is always included in the attribute when the speed is not zero; however, inclusion of the RX speed depends on the keyword you use with the command.
 - Use the **l2tp-connect-speed** keyword to specify that the RX speed is only included when it is not zero and differs from the TX speed.
 - Example

```
host1(config)#radius connect-info-format l2tp-connect-speed
```

- Use the **l2tp-connect-speed-rx-when-equal** keyword to specify that the RX speed is always included when it is not zero.

- Example

```
host1(config)#radius connect-info-format l2tp-connect-speed-rx-when-equal
```

- Use the **no** version to disable the inclusion of the RX speed when it is the same as the TX speed.

radius include connect-info

- Use to include the Connect-Info attribute in Access-Request, Acct-Start, or Acct-Stop messages.
- You can control inclusion of the Connect-Info attribute by enabling or disabling this command.

- Example

```
host1(config)#radius include connect-info access-request disable
```

- Use the **no** version to restore the default, enable.

show radius connect-info-format

- Use to display the format for the Connect-Info attribute.

- Example

```
host1(config)#show radius connect-info-format
l2tp-connect-speed-rx-when-equal
```

[82] Tunnel-Assignment-Id

Use the following command to manage the Tunnel-Assignment-Id RADIUS attribute.

- **radius include tunnel-assignment-id**

radius include tunnel-assignment-id

- Use to include the Tunnel-Assignment-Id attribute in Acct-Start or Acct-Stop messages.
- You can control inclusion of the Tunnel-Assignment-Id attribute by enabling or disabling this command.

- Example

```
host1(config)#radius include tunnel-assignment-id acct-stop enable
```

- Use the **no** version to restore the default, enable.

[83] Tunnel-Preference

Use the following command to manage the Tunnel-Preference RADIUS attribute.

- **radius include tunnel-preference**

radius include tunnel-preference

- Use to include the Tunnel-Preference attribute in Acct-Start or Acct-Stop messages.
- You can control inclusion of the Tunnel-Preference attribute by enabling or disabling this command.
- Example
host1(config)#**radius include tunnel-preference acct-start enable**
- Use the **no** version to restore the default, enable.

[87] NAS-Port-Id

Use the following commands to manage and show information for the NAS-Port-Id RADIUS attribute.

- **aaa intf-desc-format include**
- **radius include nas-port-id**
- **radius override nas-port-id remote-circuit-id**
- **show aaa intf-desc-format**
- **show radius override**

aaa intf-desc-format include

- Use to specify whether the router includes the subinterface number or adapter in the interface description it passes to RADIUS for inclusion in the NAS-Port-Id attribute. By default, the subinterface and adapter are sent (the commands are enabled).
- Examples
host1#**aaa intf-desc-format include sub-intf disable**
host1#**aaa intf-desc-format include adapter enable**
- Use the **no** version to remove the configuration.

radius include nas-port-id

- Use to include the NAS-Port-Id attribute in the Access-Request, Acct-Start, or Acct-Stop messages.
- You can control inclusion of the NAS-Port-Id attribute by enabling or disabling this command.
- Example
host1(config)#**radius include nas-port-id access-request enable**
- Use the **no** version to restore the default, enable.

radius override nas-port-id remote-circuit-id

- Use to configure RADIUS to override the standard use of the NAS-Port-Id attribute and instead use the remote circuit ID transmitted from a DSLAM device.
- Example

```
host1(config)#radius override nas-port-id remote-circuit-id
```
- Use the **no** version to restore the default NAS-Port-ID value, which is the physical interface of the NAS that is authenticating the user.

show aaa intf-desc-format

- Use to display whether the router includes or excludes the subinterface number or adapter in the interface description that the router passes to RADIUS for inclusion in the NAS-Port-Id attribute.
- Example

```
host1#show aaa intf-desc-format
exclude sub-interface
include adapter
```

show radius override

- Use to display the current override settings for the NAS-IP-Address [4], NAS-Port-Id [87], Calling-Station-Id [31], and NAS-Identifier [32] attributes.
- You can use the **radius override nas-port-id remote-circuit-id** command to override the standard NAS-Port-Id attribute with the PPPoE remote circuit ID transmitted from the DSLAM.
- Example

```
host1#show radius override
nas-ip-addr:      nas-ip-addr
nas-port-id:      remote-circuit-id
calling-station-id: remote-circuit-id
nas-info:         from current virtual router
```

[90] Tunnel-Client-Auth-Id

Use the following command to manage the Tunnel-Client-Auth-Id RADIUS attribute.

- **radius include tunnel-client-auth-id**

radius include tunnel-client-auth-id

- Use to include the Tunnel-Client-Auth-Id attribute in Access-Request, Acct-Start, or Acct-Stop messages.
- You can control inclusion of the Tunnel-Client-Auth-Id attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include tunnel-client-auth-id access-request disable
```
- Use the **no** version to restore the default, enable.

[91] Tunnel-Server-Auth-Id

Use the following command to manage the Tunnel-Server-Auth-Id RADIUS attribute.

- **radius include tunnel-server-auth-id**

radius include tunnel-server-auth-id

- Use to include the Tunnel-Server-Auth-Id attribute in Access-Request, Acct-Start, or Acct-Stop messages.
- You can control inclusion of the Tunnel-Server-Auth-Id attribute by enabling or disabling this command.
- Example
host1(config)#**radius include tunnel-server-auth-id acct-start enable**
- Use the **no** version to restore the default, enable.

[188] Ascend-Num-In-Multilink

Use the following command to manage the Ascend-Num-In-Multilink attribute.

- **radius include ascend-num-in-multilink**

radius include ascend-num-in-multilink

- Use to include the Ascend-Num-In-Multilink attribute in Access-Request, Acct-Start, or Acct-Stop messages.
- You can control inclusion of the Ascend-Num-In-Multilink attribute by enabling or disabling this command.
- Example
host1(config)#**radius include ascend-num-in-multilink acct-start enable**
- Use the **no** version to restore the default, disable.

All Tunnel Server Attributes

Use the following command to manage all tunnel server RADIUS attributes.

- **radius include tunnel-server-attributes**

radius include tunnel-server-attributes

- Use to include all supported tunnel server attributes in Access-Request, Acct-Start, or Acct-Stop messages.
- When the router functions as an LNS with a terminating PPP, then the LAC tunnel attributes are included.
- You can control inclusion of all tunnel server attributes by enabling or disabling this command.
- Example
host1(config)#**radius include tunnel-server-attributes access-request enable**
- Use the **no** version to restore the default, disable.

Juniper Networks Vendor-Specific Attributes

This section describes the Juniper Networks vendor-specific attributes (VSAs) that you can configure using CLI commands. The attributes are listed numerically and are followed by descriptions about the commands that you can use to manage the attribute.

[26-1] Virtual-Router

Use the following command to manage the Virtual-Router RADIUS attribute.

- **radius ignore virtual-router**

radius ignore virtual-router

- Use to cause the Virtual-Router attribute to be ignored in Access-Accept messages.
- You can control this behavior by enabling or disabling this command.
- Example
host1(config)#**radius ignore virtual-router enable**
- Use the **no** version to restore the default, disable.

[26-10] Ingress-Policy-Name

Use the following commands to manage the Ingress-Policy-Name RADIUS attribute.

- **radius include ingress-policy-name**
- **radius ignore ingress-policy-name**

radius include ingress-policy-name

- Use to include the Ingress-Policy-Name attribute in Acct-Start or Acct-Stop messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example
host1(config)#**radius include ingress-policy-name acct-start enable**
- Use the **no** version to restore the default.

radius ignore ingress-policy-name

- Use to cause the Ingress-Policy-Name attribute to be ignored in Access-Accept messages.
- You can control this behavior by enabling or disabling this command. The default is **disable**.
- Example
host1(config)#**radius ignore ingress-policy-name enable**
- Use the **no** version to restore the default, enable.

[26-11] Egress-Policy-Name

Use the following commands to manage the Egress-Policy-Name RADIUS attribute.

- **radius include egress-policy-name**
- **radius ignore egress-policy-name**

radius include egress-policy-name

- Use to include the Egress-Policy-Name attribute in Acct-Start or Acct-Stop messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include egress-policy-name acct-start enable
```
- Use the **no** version to restore the default, enable.

radius ignore egress-policy-name

- Use to cause the Egress-Policy-Name attribute to be ignored in Access-Accept messages.
- You can control this behavior by enabling or disabling this command.
- Example

```
host1(config)#radius ignore egress-policy-name enable
```
- Use the **no** version to restore the default, disable.

[26-14] Service-Category

Use the following command to manage the Service-Category RADIUS attribute.

- **radius ignore atm-service-category**

radius ignore atm-service-category

- Use to cause the Service-Category attribute to be ignored in Access-Accept messages.
- You can control this behavior by enabling or disabling this command.
- Example

```
host1(config)#radius ignore atm-service-category enable
```
- Use the **no** version to restore the default, disable.

[26-15] PCR

Use the following command to manage the PCR RADIUS attribute.

- **radius ignore atm-pcr**

radius ignore atm-pcr

- Use to cause the PCR attribute to be ignored in Access-Accept messages.
- You can control this behavior by enabling or disabling this command.
- Example
host1(config)#**radius ignore atm-pcr enable**
- Use the **no** version to restore the default, disable.

[26-16] SCR

Use the following command to manage the SCR RADIUS attribute.

- **radius ignore atm-scr**

radius ignore atm-scr

- Use to cause the SCR attribute to be ignored in Access-Accept messages.
- You can control this behavior by enabling or disabling this command.
- Example
host1(config)#**radius ignore atm-scr enable**
- Use the **no** version to restore the default, disable.

[26-17] MBS

Use the following command to manage the MBS RADIUS attribute.

- **radius ignore atm-mbs**

radius ignore atm-mbs

- Use to cause the MBS attribute to be ignored in Access-Accept messages.
- You can control this behavior by enabling or disabling this command.
- Example
host1(config)#**radius ignore atm-mbs enable**
- Use the **no** version to restore the default, disable.

[26-24] Pppoe-Description

Use the following command to manage the Pppoe-Description RADIUS attribute.

- **radius include pppoe-description**

radius include pppoe-description

- Use to include the Pppoe-Description attribute in Access-Request, Acct-Start, or Acct-Stop messages.
- You can control inclusion of the Pppoe-Description attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include pppoe-description acct-start enable
```
- Use the **no** version to restore the default, enable.

[26-35] Acct-Input-Gigapackets

Use the following command to manage the Acct-Input-Gigapackets RADIUS attribute.

- **radius include input-gigapkts**

radius include input-gigapkts

- Use to include Acct-Input-Gigapackets in Acct-Stop messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include input-gigapkts acct-stop disable
```
- Use the **no** version to restore the default, enable.

[26-36] Acct-Output-Gigapackets

Use the following command to manage the Acct-Output-Gigapackets RADIUS attribute.

- **radius include output-gigapkts**

radius include output-gigapkts

- Use to include the Acct-Output-Gigapackets attribute in Acct-Stop messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include output-gigapkts acct-stop disable
```
- Use the **no** version to restore the default, enable.

[26-44] Tunnel-Interface-Id

Use the following command to manage the Tunnel-Interface-Id RADIUS attribute.

- **radius include tunnel-interface-id**

radius include tunnel-interface-id

- Use to include the Tunnel-Interface-Id attribute in Access-Request, Acct-Start, or Acct-Stop messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example
host1(config)#**radius include tunnel-interface-id enable**
- Use the **no** version to restore the default, disable.

[26-51] Disconnect-Cause

Use the following command to manage the Disconnect-Cause RADIUS attribute.

- **radius include l2tp-ppp-disconnect-cause**

radius include l2tp-ppp-disconnect-cause

- Use to include the Disconnect-Cause attribute in Acct-Stop and Acct-Tunnel-Link-Stop messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example
host1(config)#**radius include l2tp-ppp-disconnect-cause acct-stop-enable**
- Use the **no** version to restore the default, disable.

[26-53] Service-Description

Use the following command to manage the Service-Description RADIUS attribute.

- **radius include profile-service-description**

radius include profile-service-description

- Use to include the Service-Description attribute in Access-Request, Acct-Start, and Acct-Stop messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example
host1(config)#**radius include profile-service-description acct-stop enable**
- Use the **no** version to restore the default, disable.

[26-55] DHCP-Options

Use the following command to manage the DHCP-Options RADIUS attribute.

- **radius include dhcp-options**

radius include dhcp-options

- Use to include the DHCP-Options attribute in Access-Request, Acct-Start, and Acct-Stop messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include dhcp-options acct-stop enable
```
- Use the **no** version to restore the default, disable.

[26-56] DHCP-MAC-Address

Use the following command to manage the DHCP-MAC-Address RADIUS attribute.

- **radius include dhcp-mac-address**

radius include dhcp-mac-address

- Use to include the DHCP-MAC-Address attribute in Access-Request, Acct-Start, and Acct-Stop messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include dhcp-mac-address acct-stop enable
```
- Use the **no** version to restore the default, disable.

[26-57] DHCP-GI-Address

Use the following command to manage the DHCP-GI-Address RADIUS attribute.

- **radius include dhcp-gi-address**

radius include dhcp-gi-address

- Use to include the DHCP-GI-Address attribute in Access-Request, Acct-Start, and Acct-Stop messages.
- You can control inclusion of the attribute by enabling or disabling this command.
- Example

```
host1(config)#radius include dhcp-gi-address acct-stop enable
```
- Use the **no** version to restore the default, disable.

[26-62] MLPPP-Bundle-Name

Use the following command to manage the MLPPP-Bundle-Name RADIUS attribute.

- **radius include mlppp-bundle-name**

radius include mlppp-bundle-name

- Use to include the MLPPP-Bundle-Name attribute in Access-Request, Acct-Start, Interim-Acct, or Acct-Stop messages.
- You can control inclusion of the MLPPP-Bundle-Name attribute by enabling or disabling this command.
- There is no explicit command to include the MLPPP-Bundle-Name attribute in Interim-Acct messages; however, the attribute is automatically included in Interim-Acct messages when the attribute is enabled for Acct-Stop messages.

- Example

```
host1(config)#radius include mlppp-bundle-name acct-start enable
```

- Use the **no** version to restore the default, disable.

[26-63] Interface-Desc

Use the following command to manage the Interface-Desc RADIUS attribute.

- **radius include interface-description**

radius include interface-description

- Use to include the Interface-Desc attribute, with the subscriber's access interface description, in Access-Request, Acct-Start, Interim-Acct, or Acct-Stop messages.
- You can control inclusion of the Interface-Desc attribute by enabling or disabling this command. Inclusion is disabled by default.
- There is no explicit command to include the Interface-Desc attribute in Interim-Acct messages; however, the attribute is automatically included in Interim-Acct messages when the attribute is enabled for Acct-Stop messages.

- Example

```
host1(config)#radius include interface-description acct-start enable
```

- Use the **no** version to restore the default, disable.

[26-81] L2C-Information

Use the following command to manage the L2C-Information RADIUS attribute.

- **radius include access-loop-parameters**

radius include access-loop-parameters

- Use to include the L2C-Information attribute in Access-Request messages.
- You can control inclusion of the L2C-Information attribute by enabling or disabling this command. Inclusion is disabled by default.

- Example

```
host1(config)#radius include access-loop-parameters access-request enable
```

- Use the **no** version to restore the default, disable.

[26-92] L2C-Up-Stream-Data

Use the following command to manage the L2C-Up-Stream-Data RADIUS attribute.

- **radius include l2c-upstream-data**

radius include l2c-upstream-data

- Use to include the L2C-Up-Stream-Data attribute in Access-Request, Acct-Start, and Acct-Stop messages.
- You can control inclusion of the L2C-Up-Stream-Data attribute by enabling or disabling this command. Inclusion is disabled by default.

- Example

```
host1(config)#radius include l2c-upstream-data access-request enable
```

- Use the **no** version to restore the default, disable.

[26-93] L2C-Down-Stream-Data

Use the following command to manage the L2C-Down-Stream-Data RADIUS attribute.

- **radius include l2c-downstream-data**

radius include l2c-downstream-data

- Use to include the L2C-Down-Stream-Data attribute in Access-Request, Acct-Start, and Acct-Stop messages.
- You can control inclusion of the L2C-Down-Stream-Data attribute by enabling or disabling this command. Inclusion is disabled by default.

- Example

```
host1(config)#radius include l2c-downstream-data access-request enable
```

- Use the **no** version to restore the default, disable.

DSL Forum Vendor-Specific Attributes

You can use the **radius include dsl-forum-attributes** command to control the inclusion of a set of DSL Forum VSAs in Access-Request, Acct-Start, Acct-Stop, and (if Acct-Stop messages are specified) Interim-Acct messages that the router sends to RADIUS.

The DSL Forum VSAs, as defined in [DSL Forum Vendor-Specific RADIUS Attributes—draft-mammoliti-radius-dsl-vsa-02.txt \(September 2006 expiration\)](#), convey information about the associated subscriber for and data rate of the DSL. This information is not otherwise available in the standard set of RADIUS attributes or Juniper Networks VSAs. A service provider might find it useful to enable inclusion of the DSL Forum VSAs in RADIUS messages in order to bill subscribers for different classes of service based on the data rate of their DSL connection.

The router receives data containing one or more of the DSL Forum VSAs from a DSLAM connected to the router via a PPPoE interface. When you enable the inclusion of the DSL Forum VSAs in these RADIUS messages, the router includes all of the following attributes in the specified message type, provided that the VSA is available in the information that the router receives from the DSLAM.



NOTE: The router uses the vendor ID assigned to the DSL Forum (3561, or DE9 in hexadecimal format) by the Internet Assigned Numbers Authority (IANA) for the DSL Forum VSAs.

Agent-Circuit-Id [26-1]	Maximum-Data-Rate-Downstream [26-136]
Agent-Remote-Id [26-2]	Minimum-Data-Rate-Upstream-Low-Power [26-137]
Actual-Data-Rate-Upstream [26-129]	Minimum-Data-Rate-Downstream-Low-Power [26-138]
Actual-Data-Rate-Downstream [26-130]	Maximum-Interleaving-Delay-Upstream [26-139]
Minimum-Data-Rate-Upstream [26-131]	Actual-Interleaving-Delay-Upstream [26-140]
Minimum-Data-Rate-Downstream [26-132]	Maximum-Interleaving-Delay-Downstream [26-141]
Attainable-Data-Rate-Upstream [26-133]	Actual-Interleaving-Delay-Downstream [26-142]
Attainable-Data-Rate-Downstream [26-134]	Access-Loop-Encapsulation [26-144]
Maximum-Data-Rate-Upstream [26-135]	IWF-Session [26-254]

For information about enabling the QoS downstream rate application to obtain downstream rates from the Actual-Data-Rate-Downstream [26-130] DSL Forum VSA, see [QoS Downstream Rate](#) in *JUNOS Quality of Service Configuration Guide, Chapter 11, Configuring QoS Parameters*.

For a more detailed description of the DSL Forum VSAs, see [DSL Forum VSAs](#) in *Appendix A, RADIUS Attribute Descriptions*.

radius include dsl-forum-attributes

- Use to include the set of DSL Forum VSAs in Access-Request, Acct-Start, and Acct-Stop messages that the router sends to RADIUS. If you enable inclusion of the DSL Forum VSAs in Acct-Stop messages, the router also includes the VSAs in Interim-Acct messages.
- You can control inclusion of the DSL Forum VSAs in the specified message type by enabling or disabling this command. Inclusion is disabled by default.
- When you enable inclusion of the DSL Forum VSAs for a specified message type, the router includes in that message all of the DSL Forum attributes that it receives from the DSLAM.
- Example

```
host1(config)#radius include dsl-forum-attributes access-request enable
```
- Use the **no** version to restore the default behavior, disable.

Including or Excluding Attributes in RADIUS Messages

For many attributes, you can configure the router to include or exclude the attribute in RADIUS messages. To see a list of the attributes that you can include or exclude, use the **show radius attributes-included** command.

radius include

- Use to enable or disable the inclusion of RADIUS attributes in Acct-On, Acct-Off, Access-Request, Acct-Start, and Acct-Stop messages.
- Examples

```
host1(config)#radius include ingress-policy-name acct-start enable
```

```
host1(config)#radius include tunnel-type access-request disable
```
- Use the **no** version to restore the default, disable.

Ignoring Attributes When Receiving Access-Accept Messages

You can configure the router to ignore or use many attributes that it receives in Access-Accept messages. To see the list of attributes that the router uses or ignores, use the **show radius attributes-ignored** command.

radius ignore

- Use to specify that a RADIUS attribute be ignored or be accepted from Access-Accept messages.
- Use the **enable** keyword to specify that the RADIUS client ignore the attribute from the RADIUS server or the **disable** keyword to use the attribute.
- Examples

```
host1(config)#radius ignore atm-scr enable
```

```
host1(config)#radius ignore framed-ip-netmask disable
```
- Use the **no** version to restore the default, enable.

Monitoring RADIUS Included and Ignored Attributes

Use the commands described in this section to monitor the status of RADIUS attributes that are included or ignored in RADIUS messages.

show radius attributes-included

- Use to display the RADIUS attributes that are included in and excluded from Acct-On, Acct-Off, Access-Request, Acct-Start, and Acct-Stop messages.
- Field descriptions
 - Attribute Name—Name of the RADIUS attribute
 - Account On—Include status of the attribute in Acct-On messages: enabled, disabled, not configurable (n/c)
 - Account Off—Include status of the attribute in Acct-Off messages: enabled, disabled, n/c
 - Access Request—Include status of the attribute in Access Request messages: enabled, disabled, n/c
 - Account Start—Include status of the attribute in Acct-Start messages: enabled, disabled, n/c
 - Account Stop—Include status of the attribute in Acct-Stop messages: enabled, disabled, n/c
- Example

host1#show radius attributes-included

Attribute Name	Account On	Account Off	Access Request	Account Start	Account Stop
acct-authentic	enabled	enabled	n/c	n/c	n/c
acct-delay-time	enabled	enabled	n/c	n/c	n/c
acct-link-count	n/c	n/c	n/c	enabled	enabled
acct-multi-session-id	n/c	n/c	disabled	enabled	enabled
acct-session-id	enabled	enabled	enabled	n/c	n/c
acct-terminate-cause	n/c	enabled	n/c	n/c	n/c
acct-tunnel-connection	n/c	n/c	enabled	enabled	enabled
ascend-num-in-multilink	n/c	n/c	disabled	disabled	disabled
called-station-id	n/c	n/c	enabled	enabled	enabled
calling-station-id	n/c	n/c	enabled	enabled	enabled
class	n/c	n/c	n/c	enabled	enabled
connect-info	n/c	n/c	enabled	enabled	enabled
dhcp-options	n/c	n/c	disabled	disabled	disabled
dhcp-mac-address	n/c	n/c	disabled	disabled	disabled
dhcp-gi-address	n/c	n/c	disabled	disabled	disabled
dsl-forum-attributes	n/c	n/c	disabled	disabled	disabled
egress-policy-name(vsa)	n/c	n/c	n/c	enabled	enabled
event-timestamp	enabled	enabled	n/c	enabled	enabled
framed-compression	n/c	n/c	n/c	enabled	enabled
framed-ip-address	n/c	n/c	n/c	enabled	n/c
framed-ip-netmask	n/c	n/c	n/c	enabled	enabled
ingress-policy-name(vsa)	n/c	n/c	n/c	enabled	enabled
input-gigapkts(vsa)	n/c	n/c	n/c	n/c	enabled
input-gigawords	n/c	n/c	n/c	n/c	enabled
l2tp-ppp-disconnect-cause	n/c	n/c	n/c	n/c	disabled
interface-description	n/c	n/c	enabled	enabled	enabled
mlppp-bundle-name	n/c	n/c	enabled	enabled	enabled
nas-identifier	enabled	enabled	enabled	enabled	enabled
nas-port	n/c	n/c	enabled	enabled	enabled

nas-port-id	n/c	n/c	enabled	enabled	enabled
nas-port-type	n/c	n/c	enabled	enabled	enabled
output-gigapbts(vsa)	n/c	n/c	n/c	n/c	enabled
output-gigawords	n/c	n/c	n/c	n/c	enabled
pppoe-description(vsa)	n/c	n/c	enabled	enabled	enabled
profile-service-descr(vsa)	n/c	n/c	disabled	disabled	disabled
tunnel-assignment-id	n/c	n/c	n/c	enabled	enabled
tunnel-client-auth-id	n/c	n/c	enabled	enabled	enabled
tunnel-client-endpoint	n/c	n/c	enabled	enabled	enabled
tunnel-interface-id	n/c	n/c	disabled	disabled	disabled
tunnel-medium-type	n/c	n/c	enabled	enabled	enabled
tunnel-preference	n/c	n/c	n/c	enabled	enabled
tunnel-server-attributes	n/c	n/c	disabled	disabled	disabled
tunnel-server-auth-id	n/c	n/c	enabled	enabled	enabled
tunnel-server-endpoint	n/c	n/c	enabled	enabled	enabled
tunnel-type	n/c	n/c	enabled	enabled	enabled

show radius attributes-ignored

- Use to display the RADIUS attributes that are ignored in Access-Accept messages.
- Example

```

host1#show radius attributes-ignored
attribute framed-ip-netmask ignored from RADIUS server
attribute atm-category (vsa) ignored from RADIUS server
attribute atm-mbs (vsa) accepted from RADIUS server
attribute atm-pcr (vsa) ignored from RADIUS server
attribute atm-scr (vsa) accepted from RADIUS server
attribute egress-policy-name (vsa) accepted from RADIUS server
attribute ingress-policy-name (vsa) accepted from RADIUS server
attribute virtual-router accepted from RADIUS server

```

Chapter 3

Configuring RADIUS Dynamic-Request Server

This chapter describes the RADIUS dynamic-request server feature on E-series routers. The following topics describe this feature:

- [Overview](#) on page 175
- [Platform Considerations](#) on page 177
- [References](#) on page 177
- [How RADIUS Dynamic-Request Server Works](#) on page 177
- [RADIUS-Initiated Disconnect](#) on page 177
- [Message Exchange](#) on page 178
- [Configuring RADIUS-Initiated Disconnect](#) on page 179
- [RADIUS-Initiated Change of Authorization](#) on page 179
- [Configuring RADIUS-Initiated Change of Authorization](#) on page 181
- [RADIUS Dynamic-Request Server Commands](#) on page 182
- [Monitoring RADIUS Dynamic-Request Servers](#) on page 183

Overview

The E-series router's RADIUS dynamic-request server feature provides an efficient way for you to use RADIUS servers to centrally manage user sessions. The RADIUS dynamic-request server enables the router to receive the following types of messages from RADIUS servers:

- Disconnect messages—Immediately terminate specific user sessions.
- Change-of-Authorization (CoA) messages—Dynamically modify session authorization attributes, such as data filters.

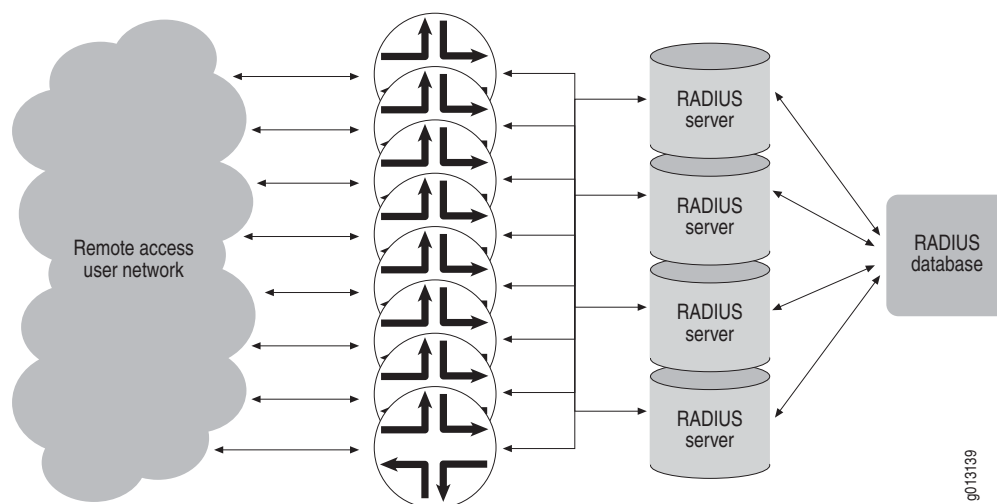


NOTE: The RADIUS dynamic-request server's support for CoA messages is used by the Service Manager and by the E-series router's packet mirroring feature. For information about using the Service Manager, see [Chapter 11, Configuring Service Manager](#) in this guide. For specific information about using the dynamic-request server with packet mirroring, see [JUNOS Policy Management Configuration Guide, Chapter 6, Packet Mirroring](#).

For example, you might use the RADIUS dynamic-request server to terminate specific user sessions. Without the RADIUS dynamic-request server, the only way to disconnect a RADIUS user is from the E-series router. This disconnect method is cumbersome when a network has many systems. The RADIUS dynamic-request server allows RADIUS servers to initiate user-related operations, such as a termination operation, by sending unsolicited request messages to an E-series router.

[Figure 5](#) shows a network that would benefit from the RADIUS dynamic-request server functionality. In [Figure 5](#), instead of disconnecting users on each E-series router, the RADIUS servers can initiate the disconnection. Although the network has multiple RADIUS servers, the servers share a common database that contains authorization and accounting information. Having a common database allows any server to view who is currently valid and connected, and allows service providers to manage the disconnection of users.

Figure 5: Sample Remote Access Network Using RADIUS



Platform Considerations

RADIUS dynamic-request server is supported on all E-series routers. For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

References

For more information about the RADIUS dynamic-request server feature, see the following references:

- [RFC 2865—Remote Authentication Dial In User Service \(RADIUS\) \(June 2000\)](#)
- [RFC 2866—RADIUS Accounting \(June 2000\)](#)
- [RFC 3576—Dynamic Authorization Extensions to Remote Authentication Dial In User Service \(RADIUS\) \(July 2003\)](#)

How RADIUS Dynamic-Request Server Works

In a typical client-server RADIUS environment, the E-series router functions as the client and the RADIUS server functions as the server. However, when using the RADIUS dynamic-request server feature, the roles are reversed. For example, during a RADIUS-initiated disconnect operation, the E-series router's RADIUS dynamic-request server functions as the server, and the RADIUS server functions as the disconnect client.

RADIUS-Initiated Disconnect

This section describes the RADIUS dynamic-request server's RADIUS-initiated disconnect feature.

Disconnect Messages

To centrally control the disconnection of remote access users, the RADIUS dynamic-request server on the router must receive and process unsolicited messages from RADIUS servers.

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

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

Message Exchange

The RADIUS server and the router's RADIUS dynamic-request server exchange messages using User Datagram Protocol (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 AAA successfully disconnects the user, the response is a RADIUS-formatted packet with a Disconnect-ACK message.
- If AAA 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.

Supported Error-Cause Codes (RADIUS Attribute 101)

When a disconnect request fails, the RADIUS dynamic-request server includes an error-cause attribute (RADIUS attribute 101) in the 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 Disconnect-NAK without an error-cause attribute. [Table 17](#) lists the supported error-cause codes.

Table 17: 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 (for example, the packet mirroring Mirror Identifier value) are not formatted properly.
503	Session context not found	The session context identified in the request does not exist on the NAS.
504	Session context not removable	The subscriber identified by attributes in the disconnect request is owned by a component that does not support RADIUS-initiated disconnect (for example, L2TP LAC subscribers cannot be disconnected).
506	Resources unavailable	A request could not be honored due to lack of available NAS resources (such as memory).

Qualifications for Disconnect

For the server to disconnect a user, the Disconnect-Request message must contain an attribute with a session ID. The Disconnect-Request message can contain an Acct-Session-Id (44) attribute or a Multi-Session-Id (50) attribute for the session ID or both. If both the Acct-Session-Id and 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 session ID are used to perform the disconnection. Authentication, authorization, and accounting (AAA) services handle the actual request.

Security/Authentication

The RADIUS server (the disconnect client) must calculate the authenticator as specified for an Accounting-Request message in RFC 2866. The router's RADIUS dynamic-request server verifies the request using authenticator calculation as specified for an Accounting-Request message in RFC 2866. A key (secret), as specified in RFC 2865, must be configured and used in the calculation of the authenticator. The response authenticator is calculated as specified for an Accounting-Response message in RFC 2866.

Configuring RADIUS-Initiated Disconnect

To configure RADIUS-initiated disconnect feature, perform the following steps to set up the RADIUS dynamic-request server that will perform the disconnect operation:

1. Configure the RADIUS dynamic-request server, and enter RADIUS Configuration mode.

```
host1(config)#radius dynamic-request server 10.10.5.10
host1(config-radius)#
```

2. Enable the RADIUS-initiated disconnect capability on the RADIUS dynamic-request server.

```
host1(config-radius)#subscriber disconnect
```

3. Define the secret used in the RADIUS Authenticator field during exchanges between the RADIUS dynamic-request server and the RADIUS server.

```
host1(config-radius)#key Secret3Clientkey
```

4. (Optional) Specify the UDP port on which the RADIUS dynamic-request server listens for messages from the RADIUS server. The default is 1700.

```
host1(config-radius)#udp-port 1770
```

RADIUS-Initiated Change of Authorization

This section describes the RADIUS dynamic-request server's support for CoA messages. CoA messages are used by the E-series router's RADIUS-initiated packet mirroring feature, which is described in [JUNOS Policy Management Configuration Guide, Chapter 6, Packet Mirroring](#), and by Service Manager, which is described in [Chapter 11, Configuring Service Manager](#) of this guide.

Change-of-Authorization Messages

The RADIUS dynamic-request server receives and processes the unsolicited CoA messages from RADIUS servers. The RADIUS-initiated CoA feature uses the following codes in its RADIUS request and response messages:

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

Message Exchange

The RADIUS server and the router's RADIUS dynamic-request server 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 AAA 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 is unsuccessful, the request is malformed, or attributes are missing, the response is a RADIUS-formatted packet with a CoA-NAK message.

Supported Error-Cause Codes (RADIUS Attribute 101)

When AAA is unsuccessful, the RADIUS dynamic-request server includes an error-cause attribute (RADIUS attribute 101) in the CoA-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 CoA-NAK without an error-cause attribute. [Table 18](#) lists the supported error-cause codes.

Table 18: 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 (for example, the packet mirroring Mirror Identifier value) are not formatted properly.
503	Session context not found	The session context identified in the request does not exist on the NAS.
504	Session context not removable	The subscriber identified by attributes in the disconnect request is owned by a component that does not support RADIUS-initiated disconnect (for example, L2TP LAC subscribers cannot be disconnected).
506	Resources unavailable	A request could not be honored due to lack of available NAS resources (such as memory).

Qualifications for Change of Authorization

To complete the change of authorization for a user, the CoA-Request must contain an Acct-Session-Id (44) attribute. AAA services handle the actual request.

Security/Authentication

For change-of-authorization operations, the RADIUS server calculates the authenticator as specified for an Accounting-Request message in RFC 2866. The RADIUS dynamic-request server verifies the request using authenticator calculation as specified for an Accounting-Request in RFC 2866. A key (secret), as specified in RFC 2865, must be configured and used in the calculation of the authenticator. The response authenticator is calculated as specified for an Accounting-Response message in RFC 2866.

Configuring RADIUS-Initiated Change of Authorization

To configure the RADIUS dynamic-request change of authorization feature, perform the following steps to set up the RADIUS dynamic-request server that will perform the CoA operation:

1. Configure the RADIUS dynamic-request server, and enter RADIUS Configuration mode.

```
host1(config)#radius dynamic-request server 10.10.5.10
```

2. Enable the CoA capability on the RADIUS dynamic-request server.

```
host1(config-radius)#authorization change
```

3. Define the key (secret) used in the RADIUS Authenticator field during exchanges between the RADIUS dynamic-request server and the RADIUS server.

```
host1(config-radius)#key Secret21Clientkey
```

4. (Optional) Specify the UDP port on which the router listens for messages from the RADIUS server. The default is 1700.

```
host1(config-radius)#udp-port 1770
```

RADIUS Dynamic-Request Server Commands

This section describes commands used to configure RADIUS dynamic-request servers.

authorization change

- Use to enable the RADIUS dynamic-request server to receive CoA messages, such as packet mirroring attributes and Service Manager attributes, from the RADIUS server.
- Example

```
host1(config)#radius dynamic-request server 192.168.5.3
host1(config-radius)#authorization change
```
- Use the **no** version to disable receipt of the messages; any currently configured operations will continue.

key

- Use to define the key (secret) that is used to calculate the RADIUS Authenticator field during exchanges between the RADIUS dynamic-request server and the RADIUS server.
- If no key is specified, the router drops all requests from the RADIUS server.
- Example

```
host1(config-radius)#key Secret3Clientkey
```
- Use the **no** version to set the default, no Authenticator.

radius disconnect client

- Use to configure a RADIUS disconnect client and enter RADIUS Configuration mode. Include the IP address of the RADIUS server that is acting as the disconnect client.
- Example

```
host1(config)#radius disconnect client 10.10.5.10
host1(config-radius)#
```
- Use the **no** version to remove the RADIUS disconnect client.



NOTE: The function of this command has been replaced by a combination of the RADIUS dynamic-request server feature and the **subscriber disconnect** command. This command might be removed completely in a future release.

radius dynamic-request server

- Use to configure a RADIUS dynamic-request server and enter RADIUS Configuration mode. Specify the IP address of the RADIUS server that exchanges messages with the RADIUS dynamic-request server.
- Example

```
host1(config)#radius dynamic-request server 10.10.5.10
host1(config-radius)#
```
- Use the **no** version to unconfigure the RADIUS dynamic-request server.

subscriber disconnect

- Use to enable the RADIUS dynamic-request server to receive RADIUS disconnect messages from a RADIUS server.
- Example

```
host1(config-radius)#subscriber disconnect
```
- Use the **no** version to disable processing of disconnect packets.



NOTE: This command and the RADIUS dynamic-request server feature replace the **radius disconnect client** command, which may be removed completely in a future release. The RADIUS Disconnect Configuration mode is also deprecated.

udp-port

- Use to specify the UDP port on which the RADIUS dynamic-request server listens to receive messages from the RADIUS server.
- Example

```
host1(config-radius)#udp-port 1770
```
- Use the **no** version to return to the default, port 1700.

Monitoring RADIUS Dynamic-Request Servers

This section describes commands used to display configuration and statistics related to RADIUS dynamic-request servers.

baseline radius dynamic-request

- Use to set a statistics baseline for packet mirroring-related RADIUS statistics.
- Use the **delta** keyword with the **show radius dynamic-request statistics** command to show baselined statistics.
- Example

```
host1#baseline radius dynamic-request
```
- There is no **no** version.

show radius servers**show radius statistics**

- Use with the **dynamic-request** keyword to display RADIUS dynamic-request server configuration information and statistics.
- Field descriptions
 - IP address—IP address of the RADIUS server
 - Udp Port—Port on which the router listens for RADIUS server
 - Disconnect—Status of RADIUS-initiated disconnect feature
 - Change of Authorization—Status of change of authorization feature
 - Secret—Secret used to connect to RADIUS server
 - Disconnect or CoA Requests—RADIUS-initiated disconnect or CoA requests received
 - Disconnect or CoA Accepts—RADIUS-initiated disconnect or CoA requests accepted
 - Disconnect or CoA Rejects—RADIUS-initiated disconnect or CoA requests rejected
 - Disconnect or CoA No Session ID—RADIUS-initiated disconnect or CoA messages rejected because the request did not include a session ID attribute
 - Disconnect or CoA Bad Authenticators—RADIUS-initiated disconnect or CoA messages rejected because the calculated authenticator in the authenticator field of the request did not match
 - Disconnect or CoA Packets Dropped—RADIUS-initiated disconnect or CoA packets dropped because of queue overflow
 - No Secret—Messages rejected because a secret was not present in the authenticator field
 - Unknown Requests—Packets received with an invalid RADIUS code for RADIUS disconnect or change of authorization
 - Invalid Addresses Received—Number of invalid addresses received

■ Example 1

```
host1#show radius dynamic-request servers
```

RADIUS Request Configuration				
IP Address	Udp Port	Disconnect	Change Of Authorization	Secret
192.168.2.3	1700	disabled	disabled	<NULL>
10.10.120.104	1700	disabled	disabled	mysecret

■ Example 2

host1#show radius dynamic-request statistics

```

      RADIUS Request Statistics
      -----
      Statistic                10.10.3.4
      -----
UDP Port                      1700
Disconnect Requests          0
Disconnect Accepts           0
Disconnect Rejects           0
Disconnect No Session ID     0
Disconnect Bad Authenticators 0
Disconnect Packets Dropped   0
CoA Requests                 0
CoA Accepts                  0
CoA Rejects                  0
CoA No Session ID            0
CoA Bad Authenticators       0
CoA Packets Dropped          0
No Secret                    0
Unknown Request              0

Invalid Addresses Received :0

```


Chapter 4

Configuring RADIUS Relay Server

This chapter describes the E-series router's RADIUS relay server feature. The RADIUS relay server provides authentication, authorization, accounting, and addressing services to wireless subscribers in public areas, such as airports and coffee shops. This chapter has the following sections:

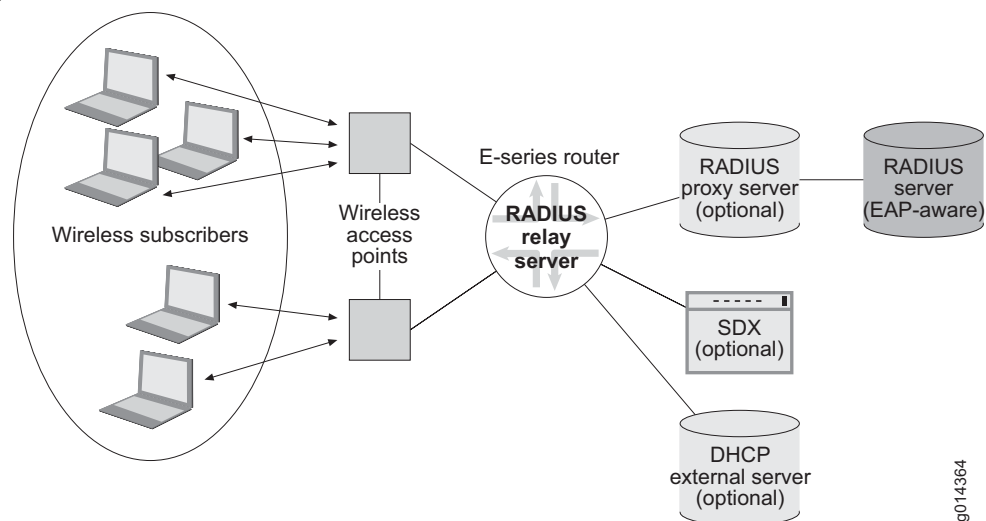
- [Overview](#) on page 187
- [Platform Considerations](#) on page 188
- [References](#) on page 188
- [How RADIUS Relay Server Works](#) on page 189
- [RADIUS Relay Server and the SDX Application](#) on page 190
- [Configuring RADIUS Relay Server Support](#) on page 191
- [Monitoring RADIUS Relay Server](#) on page 193

Overview

The JUNOSe RADIUS relay server provides authentication, authorization, accounting, and addressing services in an 802.1x-based wireless environment.

The IEEE 802.1x standard is an authentication standard for wireless LANs; it enables a wireless subscriber to be authenticated by a central authority. The standard uses the Extensible Authentication Protocol (EAP) for message exchange during the authentication process. The E-series router's RADIUS relay server enhances the 802.1x environment by including authorization, accounting, and addressing support for wireless subscribers.

[Figure 6](#) illustrates a typical 802.1x-based wireless environment. In the figure, wireless subscribers connect to wireless access points (WAPs) for authentication. The WAPs in turn connect to the E-series router's RADIUS relay server. The RADIUS relay server passes the request on to the authentication server, which might be a RADIUS or TACACS+ server. The RADIUS server authenticates the subscriber, who is then granted access. After authentication, the RADIUS relay server obtains an IP address for the subscriber from the Dynamic Host Configuration Protocol (DHCP) local or external server. The RADIUS relay server can also use the RADIUS server or optional Service Deployment System (SDX) program to provide the accounting support.

Figure 6: RADIUS Relay Server

g014364

Platform Considerations

RADIUS relay is supported on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

References

For more information about RADIUS relay server, see the following resources:

- [IEEE 802.1x-2001—Port-Based Network Access Control](#)
- [RFC 2869—RADIUS Extensions \(June 2000\)](#)
- [RFC 2284—PPP Extensible Authentication Protocol \(EAP\) \(March 1998\)](#)
- [RFC 3539—Authentication, Authorization and Accounting \(AAA\) Transport Profile \(June 2003\)](#)

How RADIUS Relay Server Works

When a wireless subscriber starts a session, the WAP encapsulates EAP attributes into a RADIUS Access-Request message and sends the request to the E-series router, which the WAP views as the RADIUS server. The encapsulated message uses the RADIUS EAP-Message (79) attribute. The RADIUS relay server does not process any of the EAP attributes in the RADIUS Access-Request message; the encrypted message is simply passed through the router to the actual RADIUS server. The RADIUS server must be EAP aware.

You can also use an optional RADIUS proxy server to provide additional enhancements to the 802.1x-based environment. For example, the RADIUS proxy server enables subscribers to be multiplexed to multiple Internet service providers (ISPs) that are customers of the same carrier. The server performs one of the following actions:

- If the ISP's RADIUS server supports EAP, the RADIUS proxy server extends the EAP session to the RADIUS server.
- If the ISP's RADIUS server does not support EAP, the RADIUS proxy server translates the EAP session into a legacy RADIUS session for the RADIUS server.

Authentication and Addressing

The WAP initiates the authentication and authorization request by sending a standard RADIUS Access-Request to the RADIUS relay server. The Access-Request must include the attributes listed in [Table 19](#). The attributes uniquely identify the wireless subscriber.

Table 19: Required RADIUS Access-Request Attributes

Attribute Name	Description
Called-Station-id [30]	Subscriber's WAP
Calling-Station-id [31]	Subscriber's media access control (MAC) address

When the RADIUS server authenticates the subscriber, the router's RADIUS relay server creates a RADIUS Access-Accept message and sends the message back to the subscriber. The router's DHCP server (either the router's DHCP local server or an external DHCP server) assigns an IP address to the subscriber and creates the subscriber interface.

For information about using the optional SDX application with the RADIUS relay server to assign IP addresses, see [RADIUS Relay Server and the SDX Application](#) on page 190.

The WAP might periodically reauthenticate a subscriber. For example, reauthentication is necessary to renegotiate a new Wired Equivalent Privacy (WEP) key. The RADIUS relay server ignores any new RADIUS attributes that are sent during a renegotiation operation.

Accounting

The RADIUS relay server's clients (the WAPs) send standard accounting request messages to the RADIUS relay server. The accounting server processes the request and sends the results back to the RADIUS relay server, which then creates a RADIUS accounting response message and forwards the information to the client WAP.

For tracking purposes, the forwarding RADIUS relay server adds the Radius-Client-Address vendor-specific attribute (VSA 26-52) to the forwarded accounting request messages. The VSA indicates the RADIUS relay server's IP address.

For information about using the SDX application with the RADIUS relay server to provide accounting, see [RADIUS Relay Server and the SDX Application](#) on page 190.

[Table 20](#) shows the RADIUS attributes that must be included in accounting requests. The attributes uniquely identify subscribers.

Table 20: Required RADIUS Accounting Attributes

For RADIUS Acct-Start and Acct-Stop Messages	Description
Called-Station-id [30]	Subscriber's WAP
Calling-Station-id [31]	Subscriber's MAC address
For RADIUS Acct-On and Acct-Off Messages	
Called-Station-id [30]	Subscriber's WAP

Terminating the Wireless Subscriber's Connection

The RADIUS relay server terminates the wireless subscriber's session when one of the following events occurs. When a subscriber session is terminated, the subscriber's IP address is released back into the available address pool.

- The RADIUS relay server receives a RADIUS accounting stop request.
- No RADIUS accounting messages are received for this subscriber for more than 24 hours.

RADIUS Relay Server and the SDX Application

The SDX software is an advanced subscriber configuration and management service. The RADIUS relay server can optionally use the SDX application to perform addressing and accounting services for the subscriber and WAP.

The RADIUS relay server uses the E-series router's DHCP local server or DHCP external server and SDX client process to communicate with the SDX software.

Using the SDX Application for Addressing

If you integrate the SDX application into the RADIUS relay server configuration, the application can contribute to the address pool selection used to lease an address to the subscriber. The SDX application only contributes to address pool selection when the DHCP local server is used; it is not supported when a DHCP external server is used.

Using the SDX Application for Accounting

If you use the SDX application with the RADIUS relay server feature, two accounting domains might actually be created. The first domain is established by the WAP, when the subscriber is authenticated. The second domain is created for the connection between the E-series router and the SDX application.

If you want to continue to use the SDX application's user session and problem-tracking features, you should *not* configure the SDX application to generate RADIUS accounting records. Also, the following attributes must be configured on the RADIUS server used by the WAP:

- Service-Bundle [26-31]
- Class [25]
- User-Name [1]

Configuring RADIUS Relay Server Support

To configure the RADIUS relay server feature, you enable support for the feature on the E-series router and identify the key (secret) used for the connection between the WAP and the RADIUS relay server. The following example configures a RADIUS relay authentication server. Use similar steps to configure a RADIUS relay accounting server.



NOTE: The E-series router supports one instance of the RADIUS relay server per virtual router. The instance can provide authentication, authorization, and accounting support.

1. Enable RADIUS relay server support on the E-series router, and enter RADIUS Relay Configuration mode.

```
host1(config)#radius relay authentication server
host1(config-radius-relay)#
```

2. Specify the IP address and mask of the network that will use the relay authentication server, and the secret used during exchanges between the relay authentication server and clients (the WAPs).

```
host1(config-radius-relay)#key 192.168.25.9 255.255.255.255 mysecret
```

3. Specify the router's User Datagram Protocol (UDP) port on which the RADIUS relay server listens.

```
host1(config-radius-relay)#udp-port 1812
```

4. (Optional) Verify the configuration.

```
host1(config-radius-relay)#exit
host1(config)#exit
host1#show radius relay servers
```

RADIUS Relay Authentication Server Configuration

IP Address	IP Mask	Secret
10.10.15.0	255.255.255.0	secret
10.10.8.15	255.255.255.255	newsecret
192.168.25.9	255.255.255.255	mysecret
192.168.102.5	255.255.255.255	999Y2K

Udp Port: 1812

RADIUS Relay Accounting Server Configuration

IP Address	IP Mask	Secret
10.10.1.0	255.255.255.0	N08pxq
192.168.102.5	255.255.255.255	12BE\$56

Udp Port: 1813

key

- Use to enter the IP address and mask of the network that will use the RADIUS relay server, and to specify the key (secret) used during exchanges between the RADIUS relay server and client.
- Example

```
host1(config-radius-relay)#key 10.10.15.25 255.255.255.0 Secret3Clientkey
```
- Use the **no** version to delete the secret.

radius relay server

- Use to configure a RADIUS relay authentication or accounting server and enter RADIUS Relay Configuration mode.
- Example

```
host1(config)#radius relay authentication server
host1(config-radius-relay)#
```
- Use the **no** version to unconfigure the RADIUS relay server.

radius relay udp-checksum

- Use to enable or disable UDP checksum for RADIUS relay packets.
- Example

```
host1(config)#radius relay udp-checksum enable
```
- Use the **no** version to restore the default, enable.

udp-port

- Use to specify the router's UDP port on which the RADIUS relay server resides.
- Example
host1(config-radius-relay)#**udp-port 1850**
- Use the **no** version to return to the default, port 1812 for authentication servers or port 1813 for accounting servers.

Monitoring RADIUS Relay Server

This section describes the commands used to display configuration and statistics related to RADIUS relay servers.

baseline radius relay

- Use to set a baseline for RADIUS relay statistics.
- To show baselined statistics, use the **delta** keyword with the **show radius relay** commands.
- Example
host1#**baseline radius relay**
- There is no **no** version.

show radius relay servers

- Use to display RADIUS relay server configuration information.
- Field descriptions
 - IP Address—Address of the RADIUS relay server
 - IP Mask—Mask of the RADIUS relay server
 - Secret—Secret used for exchanges between the RADIUS relay server and client
 - Udp Port—Router's port on which the RADIUS relay server listens
- Example

host1#**show radius relay servers**

RADIUS Relay Authentication Server Configuration

IP Address	IP Mask	Secret
10.10.8.15	255.255.255.255	newsecret
192.168.102.5	255.255.255.255	999Y2K

Udp Port: 1812

RADIUS Relay Accounting Server Configuration

IP Address	IP Mask	Secret
10.10.1.0	255.255.255.0	N08pxq
192.168.102.5	255.255.255.255	12BE\$56

Udp Port: 1813

show radius relay statistics

- Use to display RADIUS relay server statistics.
- Field descriptions
 - Access Requests—Number of access requests received
 - Access Accepts—Number of access accepts received
 - Access Challenges—Number of access challenges received
 - Access Rejects—Number of access rejects received
 - Pending Requests—Number of access requests waiting for a response
 - Duplicate Requests—Number of duplicate requests received while the previous request is pending
 - Malformed Requests—Requests with attributes having an invalid length or unexpected attributes
 - Bad Authenticators—Authenticator in the response is incorrect for the matching request; can occur if the secret for the RADIUS relay server and the WAP does not match
 - Unknown Requests—Packets received from nonconfigured clients
 - Dropped Packets—Packets dropped because of queue overflow
 - Invalid Requests—Number of invalid requests received
 - Accounting Requests—Number of accounting requests received, broken down by type of request
 - Accounting Responses—Number of accounting responses, broken down by type of request
- Example

```
host1#show radius relay statistics delta
```

```
RADIUS Relay Authentication Server Statistics
```

```
-----
Statistic      Total
-----
Access Requests 1000
Access Accepts  1000
Access Challenges 0
Access Rejects  0
Pending Requests 0
Duplicate Requests 0
Malformed Requests 0
Bad Authenticators 0
Unknown Requests 0
Dropped Packets  0
Invalid Requests 0
Statistics baseline set FRI APR 02 2004 19:01:52 UTC
```

RADIUS Relay Accounting Server Statistics

Statistic	Total
Accounting Requests	1000
Start	1000
Stop	0
Interim	0
Accounting Responses	1000
Start	1000
Stop	0
Interim	0
Pending Requests	0
Duplicate Requests	0
Malformed Requests	0
Bad Authenticators	0
Unknown Requests	0
Dropped Packets	0
Invalid Requests	0
Statistics baseline set FRI APR 02 2004 19:01:52 UTC	

show radius relay udp-checksum

- Use to display status of RADIUS relay UDP checksums.
- Example

```
host1(config)#show radius relay udp-checksum
udp-checksums enabled
```


Chapter 5

Configuring TACACS+

This chapter explains how to enable and configure TACACS + in your E-series router. It has the following sections:

- [Overview](#) on page 197
- [Platform Considerations](#) on page 201
- [References](#) on page 202
- [Before You Configure TACACS +](#) on page 202
- [Configuring TACACS + Support](#) on page 202
- [Monitoring TACACS +](#) on page 208

Overview

With the increased use of remote access, the need for managing more network access servers (NAS) has increased. Additionally, the need for control access on a per-user basis has escalated, as has the need for central administration of users and passwords.

Terminal Access Controller Access Control System (TACACS) is a security protocol that provides centralized validation of users who are attempting to gain access to a router or NAS. TACACS +, a more recent version of the original TACACS protocol, provides separate authentication, authorization, and accounting (AAA) services.



NOTE: TACACS + is a completely new protocol and is not compatible with TACACS or XTACACS.

The TACACS + protocol provides detailed accounting information and flexible administrative control over the authentication, authorization, and accounting process. The protocol allows a TACACS + client to request detailed access control and allows the TACACS + process to respond to each component of that request. TACACS + uses Transmission Control Protocol (TCP) for its transport.

TACACS + provides security by encrypting all traffic between the NAS and the process. Encryption relies on a secret key that is known to both the client and the TACACS + process.

Table 21 describes terms that are frequently used in this chapter.

Table 21: TACACS-Related Terms

Term	Description
NAS	Network access server. A device that provides connections to a single user, to a network or subnetwork, and to interconnected networks. In reference to TACACS+, the NAS is the E-series router.
TACACS+ process	A program or software running on a security server that provides AAA services using the TACACS+ protocol. The program processes authentication, authorization, and accounting requests from an NAS. When processing authentication requests, the process might respond to the NAS with a request for additional information, such as a password.
TACACS+ host	The security server on which the TACACS+ process is running. Also referred to as a TACACS+ server.

AAA Overview

TACACS+ allows effective communication of AAA information between NASs and a central server. The separation of the AAA functions is a fundamental feature of the TACACS+ design:

- **Authentication**—Determines who a user is, then determines whether that user should be granted access to the network. The primary purpose is to prevent intruders from entering your networks. Authentication uses a database of users and passwords.
- **Authorization**—Determines what an authenticated user is allowed to do. Authorization gives the network manager the ability to limit network services to different users. Also, the network manager can limit the use of certain commands to various users. Authorization cannot occur without authentication.
- **Accounting**—Tracks what a user did and when it was done. Accounting can be used for an audit trail or for billing for connection time or resources used. Accounting can occur independent of authentication and authorization.

Central management of AAA means that the information is in a single, centralized, secure database, which is much easier to administer than information distributed across numerous devices. Both RADIUS and TACACS+ protocols are client-server systems that allow effective communication of AAA information.

For information about RADIUS, see [Chapter 1, Configuring Remote Access](#) and [Chapter 2, Configuring RADIUS Attributes](#).

Administrative Login Authentication

Fundamentally, TACACS+ provides the same services as RADIUS. Every authentication login attempt on an NAS is verified by a remote TACACS+ process.

TACACS+ authentication uses three packet types. Start packets and Continue packets are always sent by the user. Reply packets are always sent by the TACACS+ process.

TACACS + sets up a TCP connection to the TACACS + host and sends a Start packet. The TACACS + host responds with a Reply packet, which either grants or denies access, reports an error, or challenges the user.

TACACS + might challenge the user to provide username, password, passcode, or other information. Once the requested information is entered, TACACS + sends a Continue packet over the existing connection. The TACACS + host sends a Reply packet. Once the authentication is complete, the connection is closed. Only three login retries are allowed.

To enable login authentication through both TACACS + and RADIUS servers, use the **aaa new-model** command to specify AAA authentication for Telnet sessions.

Privilege Authentication

The privilege authentication process determines whether a user is allowed to use commands at a particular privilege level. This authentication process is handled similarly to login authentication, except that the user is limited to one authentication attempt. An empty reply to the challenge forces an immediate access denial. The **aaa authentication enable default** command allows you to set privilege authentication for users.

Login Authorization

To allow login authorization through the TACACS + server, you can use the following commands: **aaa authorization**, **aaa authorization config-commands**, and **authorization**. For information about using these commands, see [JUNOS System Basics Configuration Guide, Chapter 8, Passwords and Security](#).

Accounting

The TACACS + accounting service enables you to create an audit trail of User Exec sessions and command-line interface (CLI) commands that have been executed within these sessions. For example, you can track user CLI connects and disconnects, when configuration modes have been entered and exited, and which configuration and operational commands have been executed.

You configure TACACS + accounting in the JUNOS software by defining accounting method lists and then associating consoles and lines with the method lists. You define an accounting method list with a service type, name, accounting mode, and method:

- service type—Specifies the type of information being recorded
- name—Uniquely identifies an accounting method list within a service type
- accounting mode—Specifies what type of accounting records will be generated
- method—Specifies the protocol for sending the accounting records to a security server

You can then configure consoles and lines with an accounting method list name for each service type:

- **Method list**—A specified configuration that defines how the NAS performs the AAA accounting service. A service type can be configured with multiple method lists with different names, and a method list name can be used for different service types. Initially, no accounting method list is defined; therefore TACACS+ accounting is disabled.
 - **Default method list**—Configuration used by consoles and lines when no named method list is assigned. You enable TACACS+ accounting by defining default accounting method lists for each service type.
 - **Named method list**—Assigned to a console, specific line, or group of lines; overrides the default method list.
- **Service type**—Specifies the type of information provided by the TACACS+ accounting service:
 - **Exec**—Provides information about User Exec terminal sessions, such as telnet, Local Area Transport (LAT), and rlogin, on the NAS.
 - **Commands < 0-15 >**—Provides information about User Exec mode CLI commands for a specified privilege level that are being executed on the NAS. Each of the sixteen command privilege levels is a separate service type. Accounting records are generated for commands executed by users, CLI scripts, and macros.
- **Accounting mode**—Specifies the type of accounting records that are recorded on the TACACS+ server. Accounting records track user actions and resource usage. You can analyze and use the records for network management, billing, and auditing purposes.
 - **start-stop**—A start accounting record is generated just before a process begins, and a stop accounting record is generated after a process successfully completes. This mode is supported only for the Exec service type.
 - **stop-only**—A stop accounting record is generated after a process successfully completes. This mode is supported only for the Commands service types.

The NAS sends TACACS + accounting packets to the TACACS + host. The accounting packets contain data in the packet header, packet body, and attribute-value pairs (AVPs). [Table 22](#) provides descriptions of the TACACS + accounting data.

Table 22: TACACS+ Accounting Information

Field/Attribute	Location	Description
major_version	Packet header	Major TACACS + version number
minor_version	Packet header	Minor TACACS + version number
type	Packet header	Type of the AAA service: Accounting
flags	Packet body	Bitmapped flags representing the record type: start accounting record or stop accounting record
priv-level	Packet body	Privilege level of the user executing the Exec session or CLI command: 0 - 15
user	Packet body	Name of user running the Exec session or CLI command
port	Packet body	NAS port used by the Exec session or CLI command
rem-addr	Packet body	User's remote location; either an IP address or the caller ID
service	AVP	User's primary service: Shell
cmd	AVP	CLI command that is to be executed: specified for Command-level accounting only
task_id	AVP	Unique sequential identifier used to match start and stop records for a task
elapsed_time	AVP	Elapsed time in seconds for the task execution: specified for Exec-level accounting stop records only
timezone	AVP	Time zone abbreviation used for all timestamps

Platform Considerations

TACACS + is supported on all E-series routers. For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

References

For additional information about the TACACS+ protocol, see the following resources:

- [The TACACS+ Protocol, Version 1.78—draft-grant-tacacs-02.txt \(January 1997 expiration\)](#)
- [RFC 2865—Remote Authentication Dial In User Service \(RADIUS\) \(June 2000\)](#)



NOTE: IETF drafts are valid for only 6 months from the date of issuance. They must be considered as works in progress. Please refer to the IETF Web site at <http://www.ietf.org> for the latest drafts.

Before You Configure TACACS+

Before you begin to configure TACACS+, you must determine the following for the TACACS+ authentication and accounting servers:

- IP addresses
- TCP port numbers
- Secret keys

Configuring TACACS+ Support

To use TACACS+, you must enable AAA. To configure your router to support TACACS+, perform the following tasks. Some of the tasks are optional. Once you configure TACACS+ support on the router, you can configure TACACS+ authentication, authorization, and accounting independent of each other.

1. Specify the names of the IP host or hosts maintaining a TACACS+ server. Optionally, you can specify other parameters, such as port number, timeout interval, and key.

```
host1(config)#tacacs-server host 192.168.1.27 port 10 timeout 3 key
your_secret primary
```

2. (Optional) Set the authentication and encryption key value shared by all TACACS+ servers that do not have a server-specific key set up by the **tacacs-server host** command.

```
host1(config)#tacacs-server key "&#889P^"
```

3. (Optional) Set alternative source address(es) to be used for TACACS + server communications.

```
host1(config)#tacacs-server source-address 192.168.134.63
```

4. (Optional) Set the timeout value for all TACACS + servers that do not have a server-specific timeout set up by the **tacacs-server host** command.

```
host1(config)#tacacs-server timeout 15
```

Configuring Authentication

Once TACACS + support is enabled on the router, you can configure TACACS + authentication. Perform the following steps:

1. Specify AAA new model as the authentication method for the vty lines on your router.

```
host1(config)#aaa new-model
```

2. Specify AAA authentication by defining an authorization methods list.

```
host1(config)#aaa authentication login tac tacacs+ radius enable
```

3. Specify the privilege level by defining a methods list that uses TACACS + for authentication.

```
host1(config)#aaa authentication enable default tacacs+ radius enable
```

4. Configure vty lines.

```
host1(config)#line vty 0 4
```

5. Apply an authentication list to the vty lines you specified on your router.

```
host1(config-line)#login authentication tac
```

Configuring Accounting

Once TACACS + support is enabled on the router, you can configure TACACS + accounting. Perform the following steps:

1. Specify AAA new model as the accounting method for your router.

```
host1(config)#aaa new-model
```

2. Enable TACACS + accounting on the router, and configure accounting method lists. For example:

```
host1(config)#aaa accounting exec default start-stop tacacs+
host1(config)#aaa accounting commands 0 listX stop-only tacacs+
host1(config)#aaa accounting commands 1 listY stop-only tacacs+
host1(config)#aaa accounting commands 13 listY stop-only tacacs+
host1(config)#aaa accounting commands 14 default stop-only tacacs+
host1(config)#aaa accounting commands 15 default stop-only tacacs+
```

3. (Optional) Specify that accounting records are not generated for users without explicit user names.

```
host1(config)#aaa accounting suppress null-username
```

4. Apply accounting method lists to a console or lines. For example:

```
host1(config)#line console 0
host1(config-line)#accounting commands 0 listX
host1(config-line)#accounting commands 1 listX
host1(config-line)#accounting commands 13 listY
host1(config-line)#exit
host1(config)#line vty 0 4
host1(config-line)#accounting commands 13 listY
```

Note that Exec accounting and User Exec mode commands accounting for privilege levels 14 and 15 are now enabled for all lines and consoles with the creation of their default method list, as shown in Step 2.

aaa accounting commands

- Use to enable TACACS+ accounting and capture accounting information for a specific JUNOS privilege level on the router and to create accounting method lists.
- Specify the JUNOS privilege level (0 through 15) for which to capture accounting information.
- Specify **default** to configure the default method list, or configure a named method list. The default method list is used by lines and consoles unless a named method list is configured for them.
- Specify **stop-only** to send a stop accounting notice at the end of a process and **tacacs+** as the accounting protocol.
- Example

```
host1(config)#aaa accounting commands 12 listX stop-only tacacs+
```
- Use the **no** version to delete the accounting method list.

aaa accounting exec

- Use to enable TACACS+ accounting and capture accounting information for User Exec terminal session on the router and to create accounting method lists.
- Specify **default** to configure the default method list, or configure a named method list. The default method list is used by lines and consoles unless a named method list is configured for them.
- Specify **start-stop** to send a start accounting notice at the beginning of a process and a stop accounting notice at the end of a successful process. Specify **tacacs+** as the accounting protocol.
- Example

```
host1(config)#aaa accounting exec default start-stop tacacs+
```
- Use the **no** version to delete the accounting method list.

aaa accounting suppress null-username

- Use to prevent JUNOS software from generating accounting records for users who do not have explicit usernames.
- Example
host1(config)#**aaa accounting suppress null-username**
- Use the **no** version to generate accounting records for users with null usernames.

aaa authentication enable default

- Use to allow privilege determination to be authenticated through the TACACS + server. This command specifies a list of authentication methods that are used to determine whether a user is granted access to the privilege command level.
- The authentication methods that you can use in a list include these options: **radius**, **line**, **tacacs +**, **none**, and **enable**.
- To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.
- Requests sent to a TACACS + server include the username that is entered for login authentication.
- If a default authentication routine is not set for a function, the default is **none**, and no authentication is performed.
- If the authentication method list is empty, the local **enable** password is used.
- Example
host1(config)#**aaa authentication enable default tacacs+ radius**
- Use the **no** version to empty the list.

aaa authentication login

- Use to set AAA authentication at login. This command creates a list that specifies the methods of authentication.
- Once you specify **aaa new-model** as the authentication method for vty lines, an authentication list called “default” is automatically assigned to the vty lines. To allow users to access the vty lines, you must create an authentication list and either:
 - Name the list “default.”
 - Assign a different name to the authentication list, and assign the new list to the vty line using the **login authentication** command.
- The authentication methods that you can use in a list include these options: **radius**, **line**, **tacacs +**, **none**, and **enable**.
- The router traverses the list of authentication methods to determine whether a user is allowed to start a Telnet session. If a specific method is available but the user information is not valid (such as an incorrect password), the router does not continue to traverse the list and denies the user a session.

- If a specific method is unavailable, the router continues to traverse the list. For example, if **tacacs+** is the first authentication type element on the list and the TACACS+ server is unreachable, the router attempts to authenticate with the next authentication type on the list, such as **radius**.
- The router assumes an implicit denial of service if it reaches the end of the authentication list without finding an available method.
- Example

```
host1(config)#aaa authentication login my_auth_list tacacs+ radius line none
```
- Use the **no** version to remove the authentication list from your configuration.

aaa new-model

- Use to specify AAA new model as the authentication method for the vty lines on your router.
- If you specify AAA new model and you do not create an authentication list, users will not be able to access the router through a vty line.
- Example

```
host1(config)#aaa new-model
```
- Use the **no** version to restore simple authentication (login and password).

accounting

- Use to specify accounting method lists used on a console or vty line. Consoles and lines are initially configured with the default method list for all accounting service types (for example, Exec, Commands).
- Specify **exec** to capture accounting information for User Exec terminal sessions or **commands** to capture accounting information for User Exec mode commands at the indicated JUNOS privilege level (0 through 15).
- Specify the name of the method list to be applied to the line or console.
- To disable accounting for a line or console, specify a nonexistent accounting method list name (for example, noAccounting).
- Example

```
host1(config)#accounting commands 12 listY
```
- Use the **no** version to restore the default method list.

line

- Use to open or configure console or vty lines.
- You can specify a single line or a range of lines. The range is 0 through 29 for vty lines, 0 for the console line.
- Example


```
host1(config)#line vty 6 10
host1(config-line)#
```
- Use the **no** version to remove a line or a range of lines from the configuration. Lines that you remove will no longer be available for use by telnet, FTP, or SSH. When you remove a vty line, the router removes all lines above that line. For example, **no line vty 6** causes the router to remove lines 6 through 19. You cannot remove lines 0 through 4.

login authentication

- Use to apply an authentication list to the vty lines you specified on your router.
- Example


```
host1(config-line)#login authentication my_auth_list
```
- Use the **no** version to specify that the router should use the default authentication list.

tacacs-server host

- Use to add or delete a host to or from the list of TACACS+ servers.
- You can optionally specify a nondefault port number, a host-specific key, a single connection and a timeout interval.
- Use the **primary** keyword to assign the host as the primary host.
- If a timeout value is specified, it overrides the global timeout value set with the **tacacs-server timeout** command for this server only.
- You can configure additional hosts by using this command. The designated primary host is always the first in the search order; the remaining hosts are contacted in the order in which they were created. If the primary host is deleted, or if you modify the primary host without specifying the **primary** keyword, the next host in the search order becomes the primary host. The search order is maintained when the NAS is reloaded.
- Example


```
host1(config)#tacacs-server host 192.168.1.27 port 10 timeout 3 key
your_secret primary
host1(config)#no tacacs-server host 192.168.1.27
```
- Use the **no** version to delete the host from the list of TACACS+ servers.

tacacs-server key

- Use to set or reset the authentication encryption key value shared by all TACACS+ servers that do not have a server-specific key set up by the **tacacs-server host** command.
- This key must match the key configured on the TACACS+ process.
- Leading spaces are ignored; however, spaces at the end of the key are recognized. If you use spaces in the key, do not enclose the key in quotation marks.
- Example
host1(config)#**tacacs-server key &# 889khj**
- Use the **no** version to reset a key value shared by all TACACS+ servers.

tacacs-server source-address

- Use to set or reset an alternative source address to be used for TACACS+ server communications.
- Existing connections are not affected by this command.
- Example
host1(config)#**tacacs-server source-address 192.168.134.63**
- Use the **no** version to remove the address.

tacacs-server timeout

- Use to set the interval in seconds that the server waits for the server host to reply. The specified interval is shared by all TACACS+ servers that do not have a server-specific timeout set up by **tacacs-server host** command.
- The timeout interval is between 1 and 300. The default is 5 seconds.
- Example
host1(config)#**tacacs-server timeout 15**
- Use the **no** version to reset the timeout to the default.

Monitoring TACACS+

You can use commands in this section to monitor the current TACACS+ configurations.

baseline tacacs

- Use to set the baseline for TACACS+ statistics.
- Example
host1#**baseline tacacs**
- There is no **no** version.

show statistics tacacs

- Use to display TACACS + statistics.
- Field descriptions
 - Statistic—IP address of the host
 - Search Order—The order in which requests are sent to hosts until a response is received
 - TCP Port—TCP port of the host
 - Auth Requests—Number of authentication requests sent to the host
 - Auth Replies—Number of authentication replies received from the host
 - Auth Pending—Number of expected but not received authentication replies from the host
 - Auth Timeouts—Number of authentication timeouts for the host
 - Author Requests—Number of authorization requests sent to the host
 - Author Replies—Number of authorization replies received from the host
 - Author Pending—Number of expected but not received authorization replies from the host
 - Author Timeouts—Number of authorization timeouts for the host
 - Acct Requests—Number of accounting requests sent to the host
 - Acct Replies—Number of accounting replies received from the host
 - Acct Pending—Number of expected but not received accounting replies from the host
 - Acct Timeouts—Number of accounting timeouts for the host
- Example

```

host1#show statistics tacacs
      TACACSPLUS Statistics
-----
      Statistic      10.5.0.174      10.5.1.199
-----
Search Order         1                2
TCP Port             3049             4049
Auth Requests        140                0
Auth Replies         85                0
Auth Pending         43                0
Auth Timeouts        12                0
Author Requests      6399             97
Author Replies       6301                0
Author Pending       0                0
Author Timeouts      98                97
Acct Requests        6321             37
Acct Replies         6280                0
Acct Pending         4                0
Acct Timeouts        37                37

```

show tacacs

- Use to display TACACS+ information.
- Use the **statistics** keyword to display overall statistics.
- Use the **delta** keyword to display statistics since they were baselined; deltas are not calculated for the pending statistics.
- Field descriptions
 - Key—Authentication and encryption key
 - Timeout—TACACS+ host response timeout in seconds
 - Source-address—Alternative source IP address configured
 - TACACSPLUS Configuration—Table contains statistics for each host
 - IP Address—IP address of the host
 - TCP Port—TCP port of the host for each IP address
 - Timeout—Timeout interval in seconds for each IP address
 - Primary—This IP address's primary host; options: y = yes, n = no
 - Key—Authentication and encryption key for this IP address
 - Search Order—The order in which requests are sent to hosts until a response is received
- Example

```
host1#show tacacs
```

```
Key = hippo
```

```
Timeout = <NOTSET>, built-in timeout of 5 will be used
```

```
Source-address = <NOTSET>
```

```
TACACS+ Configuration, (*) denotes inherited
```

IP Address	Tcp Port	Timeout	Primary	Key	Search Order
10.5.0.174	3049	5 (*)	y	hippo (*)	1
10.5.1.199	1049	5 (*)	n	hippo (*)	2

Chapter 6

Configuring L2TP

Layer 2 Tunneling Protocol (L2TP) is a client-server protocol that allows Point-to-Point Protocol (PPP) to be tunneled across a network. This chapter includes the following topics that provide information for configuring L2TP on the E-series router.

- [Overview](#) on page 212
- [Platform Considerations](#) on page 216
- [References](#) on page 218
- [Before You Configure the LAC or LNS](#) on page 219
- [Configuring the LAC](#) on page 219
- [Configuring the LNS](#) on page 239
- [Enabling Tunnel Switching](#) on page 246
- [Enabling Tunnel Selection](#) on page 247
- [Creating Persistent Tunnels](#) on page 250
- [Testing Tunnel Configuration](#) on page 250
- [Managing L2TP](#) on page 250
- [Configuring Disconnect Cause Information](#) on page 253
- [Configuring the Receive Window Size](#) on page 255
- [Configuring Peer Resynchronization](#) on page 259
- [Configuring L2TP Tunnel Switch Profiles](#) on page 262
- [Configuring the Transmit Connect Speed Calculation Method](#) on page 270
- [PPP Accounting Statistics](#) on page 279
- [Monitoring L2TP](#) on page 280

Overview

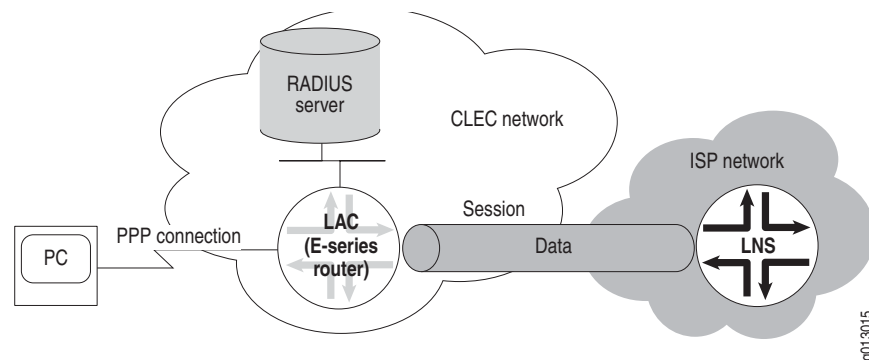
L2TP encapsulates layer 2 packets, such as PPP, for transmission across a network. An L2TP access concentrator (LAC), configured on an access device, such as an E-series router, receives packets from a remote client and forwards them to an L2TP network server (LNS), on a remote network.

You can configure your router to act as an LAC in 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 E-series router creates tunnels dynamically by using authentication, authorization, and accounting (AAA) authentication parameters and transmits L2TP packets to the LNS via IP/User Datagram Protocol (UDP). Traffic travels in an L2TP *session*. A tunnel is an aggregation of one or more sessions. [Figure 7](#) and [Figure 8](#) show typical arrangements.

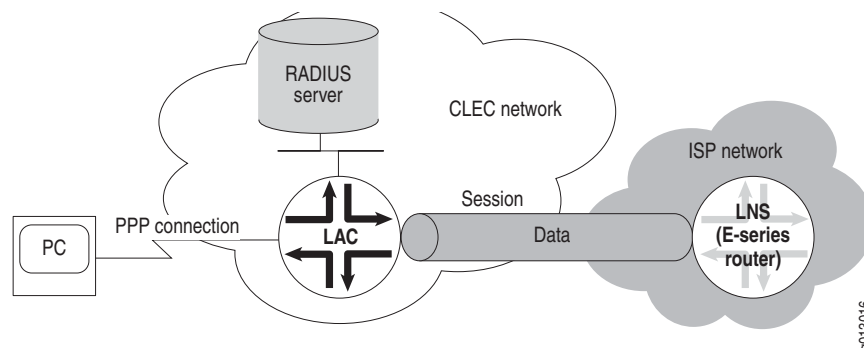
You can configure an E-series router to act as an LAC.

Figure 7: Using the E-series Router as an LAC



You can also configure an E-series router to act as an LNS.

Figure 8: Using the E-series Router as an LNS



NOTE: The E-series router does not support terminating both ends of a tunnel or session in the same router.

Terminology

Table 23 describes the basic terms for L2TP.

Table 23: L2TP Terms

Term	Description
Attribute value pair (AVP)	Combination of a unique attribute—represented by an integer—and a value containing the actual value identified by the attribute.
LAC	L2TP access concentrator (LAC)—a node that acts as one side of an L2TP tunnel endpoint and is a peer to the LNS. An LAC sits between an LNS and a remote system and forwards packets to and from each.
Call	A connection (or attempted connection) between a remote system and an LAC.
LNS	L2TP network server (LNS)—a node that acts as one side of an L2TP tunnel endpoint and is a peer to the LAC. An 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. An 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	LCP (Link Control Protocol) negotiation that is performed by the LAC on behalf of the LNS. Proxy 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. NOTE: 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.

Implementing L2TP

The implementation of L2TP for the E-series router uses four levels:

- System—The router
- Destination—The remote L2TP system
- 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 E-series router 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. For details about negotiating PPP connections, see [JUNOS Link Layer Configuration Guide, Chapter 4, Configuring Point-to-Point Protocol](#).
3. 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.
 - 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

The E-series router sets up an LNS 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. The E-series 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 proxy LCP is not present or not acceptable, the router negotiates LCP with the remote system.

8. The E-series PPP processes the proxy authentication data, if it is present, and passes the data to AAA for verification. (If the data is not present, E-series PPP requests the data from the remote system.)
9. The router passes the authentication results to the remote system.

Packet Fragmentation

The E-series router supports the reassembly of IP-fragmented L2TP packets. (For more information, see [JUNOS IP Services Configuration Guide, Chapter 12, IP Reassembly for Tunnels](#).) However, it is preferable to prevent fragmentation within L2TP tunnels because of the effects of fragmentation and reassembly on performance.

To prevent fragmentation, PPP LCP negotiation of the maximum receive unit (MRU) may be used to determine a proper maximum transmission unit (MTU). However, the normal automatic method of determining the proper MRU to negotiate (by evaluating the MRU of all lower layers in the interface stack) is not adequate for L2TP. The initial LCP negotiation between PPP in the client and the LAC is inadequate because it does not cover the entire extent of the eventual PPP session that travels all the way from the client to the LNS. Furthermore, even if PPP in the LNS chooses to renegotiate the MRU, it has no way to determine the proper MRU, since it does not know the minimum MRU on all of the intervening links between it and the LAC.

To overcome the inadequacy of normal determination of the MRU under such circumstances, you can configure the PPP MRU size by using the **ppp mru** command in Profile Configuration mode, Interface Configuration mode, or Subinterface Configuration mode. Use Profile Configuration mode for dynamic PPP interfaces, and Interface Configuration mode or Subinterface Configuration mode for static PPP interfaces.

When you specify the size, you need to take into account the MRU for all possible links between the LAC and the LNS. You must also take into account the L2TP encapsulation that is added to all packets entering the tunnel.

For example, if the link between the LAC and LNS with the lowest MRU were an Ethernet link, the following calculation applies:

Minimum link MRU	1500
L2TP encapsulating IP header	-20
L2TP encapsulating UDP header	-8
Maximum L2TP header (assumes a maximum of 16 bytes of Offset Pad)	-30
<hr/>	
MRU size to specify	1442

If the smallest intervening link is an Ethernet link, specifying **ppp mru 1442** at either the LAC or LNS guarantees that no fragmentation will occur within the L2TP tunnel.

Platform Considerations

For information about modules that support LNS and LAC on the ERX-7xx models, ERX-14xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, ERX Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support LNS and LAC.

For information about modules that support LNS and LAC on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support LNS and LAC.

Module Requirements

The supported modules for LNS depends on the type of E-series router that you have.

ERX-7xx Models, ERX-14xx Models, and the ERX-310 Router

To use an LNS on ERX-7xx models, ERX-14xx models, and the ERX-310 router, at least one Service line module (SM) or a module that supports the use of shared tunnel-server ports must be installed in the ERX router. For information about installing modules in the ERX router, see the *ERX Hardware Guide*.

SMs provide dedicated tunnel-server ports that are always configured on the module. Unlike other line modules, SMs do not pair with corresponding I/O modules that contain ingress and egress ports. Instead, they receive data from and transmit data to other line modules with access to ingress and egress ports on their own associated I/O modules.

You can also create tunnels on E-series modules that support shared tunnel-server ports. You can configure (provision) a shared tunnel-server port to use a portion of the module's bandwidth to provide tunnel services. For a list of the modules that support shared tunnel-server ports, see the *ERX Module Guide*.

For information about configuring tunnel services on dedicated and shared tunnel-server ports, see [JUNOS Physical Layer Configuration Guide, Chapter 6, Managing Tunnel-Service and IPSec-Service Interfaces](#).

For information about line modules supported by the LAC and LNS and the type of support each module type receives, see *ERX Module Guide, Appendix A, Module Protocol Support*.

E120 Router and E320 Router

To use an LNS on an E120 router or an E320 router, you must install an ES2 4G line module (LM) with an ES2-S1 Service I/O adapter (IOA), or an IOA that supports the use of shared tunnel-server ports. For information about installing modules in these routers, see the *E320 Hardware Guide*.

The ES2 4G LM and ES2-S1 Service IOA combination provides a dedicated tunnel-server port that are always configured on the IOA. Unlike SMs, the ES2 4G LM requires the ES2-S1 Service IOA to condition it to receive and transmit data to other line modules. The ES2-S1 Service IOA also does not have ingress or egress ports.

You can also create tunnels on IOAs that support shared tunnel-server ports. You can configure (provision) a shared tunnel-server port to use a portion of the IOA's bandwidth to provide tunnel services. For a list of the IOAs that support shared tunnel-server ports, see the *E120 and E320 Module Guide*.

For information about IOAs supported by the LAC and LNS and the type of support each module type receives, see *E120 and E320 Module Guide, Appendix A, IOA Protocol Support*.

Sessions and Tunnels Supported

The E120 and E320 routers support 60,000 L2TP sessions, the ERX-1440 router supports 32,000 L2TP sessions, and all other E-series routers support a maximum of 16,000 L2TP sessions. The following guidelines apply:

- On all E-series routers

The SM and the ES2-S1 Service IOA both support the termination of 16,000 LNS sessions per module. Both of these modules also support 8000 ingress policy attachments and 8000 egress policy attachments. Therefore, if you want to apply input or output policies to all of the available LNS sessions, you can only terminate a maximum of 8000 sessions per module.

- On the E120 router, E320 router, and the ERX-1440 router

You can create a systemwide maximum of 60,000 sessions per E120 or E320 router or 32,000 sessions per ERX-1440 router. The maximum session limit is spread in any combination across a maximum of 8000 tunnels. For a router that is operating as an LAC for some tunnels and as an LNS for others, the 8000 tunnels and the router's applicable maximum sessions limits apply to the combined total of LAC and LNS tunnels and sessions.

- On all E-series routers except the ERX-1440 router, E120 router, and the E320 router

You can create a systemwide maximum of 16,000 sessions spread in any combination across a maximum of 8000 tunnels shared between an LAC and an LNS. For a router that is operating as an LAC for some tunnels and as an LNS for others, the 8000 tunnels and 16,000 sessions limits apply to the combined total of LAC and LNS tunnels and sessions.



NOTE: In previous releases, the JUNOS software required that you use the **license l2tp-session** command to configure a license to enable support for the maximum allowable L2TP sessions on ERX-1440 routers, E120 routers, and E320 routers. The **license l2tp-session** command still appears in the CLI, but it has no effect on the actual enforced limit. The reported license limit is 60,000. The **show license l2tp-session** command also still appears in the CLI.

References

For more information about L2TP, see the following resources:

- [RFC 2661—Layer Two Tunneling Protocol “L2TP” \(August 1999\)](#)
- [RFC 3145—L2TP Disconnect Cause Information \(July 2001\)](#)
- [Fail Over extensions for L2TP “failover”—draft-ietf-l2tpext-failover-06.txt \(April 2006 expiration\)](#)

For information about L2TP high availability support, see *JUNOS System Basics Configuration Guide, Chapter 7, Managing High Availability*.

For information about setting up policy-based routing features for L2TP, such as rate limit profiles, classifier control lists, and policy lists, see the *JUNOS Policy Management Configuration Guide*.

For information about creating and attaching QoS profiles to L2TP sessions, see the *JUNOS Quality of Service Configuration Guide*.

For information about how to secure Layer 2 Tunneling Protocol (L2TP) tunnels with IP Security (IPSec) on your E-series router, see *JUNOS IP Services Configuration Guide, Chapter 15, Securing L2TP and IP Tunnels with IPSec*.

Before You Configure the LAC or LNS

Before you begin configuring the router as an LAC or LNS, perform the following steps:

1. Create a virtual router.

```
host1(config)#virtual-router west
```

2. Assign a router ID IP address, such as that for a loopback interface, to the virtual router. This address must be reachable by the L2TP peer.

```
host1:west(config)#ip router-id 10.10.45.3
```



CAUTION: You must explicitly assign a router ID to a virtual router rather than using a dynamically assigned router ID. A fixed ID is required because every time the ID changes, L2TP must disconnect all existing tunnels and sessions that use the old ID. If you use a dynamically assigned router ID, the value can change without warning, leading to failure of all L2TP tunnels and sessions. Also, the router could dynamically assign a router ID that is not reachable by the L2TP peer, causing a complete failure of L2TP. You must set the router ID even if you specified a source address in the domain map or a local address in the host profile.

3. If you are configuring the router as an LAC, configure the router or virtual router for Broadband Remote Access Server (B-RAS).

Configuring the LAC

A single E-series router can function as an LAC for some tunnels and an LNS for others, but the router does not support termination at both ends of the *same* tunnel or session in the *same* router.

The router can initiate L2TP tunnels based either on a locally configured domain map or RADIUS profile information. In either case, the data is selected by domain name.

I2tp checksum

- Use to enable the generation of a UDP data integrity checksum in data packets sent to an L2TP peer.
- The router always uses UDP checksums during transmission and reception of L2TP control packets.
- Example

```
host1(config)#I2tp checksum
```
- Use the **no** version to disable UDP checksum (the default).



NOTE: This command does not affect the way the router checks the UDP data integrity checksum in L2TP data packets that are received from an L2TP peer. The router checks all non-zero received checksums and discards the packet if a data integrity problem is detected.

l2tp destruct-timeout

- Use to specify the maximum time period, in the range 10–3600 seconds (1 hour), for which the router attempts to maintain dynamic destinations, tunnels, and sessions after they have been destroyed.
- This command facilitates debugging and other analysis by saving underlying memory structures after the destination, tunnel, or session is terminated.
- Any specific dynamic destination, tunnel, or session may not be maintained for this entire time period if the resources must be reclaimed early to allow new tunnels to be established.
- If you use the **l2tp destination lockout timeout** command to configure an optional lockout timeout, always configure the destruct timeout to be longer than the lockout timeout. The destruct timeout overrides the lockout timeout—when the destruct timeout expires, all information about the locked out destination is deleted, including the lockout timeout and lockout test settings. See [Managing the L2TP Destination Lockout Process](#) on page 235.
- Example

```
host1(config)#l2tp destruct-timeout 1200
```
- Use the **no** version to set this time to the default, 600 seconds (10 minutes).

l2tp retransmission

- Use to specify the number of retransmission retries, in the range 2–7.
- Use the **established** keyword to apply the retry count only to established tunnels.
- Use the **not-established** keyword to apply the retry count only to tunnels that are not established.
- If you do not include a keyword, the router applies the retry count to all tunnels.
- Example

```
host1(config)#l2tp retransmission 4 established
```
- Use the **no** version to set the retransmission retry count to the default, 5.

Configuring Calling Number AVP Formats

The E-series LAC generates L2TP Calling Number AVP 22 for incoming-call request (ICRQ) packets that the LAC sends to the LNS. By default, the E-series LAC generates the Calling Number AVP 22 in descriptive format.

You can also prevent the E-series LAC from sending the Calling Number AVP in ICRQ packets.



NOTE: You cannot change the L2TP Calling Number AVP on tunnel switched interfaces.

You can set up the router to generate AVP 22 in any of the following formats. Agent-circuit-id is suboption 1 of the tags supplied by the PPPoE intermediate agent from the DSLAM. Agent-remote-id is suboption 2.

- Descriptive format—This format includes the following elements:


```
< interface ID > < delimiter > < UID > < delimiter > < interface description >
< delimiter > < connect info > < delimiter > < PPPoE description >
```
- Descriptive include-agent-circuit-id format—This format includes the following elements:


```
< interface ID > < delimiter > < UID > < delimiter > < interface description >
< delimiter > < connect info > < delimiter > < PPPoE description > < delimiter >
< agent-circuit-id >
```
- Descriptive include-agent-circuit-id include-agent-remote-id format—This format includes the following elements:


```
< interface ID > < delimiter > < UID > < delimiter > < interface description >
< delimiter > < connect info > < delimiter > < PPPoE description > < delimiter >
< agent-circuit-id > < delimiter > < agent-remote-id >
```
- Descriptive include-agent-remote-id format—This format includes the following elements:


```
< interface ID > < delimiter > < UID > < delimiter > < interface description >
< delimiter > < connect info > < delimiter > < PPPoE description > < delimiter >
< agent-remote-id >
```
- Fixed format—This format is similar to the fixed format of RADIUS attribute 31 (Calling-Station-Id). If you set up the router to generate the Calling Number AVP in fixed format, the router formats the AVP as follows (the maximum number of characters for each field is shown in brackets):
 - For ATM: < system name [4] > < slot [2] > < port [1] > < VPI [3] > < VCI [5] >
 - For Ethernet: < system name [4] > < slot [2] > < port [1] > < VLAN [8] >
 - Example

system name = westford, slot = 4, port = 3, and VLAN = 12 produces the following calling number:

```
west0430000000012
```
- Include-agent-circuit-id format—This format includes the following element:


```
< agent-circuit-id >
```
- Include-agent-circuit-id include-agent-remote-id format—This format includes the following elements:


```
< agent-circuit-id > < delimiter > < agent-remote-id >
```

- Include-agent-remote-id format—This format includes the following element:

< agent-remote-id >

Configuration Tasks

To set up the router to generate Calling Number AVP 22 in fixed format:

1. Set the calling number format of the tunnel to **fixed**.

```
host1(config)#aaa tunnel calling-number-format fixed
```

2. Set the format of the RADIUS Calling-Station-Id to **fixed**.

```
host1(config)#radius calling-station-format fixed-format
```

To prevent the E-series LAC from sending the Calling Number AVP in ICRQ packets:

```
host1(config)#l2tp disable calling-number-avp
```

For more information about setting up the router to generate Calling Number AVP 22 in a format that includes either or both of the agent-circuit-id and agent-remote-id suboptions of the tags supplied by the PPPoE intermediate agent, see [Configuring PPPoE Remote Circuit ID Capture](#) in *JUNOS Link Layer Configuration Guide, Chapter 7, Configuring Point-to-Point Protocol over Ethernet*.

Example Scenarios

The following examples show how you can synchronize the contents of RADIUS Calling-Station-Id (Attribute 31) and L2TP Calling-Number (AVP 22).

To send the PPPoE agent-circuit-id in RADIUS Attribute 31 and L2TP AVP 22 and specify that the fixed format is used when the PPPoE agent-circuit-id is unavailable, issue the following commands:

```
host1(config)#radius calling-station-format fixed-format
host1(config)#radius remote-circuit-id-delimiter #
host1(config)#radius override calling-station-id remote-circuit-id
host1(config)#radius remote-circuit-id-format agent-circuit-id
```

```
host1(config)#aaa tunnel calling-number-format include-agent-circuit-id
host1(config)#aaa tunnel calling-number-format-fallback fixed
```

To send the PPPoE agent-circuit-id and agent-remote-id in RADIUS Attribute 31 and L2TP AVP 22 and specify that the fixed format is used when both PPPoE agent-circuit-id and agent-remote-id are unavailable, issue the following commands:

```
host1(config)#radius calling-station-format fixed-format
host1(config)#radius remote-circuit-id-delimiter #
host1(config)#radius override calling-station-id remote-circuit-id
host1(config)#radius remote-circuit-id-format agent-circuit-id agent-remote-id
```

```
host1(config)#aaa tunnel calling-number-format include-agent-circuit-id
include-agent-remote-id
host1(config)#aaa tunnel calling-number-format-fallback fixed
```

aaa tunnel calling-number-format

- Use to configure the format used by the E-series LAC to generate the L2TP Calling Number AVP 22.
- The fixed format is similar to the fixed format of RADIUS attribute 31 (Calling-Station-Id). The LAC uses this format in ICRQ packets that it sends to the LNS.
- Several different descriptive formats include information about the interface and either or both of the suboptions supplied by the PPPoE intermediate agent, agent-circuit-id and agent-remote-id.
- Several simpler formats include only either or both of the PPPoE suboptions, agent-circuit-id and agent-remote-id.
- Examples

```
host1(config)#aaa tunnel calling-number-format fixed
host1(config)#aaa tunnel calling-number-format descriptive
include-agent-circuit-id include-agent-remote-id
host1(config)#aaa tunnel calling-number-format include-agent-remote-id
```

- Use the **no** version to restore the default format, descriptive.

aaa tunnel calling-number-format-fallback

- Use to configure the fallback format that the E-series LAC uses to generate the L2TP Calling Number AVP 22 in the event that the PPPoE agent ID is null or unavailable.
- The fallback format is used only when the configured calling number format includes either or both of the agent-circuit-id and agent-remote-id suboptions.
- The calling number format determines what element triggers use of the fallback format:

Calling Number Format	Fallback Trigger
agent-circuit-id	agent-circuit-id is empty
agent-circuit-id include-agent-remote-id	Both agent-circuit-id and agent-remote-id are empty.
agent-remote-id	agent-remote-id is empty
descriptive include-agent-circuit-id	agent-circuit-id is empty
descriptive include-agent-circuit-id include-agent-remote-id	Both agent-circuit-id and agent-remote-id are empty.
descriptive include-agent-remote-id	agent-remote-id is empty

- You can specify either descriptive format or fixed format.
 - Example
- ```
host1(config)#aaa tunnel calling-number-format-fallback fixed
```
- Use the **no** version to restore the default format, descriptive.

***l2tp disable calling-number-avp***

- Use to prevent the E-series LAC from sending the Calling Number AVP in ICRO packets.
- Use this command in special situations where you do not want the LAC to send this AVP.
- Example  

```
host1(config)#l2tp disable calling-number-avp
```
- Use the **no** version to return to the default, sending of the Calling Number AVP is enabled.

***Mapping a User Domain Name to an L2TP Tunnel***

The router uses either the local database related to the domain name or a RADIUS server to determine whether to terminate or tunnel PPP connections.

For information about setting up RADIUS to provide this mapping, see [Chapter 1, Configuring Remote Access](#).

For a given domain map, you can choose one of two methods to map the domain to an L2TP tunnel locally on the router:

- Configure tunnels for a domain map and then define tunnel attributes from Domain Map Tunnel configuration mode.
- Configure a tunnel group and then define the attributes for its tunnels from Tunnel Group Tunnel Configuration mode. Use this method only when no tunnels are currently defined for the domain map from Domain Map Tunnel configuration mode. By default, tunnel groups are not assigned to the domain map.

After configuring a tunnel group and the attributes for its tunnels, you can assign the tunnel group to the domain map from Domain Map mode. The tunnel group reference in the domain map is used instead of tunnel definitions configured from Domain Map Tunnel configuration mode.

The RADIUS server can reference tunnel groups through the RADIUS Tunnel Group [26-64] attribute. The advantages of RADIUS support for tunnel groups are:

- The RADIUS server can maintain a single tunnel group attribute associated with each user instead of sets of tunnel attributes for each user.
- The RADIUS server can authenticate users before attempting to establish tunnels.



### Mapping from Domain Map Tunnel Mode

To map a domain to an L2TP tunnel locally on the router from Domain Map Tunnel mode, perform the following steps:

1. Specify a domain name.

```
host1(config)#aaa domain-map westford.com
host1(config-domain-map)#
```

2. Specify a virtual router; in this case, the *default* router is specified.

```
host1(config-domain-map)#router-name default
```

3. Specify a tunnel to configure.

```
host1(config-domain-map)#tunnel 3
```

4. Specify the LNS endpoint address of a tunnel.

```
host1(config-domain-map-tunnel)#address 192.0.2.13
```

5. Specify a preference for the tunnel.

```
host1(config-domain-map-tunnel)#preference 5
```

6. (Optional) Specify an authentication password.

```
host1(config-domain-map-tunnel)#password temporary
```



**NOTE:** If you specify a password for the LAC, the router requires that the peer (the LNS) authenticate itself to the router. In this case, if the peer fails to authenticate itself, the tunnel terminates.

---

7. (Optional) Specify a hostname for the LAC end of the tunnel.

```
host1(config-domain-map-tunnel)#client-name host4
```

8. (Optional) Specify a server name for the LNS.

```
host1(config-domain-map-tunnel)#server-name boston
```

9. (Optional) Specify a source IP address for the LAC tunnel endpoint.

```
host1(config-domain-map-tunnel)#source-address 192.0.3.3
```

10. Specify a tunnel identification. (The router groups L2TP sessions with the same tunnel identification into the same tunnel.)

```
host1(config-domain-map-tunnel)#identification acton
```

11. Specify a medium type. (L2TP supports only IP version 4 [IPv4].)

```
host1(config-domain-map-tunnel)#medium ipv4
```

12. (Optional) Specify a default tunnel client name.

```
host1(config-domain-map-tunnel)#exit
host1(config-domain-map)#exit
host1(config)#aaa tunnel client-name boxford
```

13. (Optional) Specify a default tunnel password.

```
host1(config)#aaa tunnel password 3&92k%b#q4
host1(config)#exit
```

14. (Optional) Set the format for the tunnel assignment ID.

```
host1(config)#aaa tunnel assignment-id-format assignmentID
```



**NOTE:** If you do not set the tunnel assignment ID, the software sets it to default.

15. (Optional) Specify whether or not to use the tunnel peer's Nas-Port [5] and Nas-Port-Type [61] attributes.

```
host1(config)#aaa tunnel ignore nas-port enable
host1(config)#aaa tunnel ignore nas-port-type disable
```

16. (Optional) Set up the router to ignore sequence numbers in data packets received on L2TP tunnels.

```
host1(config)#l2tp ignore-receive-data-sequencing
```

17. (Optional) Disable local tunnel authentication challenge generation.

```
host1(config)#l2tp disable challenge
```

18. Verify the L2TP tunnel configuration.

```
host1(config)#show aaa domain-map
```

```
Domain: westford.com; router-name: default; ipv6-router-name: default
```

| Tunnel<br>Tag | Tunnel<br>Peer           | Tunnel<br>Source     | Tunnel<br>Type            | Tunnel<br>Medium | Tunnel<br>Password          | Tunnel<br>Id | Tunnel<br>Client<br>Name |
|---------------|--------------------------|----------------------|---------------------------|------------------|-----------------------------|--------------|--------------------------|
| 3             | 192.168.2.13             | 192.168.3.3          | l2tp                      | ipv4             | temporary                   | acton        | host4                    |
| Tunnel<br>Tag | Tunnel<br>Server<br>Name | Tunnel<br>Preference | Tunnel<br>Max<br>Sessions | Tunnel<br>RWS    | Tunnel<br>Virtual<br>Router |              |                          |
| 3             | boston                   | 5                    | 0                         | system chooses   | vr2                         |              |                          |

```
host1#show aaa tunnel-parameters
Tunnel password is 3&92k%b#q4
Tunnel client-name is <NULL>
Tunnel nas-port-method is none
Tunnel nas-port ignore disabled
Tunnel nas-port-type ignore disabled
Tunnel assignmentId format is assignmentId
Tunnel calling number format is descriptive
```

### Mapping from Tunnel Group Tunnel Mode

To map a domain to an L2TP tunnel locally on the router from Tunnel Group Tunnel Configuration mode, perform the following steps:

1. Specify a domain name.

```
host1(config)#aaa tunnel-group westford
host1(config-tunnel-group)#
```

2. Specify a tunnel to configure.

```
host1(config-tunnel-group)#tunnel 3
host1(config-tunnel-group-tunnel)#
```

3. Specify a virtual router; in this case, the *default* router is specified.

```
host1(config-tunnel-group-tunnel)#router-name default
```

4. Specify the LNS endpoint address of a tunnel.

```
host1(config-tunnel-group-tunnel)#address 192.0.2.13
```

5. Specify a preference for the tunnel.

```
host1(config-tunnel-group-tunnel)#preference 5
```

6. (Optional) Specify an authentication password.

```
host1(config-tunnel-group-tunnel)#password temporary
```



**NOTE:** If you specify a password for the LAC, the router requires that the peer (the LNS) authenticate itself to the router. In this case, if the peer fails to authenticate itself, the tunnel terminates.

---

7. (Optional) Specify a hostname for the LAC end of the tunnel.

```
host1(config-tunnel-group-tunnel)#client-name host4
```

8. (Optional) Specify a server name for the LNS.

```
host1(config-tunnel-group-tunnel)#server-name boston
```

9. (Optional) Specify a source IP address for the LAC tunnel endpoint.

```
host1(config-tunnel-group-tunnel)#source-address 192.0.3.3
```

10. Specify a tunnel identification. (The router groups L2TP sessions with the same tunnel identification into the same tunnel.)

```
host1(config-tunnel-group-tunnel)#identification acton
```

11. Specify a medium type. (L2TP supports only IP version 4 [IPv4].)

```
host1(config-tunnel-group-tunnel)#medium ipv4
```

12. Verify the L2TP tunnel configuration.

```
host1(config)#show aaa domain-map
```

```
Domain: westford.com; router-name: default; ipv6-router-name: default
```

| Tunnel<br>Tag | Tunnel<br>Peer | Tunnel<br>Source | Tunnel<br>Type | Tunnel<br>Medium | Tunnel<br>Password | Tunnel<br>Id | Tunnel<br>Client<br>Name |
|---------------|----------------|------------------|----------------|------------------|--------------------|--------------|--------------------------|
| 3             | 192.168.2.13   | 192.168.3.3      | l2tp           | ipv4             | temporary          | acton        | host4                    |

| Tunnel<br>Tag | Tunnel<br>Server<br>Name | Tunnel<br>Preference | Tunnel<br>Max<br>Sessions | Tunnel<br>RWS  | Tunnel<br>Virtual<br>Router |
|---------------|--------------------------|----------------------|---------------------------|----------------|-----------------------------|
| 3             | boston                   | 5                    | 0                         | system chooses | vr2                         |

```
host1#show aaa tunnel-parameters
```

```
Tunnel password is 3&92k%b#q4
Tunnel client-name is <NULL>
Tunnel nas-port-method is none
Tunnel nas-port ignore disabled
Tunnel nas-port-type ignore disabled
tunnel assignmentId format is assignmentId
aaa tunnel calling number format is descriptive
```

### **aaa domain-map**

- Use to map a user domain name to a virtual router and enter Domain Map Configuration mode.
- Example
 

```
host1(config)#aaa domain-map westford.com
host1(config-domain-map)#
```
- Use the **no** version to remove the domain map.

### **aaa tunnel assignment-id-format**

- Use to determine the value of the tunnel assignment ID that is passed to PPP/L2TP.
- The tunnel assignment ID format can be either only assignmentID or clientAuthId + serverAuthId + assignmentId.
- If you do not set a tunnel assignment ID, the software sets it to default. This parameter is only used by the L2TP LAC device, and the tunnel assignment ID is generated only by the L2TP LAC device.
- Example
 

```
host1(config)#aaa tunnel assignment-id-format assignmentID
```
- Use the **no** version to return the tunnel assignment ID to the default, assignmentID.

**aaa tunnel client-name**

- Use to specify a default tunnel client name. If the tunnel client name is not included in the tunnel attributes that are returned from the domain map or authentication server, the router uses the default name.
- Example  
host1(config)#**aaa tunnel client-name boxford**
- Use the **no** version to delete the client name.

**aaa tunnel-group**

- Use to specify an AAA tunnel group and change the mode to Tunnel Group Tunnel Configuration mode. From Tunnel Group Tunnel Configuration mode, you can add up to 31 tunnel definitions.
- Example  
host1(config)#**aaa tunnel-group westford**
- Use the **no** version to delete the AAA group tunnel configuration from the router.

**aaa tunnel ignore**

- Use to specify whether or not to use the tunnel peer's NAS-Port [5] and NAS-Port-Type [61]. When enabled, the attribute is supplied by the tunnel peer. When disabled, the attribute is not supplied.
- Example  
host1(config)#**aaa tunnel ignore nas-port-type disable**
- Use the **no** version to restore the default, enable.

**aaa tunnel nas-port-method**

- Use to configure the tunnel's default NAS port type to provide limited support for a Cisco proprietary vendor-specific method when configuring the LAC to LNS NAS port identification transfer mechanism.



**NOTE:** We recommend you not use this feature; we cannot guarantee continued compatibility.

---

- Example  
host1(config)#**aaa tunnel nas-port-method cisco-avp**
- Use the **no** version to disable the command.

**aaa tunnel password**

- Use to specify a default tunnel password. If the tunnel password is not included in the tunnel attributes that are returned from the domain map or authentication server, the router uses the default password.
- Example  
host1(config)#**aaa tunnel password 3&92k%b#q4**
- Use the **no** version to delete the tunnel password.

**address**

- Use to set the LNS endpoint address of a tunnel.
- Example 1  
host1(config-domain-map-tunnel)#**address 172.31.1.98**
- Example 2  
host1(config-tunnel-group-tunnel)#**address 172.31.1.98**
- Use the **no** version to delete the tunnel address.

**client-name**

- Use to specify the hostname that the LAC sends to the LNS when communicating to the LNS about the tunnel.
- The hostname can be up to 64 characters (no spaces).



**NOTE:** If the LNS does not accept tunnels from unknown hosts, and if no hostname is specified, the LAC uses the router name as the hostname.

---

- Example 1  
host1(config-domain-map-tunnel)#**client-name host4**
- Example 2  
host1(config-tunnel-group-tunnel)#**client-name host4**
- Use the **no** version to remove the hostname.

**identification**

- Use to specify the ID of a tunnel.
- The router groups users with the same tunnel ID in the same tunnel. This occurs only when both the destination (virtual router, IP address) and the ID are the same.
- Example 1  
host1(config-domain-map-tunnel)#**identification acton**
- Example 2  
host1(config-tunnel-group-tunnel)#**identification acton**
- Use the **no** version to remove the assignment ID from the tunnel.

***l2tp disable challenge***

- Use to disable the generation of authentication challenges by the local tunnel, so that the tunnel does not send a challenge during negotiation. However, the tunnel does accept and respond to challenges it receives from the peer.
- Example  
host1(config)#**l2tp disable challenge**
- Use the **no** version to return to the default, which is local challenge generation enabled.

***l2tp ignore-receive-data-sequencing***

- Use to prevent sequence number checking for data packets received on all L2TP tunnels in the router. This command does not affect the insertion of sequence numbers in packets sent from the router.
- We recommend that you set up the router to ignore sequence numbers in received data packets if you are using IP reassembly. Because IP reassembly might reorder L2TP packets, out-of-order packets might be dropped when sequence numbers are being used on L2TP data packets.
- Example  
host1(config)#**l2tp ignore-receive-data-sequencing**
- Use the **no** version to cause the router to check sequence numbers on received L2TP data packets.

***max-sessions***

- Use to set the maximum sessions per tunnel.
- Example 1  
host1(config-domain-map-tunnel)#**max-sessions 3294967295**
- Example 2  
host1(config-tunnel-group-tunnel)#**max-sessions 3294967295**
- Use the **no** version to disable the feature and restore the default value of zero.

***medium ipv4***

- Use to specify the type of medium for a tunnel.
- The only medium type currently supported is IPv4.
- Example 1  
host1(config-domain-map-tunnel)#**medium ipv4**
- Example 2  
host1(config-tunnel-group-tunnel)#**medium ipv4**
- Use the **no** version to set the medium to the default, IPv4.

**password**

- Use to specify the password for a tunnel.
- If you specify a password, your router (the LAC) requires that the peer (the LNS) authenticate itself to the router.
- If the peer fails to authenticate itself, the tunnel terminates.
- Example 1  
host1(config-domain-map-tunnel)#**password temporary**
- Example 2  
host1(config-tunnel-group-tunnel)#**password temporary**
- Use the **no** version to remove the password.

**preference**

- Use to specify the preference level for a tunnel.
- You can specify up to eight levels of preference.
- 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.
- Example 1  
host1(config-domain-map-tunnel)#**preference 5**
- Example 2  
host1(config-tunnel-group-tunnel)#**preference 5**
- Use the **no** version to set the preference number from the tunnel to the default, 0.

**receive-window**

- Use to configure the L2TP receive window size (RWS) for a tunnel on the LAC.
- Example 1  
host1(config-domain-map-tunnel)#**receive-window 4**
- Example 2  
host1(config-tunnel-group-tunnel)#**receive-window 4**
- Use the **no** version to revert to the systemwide RWS setting configured with the L2TP tunnel. Currently, the only supported value is 4.



**router-name**

- Use to map a user domain name to a virtual router.
- Example 1  
host1(config-domain-map)#**router-name vROUT**
- Example 2  
host1(config-tunnel-group-tunnel)#**router-name vROUT**
- Use the **no** version to delete the entry.

**server-name**

- Use to specify the hostname expected from the peer (the LNS) when you set up a tunnel.
- When this name is specified, the peer must identify itself with this name during tunnel startup. Otherwise, the tunnel is terminated.
- The server name can be up to 64 characters (no spaces).
- Example 1  
host1(config-domain-map-tunnel)#**server-name boston**
- Example 2  
host1(config-tunnel-group-tunnel)#**server-name boston**
- Use the **no** version to remove the server name.

**source-address**

- Use to specify the address of the local tunnel endpoint (the LAC). All L2TP packets sent to the peer use this source address.
- By default, the router uses the virtual router's router ID as the source address. You can override this behavior for an L2TP tunnel by specifying a source address. If you do specify a source address, use the address of a stable IP interface (for example, a loopback interface). Make sure that the address is configured in the virtual router for this domain map, and that the address is reachable by the peer.
- Example 1  
host1(config-domain-map-tunnel)#**source-address 172.23.2.74**
- Example 2  
host1(config-tunnel-group-tunnel)#**source-address 172.23.2.74**
- Use the **no** version to remove the source address.

**tunnel**

- Use to specify a tunnel and to enter Domain Map Tunnel Configuration mode.

- Example 1

```
host1(config-domain-map)#tunnel 3
host1(config-domain-map-tunnel)#
```

- Example 2

```
host1(config-tunnel-group-tunnel)#tunnel 3
```

- Use the **no** version to delete the tunnel configuration.

**tunnel group**

- Use to assign a tunnel group to the domain map. You can assign a tunnel group only when no tunnels are currently defined for the domain map from AAA Domain Map Tunnel mode.

- Example

```
host1(config-domain-map)#tunnel group storm
```

- Use the **no** version to delete the tunnel group.

**type**

- Use to specify the L2TP tunnel type (RADIUS attribute 64, Tunnel-Type).

- Example 1

```
host1(config-domain-map-tunnel)#type l2tp
```

- Example 2

```
host1(config-tunnel-group-tunnel)#type l2tp
```

- Use the **no** version to delete the entry. Currently, the only supported value is L2TP.

**Configuring the RX Speed on the LAC**

You can configure the E-series LAC to generate L2TP Receive (RX) Speed AVP 38 when the receive speed equals the transmit (TX) speed. The AVPs can then be used to generate the RADIUS Connect-Info attribute [77] on the LNS. The information in the RADIUS attribute can be used by service providers to identify a customer's service.

To set up the router to generate the Receive Speed (AVP 38), complete the following steps:

1. On the ATM subinterface, configure the advisory receive speed. See [JUNOS Link Layer Configuration Guide, Chapter 1, Configuring ATM](#) for information about configuring the advisory speed.

```
host1(config-subif)#atm atm1483 advisory-rx-speed 2000
```

2. Specify that the RX Speed AVP is always generated. If you do not specify this command, the RX Speed AVP is generated only when the RX speed differs from the TX speed.

```
host1(config)#l2tp rx-connect-speed-when-equal
```

### ***l2tp rx-connect-speed-when-equal***

- Use on the LAC to always generate the RX Speed AVP if the speed is not zero. If you do not specify this command, the RX Speed AVP is generated only when the RX speed differs from the TX speed.
- Example  

```
host1(config)#l2tp rx-connect-speed-when-equal
```
- Use the **no** version to generate the AVP only when the RX speed differs from the TX speed.

## **Managing the L2TP Destination Lockout Process**

When multiple sets of tunneling parameters are available, L2TP uses a selection algorithm to choose the best tunnel for subscriber traffic. As part of this selection process, the JUNOS software's L2TP implementation includes a lockout feature in which the router locks out, or disregards, destinations that are assumed to be unavailable.

By default, when a destination becomes unavailable, L2TP locks out that destination for a lockout timeout of 300 seconds (5 minutes). After the lockout timeout expires, L2TP assumes that the destination is now available and includes the destination when performing the selection algorithm.

### **Modifying the Lockout Procedure**

You can optionally configure your own lockout procedure by specifying the lockout timeout you want to use or enabling a lockout test, or both. When the lockout timeout expires, the destination is either immediately unlocked (if lockout testing is not enabled) or begins the lockout test to verify that the destination is available.

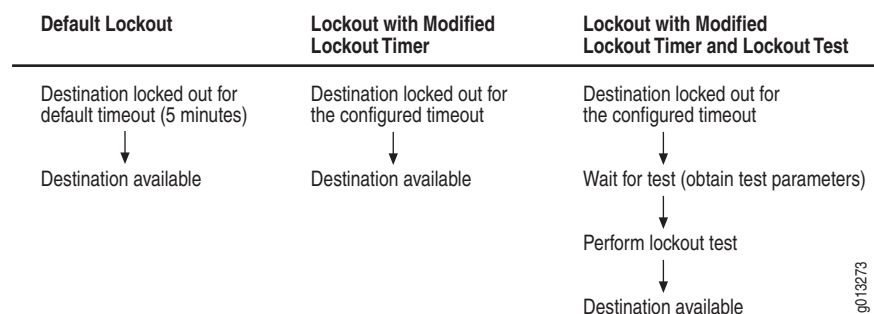
L2TP performs the lockout test by attempting to establish a tunnel to the unavailable destination. For the test, L2TP must first obtain the parameters for a tunnel to the destination. If no such tunnel currently exists, L2TP must wait until it receives a new session request that has tunnel parameters for the locked out destination. The destination remains locked out while L2TP waits for the tunnel parameters and becomes available only after successful completion of the lockout test. Therefore, if lockout testing is enabled, the destination is actually locked out longer than the lockout timer you specify.



**NOTE:** Always configure the lockout timeout to be shorter than the destruct timeout. The destruct timeout (as described for **l2tp destruct-timeout** on page 220) overrides the lockout timeout—when the destruct timeout expires, all information about the locked out destination is deleted, including the time remaining on the destination's lockout timeout and the requirement to run a lockout test prior to returning the destination to service. As a result, the locked out destination might be returned to service prior to expiration of your configured lockout timeout and without completion of the lockout test you specified.

Figure 9 shows how locked-out destinations transition from a locked-out state to available status when using the default lockout configuration, a configuration that includes a modified lockout timer, and a configuration with both a modified timer and the lockout test.

**Figure 9: Lockout States**



You can use the following commands to manage L2TP destination lockout and configure a lockout process that meets the needs of your network environment:

- Use the **l2tp destination lockout-timeout** command to modify the default lockout timeout period.
- Use the **l2tp destination lockout-test** command to configure L2TP to perform a lockout test, which verifies that a currently locked out destination is now available and to include it in the selection algorithm.
- Use the **l2tp unlock destination** command to force L2TP to immediately unlock the specified locked out destination; the destination is then considered to be available by the selection algorithm. L2TP disregards any time remaining in the existing lockout timeout and also disregards the lockout test (if configured).
- Use the **l2tp unlock-test destination** command to force L2TP to immediately begin the lockout testing procedure for the specified destination; any time remaining in the existing lockout timeout is not taken into account.
- Use the **show l2tp** and **show l2tp destination lockout** commands to view information about the L2TP configuration and statistics.

***l2tp destination lockout-test***

- Use to configure L2TP to test locked-out destinations; verifies that a previously locked-out destination is available before the router changes the destination's status.
- Example  

```
host1(config)#l2tp destination lockout-test
```
- Use the **no** version to disable testing of locked out destinations.

***l2tp destination lockout-timeout***

- Use to configure the amount of time (in seconds) between when an L2TP destination is found to be unavailable and when it is eligible for unlocking.
- When the timeout period expires, L2TP either begins the lockout test procedure (if configured to do so) or immediately returns the destination to available state.
- Always configure the lockout timeout to be shorter than the destruct timeout. The destruct timeout (as described for [l2tp destruct-timeout](#) on page 220) overrides the lockout timeout—when the destruct timeout expires, all information about the locked out destination is deleted, including the time remaining on the destination's lockout timeout and the requirement to run a lockout test prior to returning the destination to service.
- The new lockout timeout only affects future locked-out destinations; it does not affect destinations that are currently locked out.
- Specify a lockout timeout in the range 60–3600 seconds (1 minute–1 hour).
- Example  

```
host1(config)#l2tp destination lockout-timeout 500
```
- Use the **no** version to restore the default lockout timeout value, 300 seconds (5 minutes).

***l2tp unlock destination***

- Use to force L2TP to immediately unlock the specified L2TP destination, which is currently locked out and unavailable. L2TP then considers the destination to be available.
- Any remaining lockout time and the lockout test setting (if configured) are not taken into account.
- You must be at privilege level 10 or higher to use this command.
- Example  

```
host1(config)#l2tp unlock destination ip 192.168.1.98
```
- There is no **no** version.

***l2tp unlock-test destination***

- Use to force L2TP to immediately start the lockout test for the specified destination.
- Any remaining lockout time for the destination is ignored.
- If lockout testing is not configured, this command immediately unlocks the destination and L2TP then considers the destination to be available.
- You must be at privilege level 10 or higher to use this command.
- Example  

```
host1(config)#l2tp unlock-test destination ip 192.169.110.8
```
- There is no **no** version.

***Managing Address Changes Received from Remote Endpoints***

A remote endpoint can use the Start-Control-Connection-Reply (SCCRP) packets that it sends to the E-series LAC to change the address that the LAC uses to communicate with the endpoint. By default, the LAC accepts the change and uses the new address to communicate with the endpoint. However, you can configure the LAC to ignore or reject the requested change. Setting up the LAC to ignore address changes in SCCRPs enables the router to construct tunnels with separate receive and transmit addresses and to avoid problems due to a misconfiguration. Three possible configurations are available:

- Default configuration—The E-series LAC accepts the change from the endpoint. The LAC then sends all subsequent packets to, and accepts packets from, the new address.
- Ignore configuration (specified by the **l2tp ignore-transmit-address-change** command)—The LAC continues to send packets to the original address but accepts packets from the new address.
- Reject configuration (specified by the **l2tp reject-transmit-address-change** command)—The LAC sends a Stop-Control-Connection-Notification (StopCCN) to the original address, then terminates the connection to the endpoint.

The reject specification takes precedence over the ignore specification.

The router accepts a change in receive address only once, during the tunnel establishment phase, and only on an SCCRPs packet. Subsequent changes result in the router dropping packets. Any changes do not affect established tunnels.

Use the **show l2tp** command to display the SCCRPs address change configuration.

***l2tp ignore-transmit-address-change***

- Use to set up the router to ignore address changes in SCCRPs control packets received from the remote endpoint.
- Use the **ip-address** or **udp-port** keyword to ignore the specific address component. Omit the keywords to ignore the entire address change in the SCCRPs packet.

- Example  
`host1(config)#l2tp ignore-transmit-address-change`
- Use the **no** version to return to the default; the router accepts address changes and port changes in SCCRP packets.

### ***l2tp reject-transmit-address-change***

- Use to set up the router to reject address changes in SCCRP control packets received from the remote endpoint.
- Use the **ip-address** or **udp-port** keyword to reject the specific address component. Omit the keywords to reject the entire address change in the SCCRP packet.
- Example  
`host1(config)#l2tp reject-transmit-address-change ip-address`
- Use the **no** version to return to the default; the router accepts address changes in SCCRP packets.

## **Configuring the LNS**

When you configure an LNS, you can configure it to accept calls from any LAC.



**NOTE:** If there is no explicit LNS configuration on the router, the UDP port used for L2TP traffic is closed, and no tunnels or sessions can be established.

To enable an LAC to connect to the LNS, you must create the following profiles:

- An L2TP destination profile—Defines the location of each LAC
- An L2TP host profile—Defines the attributes used when communicating with an LAC



**NOTE:** If you remove a destination profile or modify attributes of a host profile, all tunnels and sessions using the profile will be dropped.

To configure an LNS, perform the following steps:

1. Create a destination profile that defines the location of the LAC, and access L2TP Destination Profile Configuration mode.

```
host1:boston(config)#l2tp destination profile boston4 ip address 192.168.76.20
host1:boston(config-l2tp-dest-profile)#
```

2. Define the L2TP host profile and enter L2TP Destination Profile Host Configuration mode.

```
host1:boston(config-l2tp-dest-profile)#remote host default
host1:boston(config-l2tp-dest-profile-host)#
```

3. (Optional) Assign a profile name for a remote host.

```
host1:boston(config-l2tp-dest-profile-host)#profile georgeProfile1
```

4. (Optional) Disable the use of proxy LCP when connecting to the selected host.

```
host1(config-l2tp-dest-profile-host)#disable proxy lcp
```

5. (Optional) Enable the use of proxy authentication when connecting to the selected host.

```
host1(config-l2tp-dest-profile-host)#enable proxy authenticate
```

6. (Optional) Specify the local hostname to be used in any hostname AVP sends to the LAC.

```
host1(config-l2tp-dest-profile-host)#local host andy
```

7. (Optional) Specify the local IP address to be used in any packets sent to the LAC.

```
host1(config-l2tp-dest-profile-host)#local ip address 192.168.23.1
```

8. (Optional) Specify the shared secret used to authenticate the tunnel.

```
host1:boston(config-l2tp-dest-profile-host)#tunnel password saco
```

9. (Optional) Specify that L2TP create an MLPPP interface when LCP proxy data is not forwarded from the LAC.

```
host1:boston(config-l2tp-dest-profile-host)#default-upper-type mlppp
```



**NOTE:** When acting as the LNS, the E-series router supports dialed number identification service (DNIS). With DNIS, if users have a called number associated with them, the router searches the domain map for the called number. If it finds a match, the router uses the matching domain map entry information to authenticate the user. If the router does not find a match, it searches the domain map using normal processing. See [Using DNIS](#) in *Chapter 1, Configuring Remote Access*.

---



## Configuring Maximum LNS Sessions

You can use the **max-sessions** command in both L2TP Destination Profile Configuration mode and L2TP Destination Profile Host Configuration mode to configure the number of sessions allowed by the L2TP network server (LNS).

The LNS uses a two-step process to ensure that the maximum number of allowed sessions is not exceeded. When a session is requested, the LNS first checks the maximum sessions set for the L2TP destination profile. If no limit is set, or if the current count is less than the configured limit, the LNS then performs the same check on the L2TP destination host profile limit. If the current count is also less than the L2TP destination host profile limit, then the new session can be established. If a session request exceeds either of the max-sessions settings, the LNS rejects the session.



**NOTE:** New sessions are rejected once the chassis-wide session limit is exceeded, even if the destination profile or host profile maximum session limit is not exceeded.

### **default-upper-type mlppp**

- Use to specify that L2TP automatically create a Multilink PPP (MLPPP) interface for the LNS when LCP proxy data is not forwarded from the LAC. For example, the MLPPP interface is created if the LAC does not send the initial received or last received LCP configuration request.
- If full LCP proxy data is available, this command is ignored.
- Example  

```
host1(config-l2tp-dest-profile-host)#default-upper-type mlppp
```
- Use the **no** version to delete the default setting of MLPPP.

### **disable proxy lcp**

- Use to disable the use of proxy LCP when connecting to the selected host.
- Example  

```
host1(config-l2tp-dest-profile-host)#disable proxy lcp
```
- Use the **no** version to return to the default, proxy LCP enabled.

### **enable proxy authenticate**

- Use to enable the use of proxy authentication when connecting to the selected host.
- Example  

```
host1(config-l2tp-dest-profile-host)#enable proxy authenticate
```
- Use the **no** version to return to the default, proxy authentication disabled.

***l2tp destination profile***

- Use to create the destination profile that defines the location of the LAC, and access L2TP Destination Profile Configuration mode.
- If no virtual router is specified, the current virtual router context is used.
- If the destination address is 0.0.0.0, then any LAC that can be reached via the specified virtual router is allowed to access the LNS. If the destination address is nonzero, then it must be a host-specific IP address.
- The router supports up to 4,000 L2TP destination profiles.
- Example  

```
host1:boston(config)#l2tp destination profile boston ip address 10.10.76.12
host1:boston(config-l2tp-dest-profile)#
```
- Use the **no** version to remove the L2TP destination profile and all of its host profiles.



**NOTE:** If you remove a destination profile, all tunnels and sessions using that profile will be dropped.

---

***local host***

- Use to specify the local hostname to be used in any hostname AVP sends to the LAC.
- Example  

```
host1(config-l2tp-dest-profile-host)#local host l2tpHostP
```
- Use the **no** version to remove the local hostname and use the default, the router name.

***local ip address***

- Use to specify the local IP address to be used in any packets sent to the LAC.
- Example  

```
host1(config-l2tp-dest-profile-host)#local ip address 192.168.23.1
```
- Use the **no** version to remove the local IP address and use the default, the router's router ID.

***max-sessions***

- Use to configure the maximum number of sessions allowed by the LNS.
- Use in L2TP Destination Profile Configuration mode to set the maximum sessions allowed for the specified destination.
- Use in L2TP Destination Profile Host Configuration mode to set the maximum session allowed for the specified host.
- Example  

```
host1(config)#l2tp destination profile westford 10.10.21.2
host1(config-l2tp-destination-profile)#max-sessions 20000
```
- Use the **no** version to restore the default chassis-wide limit.

**remote host**

- Use to define the L2TP host profile and access L2TP Destination Profile Host Configuration mode.
- Each L2TP destination profile can have multiple L2TP host profiles.
- For an LAC to connect to an LNS, the appropriate L2TP destination profile *must* have at least one L2TP host profile.
- If you specify any name other than *default* for the remote host, then the LAC must supply the specified hostname in order for the tunnel to be set up. The remote hostname is matched against the hostname AVP in the received Start-Control-Connection-Request (SCCRQ).
- The remote hostname can be up to 64 characters (no spaces).
- Example

```
host1:boston(config)#l2tp destination profile boston1 ip address 192.168.76.12
host1:boston(config-l2tp-dest-profile)#remote host default
host1(config-l2tp-dest-profile-host)#
```

- Use the **no** version to remove the L2TP host profile.



**NOTE:** If you modify any attributes of a host profile, all tunnels and sessions using that profile will be dropped.

**tunnel password**

- Use to specify the shared secret to be used to authenticate the tunnel. The same password must be specified at both ends of the tunnel.
  - Example
- ```
host1:boston(config-l2tp-dest-profile-host)#tunnel password sacro
```
- Use the **no** version to remove the tunnel password. (This results in no tunnel authentication.)

Configuring the RADIUS Connect-Info Attribute on the LNS

You can configure the LNS to generate the RADIUS Connect-Info attribute [77]. Service providers can then use the information in the RADIUS attribute to identify a customer's service.

On the LNS, the Connect-Info attribute is based on the L2TP connect-speed AVPs received from the LAC. The LNS does not generate the attribute by default. The format of the Connect-Info attribute is as follows, where the TX speed and RX speed are equal to the respective L2TP AVPs:

```
tx-speed [ /rx-speed ]
```

Use the **radius connect-info-format** command to configure the LNS to generate the RADIUS Connect-Info attribute.

radius connect-info-format

- Use on the LNS to enable the generation of the RADIUS Connect-Info attribute.
- The TX speed is always included in the attribute when the speed is not zero; however, inclusion of the RX speed depends on the keyword you use with the command.
 - Use the **l2tp-connect-speed** keyword to specify that the RX speed is only included when it is not zero and also is different than the TX speed.
 - Example


```
host1(config)#radius connect-info-format l2tp-connect-speed
```
 - Use the **l2tp-connect-speed-rx-when-equal** keyword to specify that the RX speed is always included when it is not zero.
 - Example


```
host1(config)#radius connect-info-format l2tp-connect-speed-rx-when-equal
```
- Use the **no** version to disable the generation of the RADIUS Connect-Info attribute.

Selecting Tunnel-Service Modules for LNS Sessions Using MLPPP

You can install multiple tunnel-service modules in an E-series router deployed as an LNS where the tunnel sessions carry MLPPP. To use an LNS, at least one Service line module (SM), ES2-S1 Service IOA, or a module that supports the use of shared tunnel-server ports must be installed in the E-series router. For more information, see [Configuring the LAC](#) on page 219.

The router selects tunnel-service modules based on the LNS sessions that underlie the PPP link interfaces of an MLPPP bundle, also known as *bundled sessions*. To determine the appropriate SM where it places the first bundled session for an MLPPP bundle, the router uses a load-balancing mechanism. After the router determines the appropriate SM, it places all sessions for the same bundle on the same SM. By default, the router determines *bundled membership* based on the endpoint discriminator that the LNS receives from the LAC in the proxy LCP information.

For example, an ERX-1440 router has tunnel-service modules installed in slots 4, 9, and 12. Using the load-balancing mechanism, the router determines that the SM in slot 4 can accommodate the first bundled session for MLPPP bundle A, and places it there. The first bundled session for bundle A has an endpoint discriminator of 5. The router subsequently places all bundled sessions for bundle A (which have an endpoint discriminator of 5) on the SM in slot 4.

When the SM on which the bundled sessions reside has no more space for additional sessions, the router refuses the L2TP session. This can happen even when other tunnel-service modules installed in the router have available space.

For more information about endpoint discriminators, see [JUNOS Link Layer Configuration Guide, Chapter 5, Configuring Multilink PPP](#).

Assigning Bundled Group Identifiers

In some cases, an endpoint discriminator is not available for the LNS to use to identify the links in a bundled session.

This situation might occur when:

- PPP clients provide endpoint discriminators with null values.
- PPP clients do not provide an endpoint discriminator option when negotiating LCP with the LAC.
- The LAC does not include a endpoint discriminator option in the LCP proxy AVPs.

The router places all bundled sessions without endpoint discriminators on the same SM. However, if there are many such bundled sessions, the load-balanced distribution of LNS sessions across the tunnel-service modules can deteriorate because the router places all bundled sessions on the same SM without evenly distributing the load.

The **bundled-group-id** command enables you to correct this situation by assigning a numeric bundled group identifier for the router to use when the endpoint discriminator is unavailable to identify the bundled membership. The router places bundled sessions with the same bundled group identifier on the same SM in the same way that it does with endpoint discriminators.

The bundled group identifier applies to the entire router; therefore, if you assign the same bundled group identifier for different L2TP destination host profiles, the router places all of the bundled sessions with the same bundled group identifier on the same SM.



NOTE: We recommend that you assign bundled group identifiers only when you are certain that endpoint discriminators are unavailable to identify bundle membership.

Overriding All Endpoint Discriminators

You can also configure the router to ignore the value of all endpoint discriminators when it selects a SM and to use only the bundled group identifier that you assigned by issuing the **bundled-group-overrides-mlppp-ed** command.

Issuing the **bundled-group-id** and **bundled-group-id-overrides-mlppp-ed** commands together forces the router to place the bundled sessions on the same SM when a PPP client incorrectly specifies different endpoint discriminators for links in the same bundle.



NOTE: We strongly recommend that you use this feature only with the support of JTAC.

bundled-group-id

- Use to assign a bundled group identifier that the router uses when selecting a SM for bundled sessions when no endpoint discriminator is available.
- The router places all bundled sessions with the same bundled group identifier on the same SM.
- The bundled group identifier applies to the entire router; therefore, if you assign the same bundled group identifier for different L2TP destination host profiles, the router places all of the bundled sessions with the same bundled group identifier on the same SM.
- Example:
host1:boston(config-l2tp-dest-profile-host)#**bundled-group-id 4**
- Use the **no** version to restore the default, no assigned bundled group identifier.



NOTE: We recommend that you assign bundled group identifiers only when you are certain that endpoint discriminators are unavailable to identify bundle membership.

bundled-group-id-overrides-mlppp-ed

- Use to configure the router to ignore the value of all endpoint discriminators when selecting a SM and use only the bundled group identifiers that you assigned with the **bundled-group-id** command.
- Example
host1:boston(config-l2tp-dest-profile-host)#**bundled-group-id-overrides-mlppp-ed**
- Use the **no** version to remove the override.



NOTE: We strongly recommend that you use this command only with the support of JTAC.

Enabling Tunnel Switching

L2TP tunnel switching allows you to switch packets between one session terminating at an L2TP LNS and another session originating at an L2TP LAC. What distinguishes a tunnel-switched LAC from a conventional one is that there are two interface columns: one for the incoming session (LNS) and one for the outgoing session (LAC). The router forwards traffic from the incoming session to the outgoing session and vice versa.

You can select tunnel switching on a per-chassis basis. By default, tunnel switching is disabled. This preserves current behavior and prevents inadvertent attempts to switch tunnels.



NOTE: Each individual L2TP session involved in tunnel switching is counted toward the maximum number of sessions supported on an E-series router.

l2tp tunnel-switching

- Use to enable tunnel switching.
- Example
host1(config)#**l2tp tunnel-switching**
- Use the **no** version to disable tunnel switching. This is the default setting.

Enabling Tunnel Selection

This section presents the capabilities of the LAC's tunnel selection process. L2TP allows 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.

For information about setting up destinations and preference levels for a domain, see [Mapping a User Domain Name to an L2TP Tunnel](#) on page 224.

When the E-series 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

Failover Between Preference Levels

This tunnel selection method is the default method. If you do not set any tunnel selection parameters, the router uses this method.

When a user tries to log into a domain, the router attempts to connect to a destination in that domain with the highest preference level. If more than one destination in the preference level is considered reachable, the router randomly selects a destination and attempts to contact it. 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. The router makes up to eight attempts to connect to a destination for a domain—one attempt for each preference level.

If all destinations at a preference level are marked as unreachable, the router chooses the destination that failed first and tries to make a connection. The key is to understand that the router chooses a single destination at each level of preference, even if all destinations have recently failed. Thus the 5-minute timer normally used to reinstate failed destinations is ignored under certain conditions.

For example, suppose you have three destinations for a domain: A, B, and C. You assign the following preferences:

- A, B, and C at preference 0
- A, B, and C at preference 1
- A, B, and C at preference 2

A, B, and C are all considered reachable.

If a PPP user tries to connect to the domain, suppose the router randomly selects destination A from preference 0. If this connection attempt fails, the router excludes destination A for 5 minutes and goes to the next level (preference 1). From here, it randomly selects destination B, one of the two remaining choices. If the second connection attempt also fails, the router excludes destination B, as well as destination A, and attempts to connect to destination C, the only destination available with preference 2. The router has had an opportunity to connect to every destination available for the domain.

Support for multiple destinations affects the procedure for mapping a user domain name to an L2TP tunnel. To learn how to complete this mapping, see [Mapping a User Domain Name to an L2TP Tunnel](#) on page 224.

Failover Within a Preference Level

In this selection method, 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 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.

I2tp fail-over-within-preference

- Use to enable tunnel selection failover within a preference level.
- Example

```
host1(config)#I2tp fail-over-within-preference
```
- Use the **no** version to disable this feature and use the default round-robin selection method of tunnel selection.

Maximum Sessions per Tunnel

You can configure the maximum number of sessions per tunnel, either through a RADIUS server or the command-line interface. If you set the maximum sessions per tunnel parameter, the router takes the setting into consideration when it selects a tunnel. If a randomly selected tunnel has a current session count equal to its maximum session count, the router does not attempt to contact that tunnel. Instead, it makes an alternate tunnel selection 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 next selection. This process is consistent, regardless of which fail-over scheme is currently running on the router. A tunnel without a configured maximum sessions value has no upper limit on the number of sessions it can support.

max-sessions

- Use to configure the maximum sessions per tunnel.
- Example

```
host1(config)#aaa domain-map lacOne
host1(config-domain-map)#tunnel 1
host1(config-domain-map-tunnel)#max-sessions 1500
```
- Use the **no** version to disable this feature and return to the default value of 0 (zero), which allows unlimited sessions in the tunnel.

Weighted Load Balancing

With the weighted load-balancing method, 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 largest weight; the tunnel with the next largest maximum session value has the next largest weight, down to the tunnel with the smallest maximum session value that has the smallest weight.

I2tp weighted-load-balancing

- Use to base tunnel selection within a preference level on the maximum sessions per tunnel.
- Example

```
host1(config)#I2tp weighted-load-balancing
```
- Use the **no** version to disable this feature and return to the default round-robin tunnel selection method.

Creating Persistent Tunnels

The E-series router supports persistent tunnels. A persistent tunnel is one that is configured to remain available. Persistent tunnels have only local significance; that is, they apply only to the end of the tunnel where they are set. If the other end of the tunnel chooses to terminate the tunnel, the tunnel is removed.

l2tp tunnel idle-timeout

- Use to configure L2TP tunnel idle timeout.
- Use to create a persistent tunnel. You do this by setting the idle-timeout value to zero.
- Example

```
host1(config)#l2tp tunnel idle-timeout 0
```
- Use the **no** version to remove the idle timeout setting.

Testing Tunnel Configuration

The **l2tp tunnel test** command allows you to force the establishment of a tunnel to verify both the tunnel configuration and connectivity.

l2tp tunnel test

- Use to test a tunnel's configuration and connectivity.
- This command supports tunnel initiation: incoming calls on the LAC; outgoing calls on the LNS.
- This command does not support tunnel respondent: outgoing calls on the LAC; incoming calls on the LNS.
- Examples:

```
host1#l2tp tunnel test boston.com
host1#l2tp tunnel test portland.com gold
```
- There is no **no** version.

Managing L2TP

Configuring an E-series router for B-RAS enables the router to operate as an LAC with default settings. You can modify the default settings as follows:

- Enable the verification of data integrity via UDP.
- Specify the time period for which the router maintains dynamic destinations, tunnels, or sessions after termination.



NOTE: The previous two operations also apply to an LNS, however there is no default configuration that enables the LNS.

When the router is established as an LAC or LNS and is creating destinations, tunnels, and sessions, you can manage them as follows:

- Prevent the creation of new sessions, tunnels, and destinations.
- Close and reopen all or selected destinations, tunnels, and sessions.
- Specify the drain timeout, which is the amount of time a disconnected LAC tunnel waits before restarting after receiving a restart request.



NOTE: All the commands in this section apply to both the LAC and the LNS.

I2tp drain

- Use to prevent the creation of new destinations, tunnels, and sessions on the router.
- This command and the **I2tp shutdown** command both affect the administrative state of L2TP on the router. Although each command has a different effect, the **no** version of each command is equivalent. Each command's **no** version leaves L2TP in the enabled state.
- Example

```
host1(config)#I2tp drain
```
- Use the **no** version to enable the creation of destinations, tunnels, and sessions on the router.

I2tp drain destination

- Use to prevent the creation of new tunnels and sessions at a destination.
- This command and the **I2tp shutdown destination** command both affect the administrative state of L2TP for the destination. Although each command has a different effect, the **no** version of each command is equivalent. Each command's **no** version leaves L2TP in the enabled state.
- Example

```
host1(config)#I2tp drain destination ip 172.31.1.98
```
- Use the **no** version to enable the creation of tunnels and sessions for a destination.

I2tp drain tunnel

- Use to prevent the creation of new sessions for a tunnel.
- This command and the **I2tp shutdown tunnel** command both affect the administrative state of L2TP for the tunnel. Although each command has a different effect, the **no** version of each command is equivalent. Each command's **no** version leaves L2TP in the enabled state.

- Example
host1(config)#**l2tp drain tunnel virtual-router default ip 172.31.1.98 isp.com**
- Use the **no** version to enable the creation of sessions for a tunnel.

l2tp retransmission

- Use to specify the number of retransmission retries, in the range 2–7.
- Use the **established** keyword to apply the retry count only to established tunnels.
- Use the **not-established** keyword to apply the retry count only to tunnels that are not established.
- If you do not include a keyword, the router applies the retry count to both established and nonestablished tunnels.
- Example
host1(config)#**l2tp retransmission 4 established**
- Use the **no** version to set the retransmission retry count to the default, 5.

l2tp tunnel short-drain-timeout

- Use to specify the amount of time a disconnected LAC L2TP tunnel waits before restarting after it receives a restart request.
- Specify a drain timeout in the range 0–31 seconds. This feature enables the router to restart tunnels more quickly than the standard 31-second drain time specified by RFC-2661.
- Example
host1(config)#**l2tp tunnel short-drain-timeout 12**
- Use the **no** version to restore the default short-drain timeout of 2 seconds.

l2tp shutdown

- Use to close all destinations, tunnels, and sessions, and to prevent the creation of new destinations, tunnels, and sessions on the router.
- This command and the **l2tp drain** command both affect the administrative state of L2TP on the router. Although each command has a different effect, the **no** version of each command is equivalent. Each command's **no** version leaves L2TP in the enabled state.
- Example
host1(config)#**l2tp shutdown**
- Use the **no** version to enable the creation of new destinations, tunnels, and sessions.

I2tp shutdown destination

- Use to close all tunnels and sessions for a destination and to prevent the creation of tunnels and sessions for that destination.
- This command and the **i2tp drain destination** command both affect the administrative state of L2TP for the destination. Although each command has a different effect, the **no** version of each command is equivalent. Each command's **no** version leaves L2TP in the enabled state.
- Example

```
host1(config)#i2tp shutdown destination 1
```
- Use the **no** version to enable the creation of new tunnels and sessions for a destination.

I2tp shutdown session

- Use to close selected sessions.
- Example

```
host1(config)#i2tp shutdown session 1/1/1
```
- The **no** version has no effect, because sessions can be created only dynamically at this release.

I2tp shutdown tunnel

- Use to close all sessions in a tunnel and to prevent the creation of sessions in a tunnel.
- This command and the **i2tp drain tunnel** command both affect the administrative state of L2TP for the tunnel. Although each command has a different effect, the **no** version of each command is equivalent. Each command's **no** version leaves L2TP in the enabled state.
- Example

```
host1(config)#i2tp shutdown tunnel 1/isp.com
```
- Use the **no** version to enable the creation of new sessions for the tunnel.

Configuring Disconnect Cause Information

You can configure an E-series LNS to convey PPP-related disconnect cause information to its L2TP peer. Enabling an LNS to send disconnect cause information to an LAC is particularly useful in an environment where the LAC initiates tunnels without a client's request, knowledge, or approval. In this type of environment, all PPP signaling for the tunnel session takes place between the LNS and the client, without active participation of the LAC. As a result, the LAC is not aware of the reason that a session has disconnected.

Perform the following tasks to use the disconnect cause information feature:

- Enable disconnect cause AVP generation—You can specify that the LNS include the PPP Disconnect Cause Code AVP in all L2TP Call-Disconnect-Notify (CDN) messages that it sends to the LAC or you can limit generation for tunnels that use a particular host profile.

- Enable disconnect cause generation chassis-wide on the LNS:

```
host1(config)#l2tp disconnect-cause
```

- Enable disconnect cause generation for all tunnels that use a particular host profile on the LNS:

```
host1(config-l2tp-dest-profile-host)#disconnect-cause
```

- Enable RADIUS disconnect cause accounting—Specify that the Disconnect-Cause RADIUS attribute (VSA 26-51) is generated. At the LAC, this accounting will report remotely generated disconnect cause information received from the LNS. At the LNS, the accounting will report locally generated disconnect cause information.

```
host1(config)#radius include l2tp-ppp-disconnect-cause acct-stop enable
```

- Display the disconnect cause statistics—Display chassis-wide summary statistics for all disconnect cause information received by the LAC, sorted by code number.

```
host1(config)#show l2tp received-disconnect-cause-summary
```



NOTE: An E-series LAC does not send PPP Disconnect Cause Code AVPs to an LNS. In the event that a third-party LAC does send the AVP to an E-series LNS, the LNS discards the AVP.

disconnect-cause

- Use to specify that the E-series LNS generate PPP Disconnect Cause Code AVPs. This enables the LAC to obtain information about the cause of a session disconnection.
- This command pertains only to L2TP sessions to which the L2TP destination host profile applies. The AVP is included in all L2TP CDN messages that the LNS sends to an LAC for covered sessions.
- This command is used only for dial-in sessions; use **l2tp disconnect-cause** command in Global Configuration mode to generate PPP Disconnect Cause Code AVPs for dial-out sessions.

- Example

```
host1(config-l2tp-dest-profile-host)#disconnect-cause
```

- Use the **no** version to disable generation of the PPP Disconnect Cause Code AVP for all covered sessions.

l2tp disconnect-cause

- Use to specify that the E-series LNS generate PPP Disconnect Cause Code AVPs, which enables the LAC to obtain information about the cause of a session disconnection.
- This command enables generation of the PPP Disconnect Cause Code AVP for all L2TP sessions for the LNS. The AVP is included in all L2TP CDN messages that the LNS sends to an LAC.
- Example

```
host1(config)#l2tp disconnect-cause
```
- Use the **no** version to restore the default setting, which disables chassis-wide generation of the PPP Disconnect Cause Code AVP for all L2TP sessions for the LNS. Sessions for which the AVP generation is enabled by the host-profile-specific **disconnect-cause** command continue to generate the AVP.

radius include l2tp-ppp-disconnect-cause acct-stop enable

- Use to enable disconnect cause accounting by specifying that the Disconnect-Cause RADIUS attribute (VSA 26-51) is included in RADIUS acct-stop and acct-tunnel-link-stop records.
 - At the LAC, disconnect cause accounting reports remotely generated disconnect cause information received from the LNS.
 - At the LNS, the accounting reports locally generated disconnect cause information.
- Example

```
host1(config)#radius include l2tp-ppp-disconnect-cause acct-stop enable
```
- Use the **acct-stop disable** version to disable the inclusion of the RADIUS attribute.
- Use the **no** version to restore the default setting, which disables the inclusion of the RADIUS attribute.

Configuring the Receive Window Size

You can configure the L2TP receive window size (RWS) for an L2TP tunnel. L2TP uses the RWS to implement a sliding window mechanism for the transmission of control messages.

When you configure the RWS, you specify the number of packets that the L2TP peer can transmit without receiving an acknowledgment from the router. If the RWS is not configured, the router determines the RWS and uses this value for all new tunnels on both the LAC and the LNS.

You can configure the L2TP RWS in the following ways:

- Configure the systemwide default RWS setting for a tunnel on both the LAC and the LNS by using the **l2tp tunnel default-receive-window** command (in Global Configuration mode).
- Configure the RWS for a tunnel on the LAC by using either the **receive-window** command (in Domain Map Tunnel Configuration mode) or by including the L2tp-Recv-Window-Size RADIUS attribute (VSA 26-54) in RADIUS Access-Accept messages.
- Configure the RWS for all tunnels that use a particular host profile on the LNS by using the **receive-window** command (in L2TP Destination Profile Host Configuration mode).

The following sections describe each of these methods for configuring the RWS.

Configuring the Default RWS

To configure the default RWS setting:

1. From Global Configuration mode, set the L2TP default RWS. The only value supported for the default RWS is 4.

```
host1(config)#l2tp tunnel default-receive-window 4
```

The router uses this RWS value for all new tunnels on both the LAC and the LNS.

2. (Optional) Use the **show l2tp** command to verify the default RWS configuration.

```
host1#show l2tp
Configuration
  L2TP administrative state is enabled
  Dynamic interface destruct timeout is 600 seconds
  Data packet checksums are disabled
  Receive data sequencing is not ignored
  Tunnel switching is disabled
  Retransmission retries for established tunnels is 5
  Retransmission retries for not-established tunnels is 5
  Tunnel idle timeout is 60 seconds
  Failover within a preference level is disabled
  Weighted load balancing is disabled
  Tunnel authentication challenge is enabled
  Calling number avp is enabled
  Ignore remote transmit address change is disabled
  Disconnect cause avp is disabled
  Default receive window size is 4
Sub-interfaces      total    active    failed    auth-errors
Destinations        0         0         0         n/a
Tunnels              0         0         0         0
Sessions             0         0         0         n/a
Switched-sessions   0         0         0         n/a
```


l2tp tunnel default-receive-window

- Use to configure the default L2TP RWS for a tunnel on both the LAC and the LNS.
- The default L2TP RWS is the number of packets that the L2TP peer can transmit without receiving an acknowledgment from the router. The only supported value is 4.
- This command affects only those tunnels configured on the router after the command is issued; it has no effect on previously configured tunnels.
- Example

```
host1(config)#l2tp tunnel default-receive-window 4
```

- Use the **no** version to restore the default behavior, in which the router chooses the default L2TP RWS.

Configuring the RWS on the LAC

To configure the RWS for a tunnel on the LAC:

1. Access Domain Map Tunnel Configuration mode as described in [Mapping a User Domain Name to an L2TP Tunnel](#) on page 224. For example:

```
host1(config)#aaa domain-map fms.com
host1(config-domain-map)#router-name westford
host1(config-domain-map)#tunnel 3
host1(config-domain-map-tunnel)#
```

2. From Domain Map Tunnel Configuration mode, set the tunnel RWS. The only value supported for the tunnel RWS is 4, and it must be the same for all users of the same tunnel.

```
host1(config-domain-map-tunnel)#receive-window 4
```

3. (Optional) Use the **show aaa domain-map** command to verify the RWS configuration.

```
host1#show aaa domain-map
```

```
Domain: fms.com; router-name: westford; ipv6-router-name: default
```

Tunnel Tag	Tunnel Peer	Tunnel Source	Tunnel Type	Tunnel Medium	Tunnel Password	Tunnel Id	Tunnel Client Name
3	<null>	<null>	l2tp	ipv4	<null>	<null>	<null>

Tunnel Tag	Tunnel Server Name	Tunnel Preference	Tunnel Max Sessions	Tunnel RWS
3	<null>	2000	0	4

You can also configure the RWS for a tunnel on the LAC by including the L2tp-Recv-Window-Size RADIUS attribute (VSA 26-54) in RADIUS Access-Accept messages. For more information about RADIUS Access-Accept messages, see [Chapter 2, Configuring RADIUS Attributes](#). For more information about the L2tp-Recv-Window-Size attribute, see [Appendix A, RADIUS Attribute Descriptions](#).

receive-window

- Use to configure the L2TP RWS for a tunnel on the LAC.
- The tunnel RWS is the number of packets that the L2TP peer can transmit without receiving an acknowledgment from the router. The only supported value supported is 4.
- The RWS setting must be the same for all users of the same tunnel.
- If you modify the RWS setting for an existing tunnel, subsequent tunnel users might be not be able to log in if their RWS setting conflicts with the new RWS setting for the tunnel.
- Example

```
host1(config-domain-map-tunnel)#receive-window 4
```
- Use the **no** version to revert to the systemwide RWS setting configured with the **l2tp tunnel default-receive-window** command.

Configuring the RWS on the LNS

To configure the RWS for a tunnel on the LNS:

1. Access L2TP Destination Profile Host Configuration mode as described in [Configuring the LNS](#) on page 239. For example:

```
host1(config)#virtual-router fms02
host1:fms02(config)#l2tp destination profile fms02 ip address 192.168.5.61
host1:fms02(config-l2tp-dest-profile)#remote host fms03
host1:fms02(config-l2tp-dest-profile-host)#
```

2. From Destination Profile Host Configuration mode, set the tunnel RWS. The only value supported for the tunnel RWS is 4.

```
host1:fms02(config-l2tp-dest-profile-host)#receive-window 4
```

3. (Optional) Use the **show l2tp destination profile** command to verify the RWS configuration.

```
host1:fms02#show l2tp destination profile fms02
L2TP destination profile fms02
Destination address
  Transport ipUdp
  Virtual router fms02
  Peer address 192.168.5.61
Host profile attributes
  Remote host is fms03
  Receive window size is 4
1 L2TP host profile found
```

receive-window

- Use to configure the L2TP RWS for a tunnel on the LNS.
- The RWS is the number of packets that the L2TP peer can transmit without receiving an acknowledgment from the router. The only value supported for the RWS is 4.
- If you modify the RWS setting of a host profile for an existing tunnel, the router drops the tunnel. This action is consistent with router behavior when you modify an L2TP host profile.
- Example

```
host1:boston(config-l2tp-dest-profile-host)#receive-window 4
```
- Use the **no** version to revert to the systemwide RWS setting configured with the **l2tp tunnel default-receive-window** command.

Configuring Peer Resynchronization

The JUNOS software enables you to configure the peer resynchronization method you want the router to use. Peer resynchronization enables L2TP to recover from a router warm start and to allow an L2TP failed endpoint to resynchronize with its peer non-failed endpoint.

L2TP peer resynchronization:

- Prevents the non-failed 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 non-failed endpoint

To ensure successful peer resynchronization between endpoints, the non-failed endpoint must support a complete RFC-compliant L2TP implementation.

JUNOS software supports both the L2TP silent failover method and the L2TP failover protocol method, which is described in Fail Over extensions for L2TP “failover” draft-ietf-l2tpext-failover-06.txt. You can configure L2TP to use the failover protocol method as the primary peer resynchronization method, but then fall back to the silent failover method if the peer does not support the failover protocol method.

The following list highlights differences between the failover protocol and silent failover peer resynchronization methods:

- With the L2TP failover protocol method, both endpoints must support the method or recovery always fails. The L2TP failover protocol method also requires a non-failed endpoint to wait an additional recovery time period while the failed endpoint is recovering to prevent the non-failed endpoint from prematurely disconnecting the tunnel. The additional recovery period makes L2TP less responsive to the loss of tunnel connectivity.
- Silent failover operates entirely within the failed endpoint and does not require non-failed endpoint support—this improves interoperability between peers. Silent failover does not require additional recovery time by the non-failed endpoint, which also eliminates the potential for degraded responsiveness to the loss of tunnel connectivity.



NOTE: L2TP silent failover is not supported on E3 ATM and CT1 line modules in peer-facing configurations.

You can use the CLI or RADIUS to configure the resynchronization method for your router.

Using the CLI to Configure Peer Resynchronization

The JUNOS CLI enables you to configure the peer resynchronization method globally, for a host profile, or for a domain map tunnel. A host profile or domain map tunnel configuration takes precedence over the global peer resynchronization configuration.

When you change the peer resynchronization method, the change is not immediately applied to existing tunnels. Tunnels continue using their current resynchronization method until the next time the tunnel is reestablished.

failover-resync

- Use to configure the L2TP peer resynchronization method for L2TP host profiles and AAA domain map tunnels.
- This command takes precedence over the global peer resynchronization configuration.
- Choose one of the following keywords to specify the peer resynchronization method.
 - **failover-protocol**—The tunnel uses the L2TP failover protocol method. If the peer non-failed endpoint does not support the L2TP failover protocol, a failover forces disconnection of the tunnel and all of its sessions.
 - **failover-protocol-fallback-to-silent-failover**—The tunnel uses the L2TP failover protocol method; however, if the peer non-failed endpoint does not support the L2TP failover protocol method, the tunnel falls back to using the silent failover method.
 - **silent-failover**—The tunnel uses the silent failover method. The tunnel also informs its peer that it supports the failover protocol method for the peer's failovers.

- **disable**—The tunnel does not use any peer resynchronization method for its own failovers. The tunnel informs its peer that it supports the failover protocol method for the peer's failovers. A failover forces the disconnection of the tunnel and all of its sessions.
- **not-configured**—Peer resynchronization is not configured for L2TP host profiles and AAA domain map tunnels. L2TP uses the global failover method.
- By default, peer resynchronization is not configured at the L2TP profile-level or the domain map-level—therefore, the global configuration is used. This is different than using the **disable** keyword, which specifies that no peer synchronization method is used.
- Use the **show l2tp destination profile** command to display a host profile's peer resynchronization configuration and the **show aaa domain-map** command to display a domain map's configuration.
- Example 1—L2TP Host Profiles

```
host1(config)#l2tp destination profile lac-dest ip address 192.168.20.2
host1(config-l2tp-dest-profile)#remote host lac-host
host1(config-l2tp-dest-host-profile-host)#failover-resync silent-failover
```
- Example 2—AAA Domain Map Tunnels

```
host1(config)#aaa domain-map lac-tunnel
host1(config-domain-map)#tunnel 10
host1(config-domain-map-tunnel)#failover-resync silent-failover
```
- Use the **no** version to restore the default not-configured setting, in which no peer resynchronization method is configured.

l2tp failover-resync

- Use to configure the global L2TP peer resynchronization method that L2TP failed endpoints use to resynchronize with a peer non-failed endpoint.
- Choose one of the following keywords to specify the peer resynchronization method. All tunnels in the chassis use the specified method unless it is overridden by an L2TP host profile configuration or an AAA domain map configuration.
 - **failover-protocol**—Tunnels use the L2TP failover protocol method. If the peer non-failed endpoint does not support the L2TP failover protocol, a failover forces disconnection of all tunnels and their sessions.
 - **failover-protocol-fallback-to-silent-failover**—Tunnels use the L2TP failover protocol method; however, if the peer non-failed endpoint does not support the L2TP failover protocol method, the tunnel falls back to using the silent failover method.
 - **silent-failover**—Tunnels use the silent failover method. The tunnels also inform their peers that they support the failover protocol method for peer failovers.
 - **disable**—Tunnels do not use any peer resynchronization method for their own failovers. Tunnels inform their peers that they support the failover protocol method for peer failovers. A failover forces the disconnection of all tunnels and sessions.

- Use the **show l2tp** command to display the global peer resynchronization configuration.
- Example

```
host1(config)#l2tp failover-resync silent-failover
```
- Use the **default** version to restore the global default setting of the **failover-protocol-fallback-to-silent-failover** method.
- Use the **no** version to disable peer resynchronization—this is the same as using the **disable** keyword.

Using RADIUS to Configure Peer Resynchronization

The JUNOS software supports the use of RADIUS to configure the L2TP peer resynchronization method used by your L2TP tunnels. You use the L2TP-Resynch-Method RADIUS attribute (VSA 26-90) in RADIUS Access-Accept messages to specify the L2TP peer resynchronization method.

[Table 24](#) describes the L2TP-Resynch-Method RADIUS attribute. For more information about RADIUS Access-Accept messages, see [Chapter 2, Configuring RADIUS Attributes](#). For more information about the L2TP-Resynch-Method attribute, see [Appendix A, RADIUS Attribute Descriptions](#).

Table 24: L2TP-Resynch-Method RADIUS Attribute

Standard Number	Attribute Name	Description	Length	Subtype Length	Value
[26-90]	L2TP-Resynch-Method	L2TP peer resynchronization method	12	6	integer: <ul style="list-style-type: none"> ■ 0 = disabled ■ 1 = failover protocol ■ 2 = silent failover ■ 3 = failover protocol with silent failover as backup

Configuring L2TP Tunnel Switch Profiles

You can use the **l2tp switch-profile** command to create an L2TP tunnel switch profile. An *L2TP tunnel switch profile* is a set of characteristics that defines the behavior of L2TP tunnel switching for the interfaces to which the profile is assigned.

Within the L2TP tunnel switch profile, you configure a particular tunnel switching behavior for a specified L2TP AVP. For example, you can configure the router to preserve the value of (relay) a specified AVP type across the LNS/LAC boundary in an L2TP tunnel-switched network.

Applying the L2TP Tunnel Switch Profile

Configuring an L2TP tunnel switch profile has no effect by itself. To use the tunnel switch profile in an L2TP tunnel-switched network, you must apply it to an L2TP outbound LAC session by using one of the following methods:

- Authentication, authorization, and accounting (AAA) domain maps
- AAA tunnel groups
- RADIUS Access-Accept messages

If none of these methods are used, you can apply the L2TP tunnel switch profile as an AAA default tunnel parameter. The default tunnel switch profile has lower precedence than the other methods for applying the tunnel switch profile.

For more information about the methods for applying L2TP tunnel switch profiles, see [Configuration Tasks](#) on page 264.

Configuration Guidelines

The following rules apply when you configure L2TP tunnel switch profiles:

- L2TP tunnel switching must be enabled for tunnel switch profiles to take effect. For information, see [Enabling Tunnel Switching](#) on page 265.
- L2TP tunnel switch profiles have no effect when they are assigned to a LAC session that is not tunnel switched.
- The router can relay only those AVPs that are accepted at the LNS. Malformed AVPs are never relayed.
- If a tunnel grant response specifies a named tunnel switch profile that has not been configured on the router, the router prohibits connection of the L2TP tunnel-switched session.
- If you remove a tunnel switch profile, the router also disconnects all associated L2TP switched sessions using that profile.
- In some cases, attributes configured in a tunnel switch profile take precedence over similar attributes configured globally on the router.

For example, configuring L2TP Calling Number AVP 22 for relay overrides the **l2tp disable calling-number-avp** command issued from Global Configuration mode to prevent the router from sending AVP 22 in incoming-call-request (ICRQ) packets. In this scenario, the router relays the Calling Number AVP.

Configuring L2TP AVPs for Relay

Previously, the router did not preserve the values of incoming L2TP AVPs across the LNS/LAC boundary in an L2TP tunnel-switched network. The router regenerated most incoming AVPs, such as L2TP Calling Number AVP 22, based on the local policy in effect. However, some AVPs, such as Cisco NAS Port Info AVP 100, were dropped.

In an L2TP tunnel switch profile, you can define the types of AVPs that the router can relay unchanged across the LNS/LAC boundary. You can specify that the router relay one or more of the following AVP types:

- L2TP Bearer Type AVP 18
- L2TP Calling Number AVP 22
- Cisco NAS Port Info AVP 100

When you configure any of these AVP types for relay in an L2TP tunnel-switched network, the router preserves the value of an incoming AVP of this type when packets are switched between the inbound LNS session and the outbound LAC session.

Configuration Tasks

To configure and use an L2TP tunnel switch profile in an L2TP tunnel-switched network:

1. Ensure that L2TP tunnel switching is enabled on the router.
2. Configure the L2TP tunnel switch profile.
3. Apply the L2TP tunnel switch profile to the tunnel in one of the following ways:
 - To apply a named tunnel switch profile through an AAA domain map, use the **switch-profile** command from Domain Map Tunnel Configuration mode. For details, see [Applying L2TP Tunnel Switch Profiles by Using AAA Domain Maps](#) on page 266.
 - To apply a named tunnel switch profile through an AAA tunnel group, use the **switch-profile** command from Tunnel Group Tunnel Configuration mode. For details, see [Applying L2TP Tunnel Switch Profiles by Using AAA Tunnel Groups](#) on page 267.
 - To apply a named tunnel switch profile through RADIUS, include the Tunnel-Switch-Profile RADIUS attribute (VSA 26-91) in RADIUS Access-Accept messages. For details, see [Applying L2TP Tunnel Switch Profiles by Using RADIUS](#) on page 268.
 - To apply a default tunnel switch profile to a virtual router, use the **aaa tunnel switch-profile** command from Global Configuration mode. For details, see [Applying Default L2TP Tunnel Switch Profiles](#) on page 269.

The following sections describe how to perform each of these tasks.

Enabling Tunnel Switching

To enable L2TP tunnel switching on the router, use the **l2tp tunnel-switching** command. By default, tunnel switching is disabled.

For more information, see [Enabling Tunnel Switching](#) on page 246.

l2tp tunnel-switching

- Use to enable tunnel switching.
- Example

```
host1(config)#l2tp tunnel-switching
```
- Use the **no** version to disable tunnel switching. This is the default setting.

Configuring L2TP Tunnel Switch Profiles

To configure an L2TP tunnel switch profile:

1. Create the L2TP tunnel switch profile and assign it a name. The **l2tp switch-profile** command accesses L2TP Tunnel Switch Profile Configuration mode.

```
host1(config)#l2tp switch-profile concord
host1(config-l2tp-tunnel-switch-profile)#
```

2. Configure the L2TP tunnel switching behavior for the interfaces to which this profile is assigned.

The following commands configure the router to relay the Bearer Type, Calling Number, and Cisco NAS Port Info AVP types across the LNS/LAC boundary.

```
host1(config-l2tp-tunnel-switch-profile)#avp bearer-type relay
host1(config-l2tp-tunnel-switch-profile)#avp calling-number relay
host1(config-l2tp-tunnel-switch-profile)#avp cisco-nas-port relay
```

3. (Optional) Use the **show l2tp switch-profile** command to verify configuration of the tunnel switch profile.

```
host1(config-l2tp-tunnel-switch-profile)#run show l2tp switch-profile
L2TP tunnel switch profile concord
L2TP tunnel switch profile myProfile
2 L2TP tunnel switch profiles found

host1(config-l2tp-tunnel-switch-profile)#run show l2tp switch-profile concord
L2TP tunnel switch profile concord
  AVP bearer type action is relay
  AVP calling number action is relay
  AVP Cisco nas port info action is relay
```

avp

- Use in an L2TP tunnel switch profile to define the L2TP tunnel switching behavior for a specified L2TP AVP type.
- To cause the router to preserve the value of an incoming AVP of this type when packets are switched between an inbound LNS session and an outbound LAC session, issue the **avp** command with the **relay** keyword.
- You can use any of the following keywords to specify the AVPs for the router to relay:
 - **bearer-type**—L2TP Bearer Type AVP 18; by default, the router regenerates this AVP at the outbound LAC session, based on the local policy in effect
 - **calling-number**—L2TP Calling Number AVP 22; by default, the router regenerates this AVP at the outbound LAC session, based on the local policy in effect
 - **cisco-nas-port**—Cisco NAS Port Info AVP 100; by default, the router drops this AVP
- Example


```
host1(config-l2tp-tunnel-switch-profile)#avp calling-number relay
```
- Use the **no** version to restore the default L2TP tunnel switching behavior (regenerate or drop) for incoming AVPs of the specified type.

l2tp switch-profile

- Use to create and name an L2TP tunnel switch profile.
- The **l2tp switch-profile** command accesses L2TP Tunnel Switch Profile Configuration mode, from which you can define the L2TP tunnel switching behavior for the interfaces to which this profile is assigned.
- You must specify a name for the L2TP tunnel switch profile; the name can be a string of up to 64 alphanumeric characters.
- Example


```
host1(config)#l2tp switch-profile newyork
```
- Use the **no** version to remove the named tunnel switch profile from the router.

Applying L2TP Tunnel Switch Profiles by Using AAA Domain Maps

To apply an L2TP tunnel switch profile to sessions associated with an AAA domain map:

1. Access Domain Map Tunnel Configuration mode.

```
host1(config)#aaa domain-map westford.com
host1(config-domain-map)#router-name default
host1(config-domain-map)#tunnel 3
host1(config-domain-map-tunnel)#
```

For more information about how to map a domain to an L2TP tunnel from Domain Map Tunnel Configuration mode, see [Mapping a User Domain Name to an L2TP Tunnel](#) on page 224.

- From Domain Map Tunnel Configuration mode, issue the **switch-profile** command to apply the specified L2TP switch profile to the sessions associated with this domain map.

```
host1(config-domain-map-tunnel)#switch-profile concord
```

- (Optional) Use the **show aaa domain-map** command to verify application of the tunnel switch profile.

```
host1(config-domain-map-tunnel)#run show aaa domain-map
```

```
Domain: westford.com; router-name: default; ipv6-router-name: default
```

Tunnel Tag	Tunnel Peer	Tunnel Source	Tunnel Type	Tunnel Medium	Tunnel Password	Tunnel Id	Tunnel Client Name
3	<null>	<null>	l2tp	ipv4	<null>	<null>	<null>

Tunnel Tag	Tunnel Server Name	Tunnel Preference	Tunnel Max Sessions	Tunnel RWS	Tunnel Virtual Router	Tunnel Switch Profile
3	<null>	2000	0	system chooses	<null>	concord

switch-profile

- Use from Domain Map Tunnel Configuration mode to apply the specified L2TP tunnel switch profile to sessions associated with an AAA domain map.
- Example

```
host1(config-domain-map-tunnel)#switch-profile boston
```

- Use the **no** version to remove the tunnel switch profile assignment from the AAA domain map.

Applying L2TP Tunnel Switch Profiles by Using AAA Tunnel Groups

To apply an L2TP tunnel switch profile to sessions associated with an AAA tunnel group:

- Access Tunnel Group Tunnel Configuration mode.

```
host1(config)#aaa tunnel-group sunnyvale
host1(config-tunnel-group)#tunnel 3
host1(config-tunnel-group-tunnel)#
```

For more information about how to map a domain to an L2TP tunnel from Tunnel Group Tunnel Configuration mode, see [Mapping a User Domain Name to an L2TP Tunnel](#) on page 224.

- From Tunnel Group Tunnel Configuration mode, issue the **switch-profile** command to apply the specified L2TP switch profile to the sessions associated with this tunnel group.

```
host1(config-tunnel-group-tunnel)#switch-profile sanjose
```

- (Optional) Use the **show aaa tunnel-group** command to verify application of the tunnel switch profile.

```
host1(config-tunnel-group-tunnel)#run show aaa tunnel-group
```

```
Tunnel Group: sunnyvale
```

Tunnel Tag	Tunnel Peer	Tunnel Source	Tunnel Type	Tunnel Medium	Tunnel Password	Tunnel Id	Tunnel Client Name
3	<null>	<null>	l2tp	ipv4	<null>	<null>	<null>
Tunnel Tag	Tunnel Server Name	Tunnel Preference	Tunnel Max Sessions	Tunnel RWS		Tunnel Virtual Router	Tunnel Switch Profile
3	<null>	2000	0	system chooses		<null>	sanjose

switch-profile

- Use from Tunnel Group Tunnel Configuration mode to apply the specified L2TP tunnel switch profile to sessions associated with an AAA tunnel group.

- Example

```
host1(config-tunnel-group-tunnel)#switch-profile chicago
```

- Use the **no** version to remove the tunnel switch profile assignment from the AAA tunnel group.

Applying L2TP Tunnel Switch Profiles by Using RADIUS

On the LAC, the router can receive tunnel configuration attributes through a RADIUS authentication server. To use RADIUS to apply an L2TP tunnel switch profile to a session, you can configure RADIUS to include the Tunnel-Switch-Profile RADIUS attribute (VSA 26-91) in RADIUS Access-Accept messages.

For more information about RADIUS Access-Accept messages, see [Chapter 2, Configuring RADIUS Attributes](#). For more information about the Tunnel-Switch-Profile attribute, see [Appendix A, RADIUS Attribute Descriptions](#).

Applying Default L2TP Tunnel Switch Profiles

You can apply a default L2TP tunnel switch profile to a virtual router by issuing the **aaa tunnel switch-profile** command from Global Configuration mode. The router uses the default tunnel switch profile if the tunnel attributes returned from an AAA domain map or tunnel group or from a RADIUS authentication server do not include a named tunnel switch profile.

The default L2TP tunnel switch profile applies to a specific virtual router. You can apply a different default tunnel switch profile to each virtual router configured.

To apply a default L2TP tunnel switch profile to a virtual router:

1. Create the virtual router to which you want to apply the default tunnel switch profile.

```
host1(config)#virtual-router east
host1:east(config)#
```

2. Issue the **aaa tunnel switch-profile** command to apply the default L2TP tunnel switch profile in the context of this virtual router.

```
host1:east(config)#aaa tunnel switch-profile boston
```

3. (Optional) Use the **show aaa tunnel-parameters** command to verify application of the default tunnel switch profile.

```
host1:east(config)#run show aaa tunnel-parameters
Tunnel password is <NULL>
Tunnel client-name is <NULL>
Tunnel nas-port-method is none
Tunnel switch-profile is boston
Tunnel nas-port ignore disabled
Tunnel nas-port-type ignore disabled
Tunnel assignmentId format is assignmentId
Tunnel calling number format is descriptive
```

aaa tunnel switch-profile

- Use to apply a default L2TP tunnel switch profile to a virtual router.
- The router uses the default tunnel switch profile if the tunnel attributes returned from an AAA domain map or tunnel group or from a RADIUS authentication server *do not include* a named tunnel switch profile.

The router ignores the default tunnel switch profile if the tunnel attributes returned from an AAA domain map or tunnel group or from a RADIUS authentication server *do include* a named tunnel switch profile.

- Example

```
host1:west(config)#aaa tunnel switch-profile denver
```

- Use the **no** version to remove the tunnel switch profile assignment from the virtual router.

Configuring the Transmit Connect Speed Calculation Method

You can configure the method that the router uses to calculate the transmit connect speed of the subscriber's access interface for a tunneled L2TP session. L2TP reports the transmit connect speed in L2TP Transmit (TX) Speed AVP 24. During the establishment of an L2TP tunnel session, the LAC sends AVP 24 to the LNS to convey the transmit speed of the subscriber's access interface.

You can configure the calculation method for the transmit connect speed reported in L2TP Transmit (TX) Speed AVP 24 in any of the following ways. The first three methods—AAA domain maps, AAA tunnel groups, and RADIUS—are mutually exclusive.

- AAA domain maps—Use the **tx-connect-speed-method** command from Domain Map Tunnel Configuration mode. For instructions, see [Using AAA Domain Maps to Configure the Transmit Connect Speed Calculation Method](#) on page 274.
- AAA tunnel groups—Use the **tx-connect-speed-method** command from Tunnel Group Tunnel Configuration mode. For instructions, see [Using AAA Tunnel Groups to Configure the Transmit Connect Speed Calculation Method](#) on page 275.
- RADIUS—Include the Tunnel-Tx-Speed-Method RADIUS attribute (Juniper Networks VSA 26-94) in RADIUS Access-Accept messages. For instructions, see [Using RADIUS to Configure the Transmit Connect Speed Calculation Method](#) on page 276.
- AAA default tunnel parameters—Use the **aaa tunnel tx-connect-speed-method** command from Global Configuration mode. The router uses the calculation method specified with this command if the tunnel attributes returned from an AAA domain map, an AAA tunnel group, or a RADIUS authentication server do not include the transmit connect speed calculation method. For instructions, see [Using AAA Default Tunnel Parameters to Configure the Transmit Connect Speed Calculation Method](#) on page 277.

Calculation Methods

In previous releases, the router calculated the transmit speed of the subscriber's access interface based only on statically configured settings for the underlying layer 2 access interface. With this feature, you can obtain a more accurate representation of the transmit connect speed by choosing a calculation method that reflects changes to the layer 2 interface due to statically configured settings, dynamically configured settings, or QoS settings.

You can choose one of the following methods for calculating the transmit connect speed that is reported in L2TP Transmit (TX) Speed AVP 24:

- Static layer 2
- Dynamic layer 2
- QoS
- Actual (lesser of dynamic layer 2 or QoS)

The following sections describe each of these calculation methods.



NOTE: Configuring the transmit connect speed calculation method has no effect on the operation of the L2TP Receive (RX) Speed AVP 38 or the Connect-Info RADIUS attribute [77] at the LAC.

Static Layer 2

The static layer 2 method calculates the transmit connect speed of the subscriber's access interface based on the statically configured settings for the underlying layer 2 ATM 1483 or Ethernet interface. The static layer 2 method does not reflect changes to the transmit speed of the layer 2 interface due to dynamically configured settings or to QoS.

For ATM 1483 circuits, the static layer 2 value is based on the bandwidth that the connection requires. The router uses certain traffic parameters for each service category to determine the required bandwidth for the connection. For more information about how the router computes bandwidth for ATM 1483 circuits, see [Connection Admission Control](#) in *JUNOS Link Layer Configuration Guide, Chapter 1, Configuring ATM*.

For Ethernet VLANs, the static layer 2 value is the advisory transmit speed of the VLAN subinterface, if configured with the **vlan advisory-tx-speed** command, or the speed of the underlying physical port if the advisory transmit speed is not configured.

If there is no explicit static configuration for the layer 2 interface, L2TP reports the speed of the underlying physical port as the transmit connect speed.

Dynamic Layer 2

The dynamic layer 2 method calculates the transmit connect speed of the subscriber's access interface based on the dynamically configured settings for the underlying layer 2 interface.

If there is no dynamic configuration for the layer 2 interface, L2TP reports the transmit connect speed based on statically configured settings. If there is no static speed configuration for the layer 2 interface, L2TP reports the speed of the underlying physical port as the transmit connect speed.

QoS

The QoS method calculates the transmit connect speed of the subscriber's access interface based on settings determined by static or dynamic QoS configurations. This calculation is based on the interface columns that QoS uses to build scheduler profiles for L2TP sessions. For example, a typical interface column might consist of an L2TP session over an Ethernet VLAN over a Gigabit Ethernet interface.

You can configure QoS to control the rate of any logical interface in the interface column. For those logical interfaces with a rate controlled by QoS, QoS reports this configured rate as the transmit connect speed for that interface. For those logical interfaces that do not have a QoS-configured rate, QoS reports the speed of the underlying physical port as the transmit connect speed.

For more information, see [QoS and L2TP TX Speed AVP 24](#) in *JUNOS Quality of Service Configuration Guide, Chapter 10, Configuring QoS for L2TP*.

Actual

The actual method calculates the transmit connect speed of the subscriber's access interface as the lesser of the following two values:

- Value using the dynamic layer 2 calculation method
- Value using the QoS calculation method

Calculation Examples

The examples in this section illustrate how the router uses the methods described in [Calculation Methods](#) on page 270 to calculate the transmit connect speed.

Example 1: L2TP Session over ATM 1483 Interface

In this example, an L2TP session is established over an ATM 1483 subinterface on an OC3/STM1 ATM IOA. The configuration has the following characteristics:

- There is no explicit static configuration for the layer 2 (ATM 1483) interface.
- A transmit connect speed of 10 Mbps is provided dynamically from a RADIUS authentication server when the subscriber logs in.
- The transmit connect speed calculated by QoS is 5 Mbps.

Based on these characteristics, [Table 25](#) lists the transmit connect speed value reported in L2TP Transmit (TX) Speed AVP 24 for each calculation method, and the reason why L2TP reports this value.

Table 25: Transmit Connect Speeds for L2TP over ATM 1483 Example

Calculation Method	Transmit Connect Speed Reported in AVP 24	Reason
Static layer 2	155 Mbps	L2TP reports the speed of the underlying OC3 physical port because there is no explicit static configuration for the layer 2 interface.
Dynamic layer 2	10 Mbps	L2TP reports the transmit connect speed provided by RADIUS.
QoS	5 Mbps	L2TP reports the transmit connect speed calculated by QoS.
Actual	5 Mbps	L2TP reports the lesser of the dynamic layer 2 speed (10 Mbps) or the QoS speed (5 Mbps).

Example 2: L2TP Session over Ethernet VLAN Interface

In this example, an L2TP session is established over a PPPoE subinterface over an Ethernet VLAN subinterface. The configuration has the following characteristics:

- The Ethernet VLAN subinterface is configured with an advisory transmit speed of 100 Mbps.
- The dynamic layer 2 setting does not apply to the VLAN subinterface.
- The transmit connect speed calculated by QoS is 10 Mbps.

Based on these characteristics, [Table 26](#) lists the transmit connect speed value reported in L2TP Transmit (TX) Speed AVP 24 for each calculation method, and the reason why L2TP reports this value.

Table 26: Transmit Connect Speeds for L2TP over Ethernet Example

Calculation Method	Transmit Connect Speed Reported in AVP 24	Reason
Static layer 2	100 Mbps	L2TP reports the advisory transmit speed configured on the VLAN subinterface. If configured, the advisory transmit speed takes precedence over the physical port speed for a VLAN subinterface.
Dynamic layer 2	100 Mbps	L2TP reports the static layer 2 value because the dynamic layer 2 setting does not apply to a VLAN subinterface.
QoS	10 Mbps	L2TP reports the transmit connect speed calculated by QoS.
Actual	10 Mbps	L2TP reports the lesser of the dynamic layer 2 speed (100 Mbps) or the QoS speed (10 Mbps).

Transmit Connect Speed Reporting Considerations

The following considerations affect the transmit connect speed value reported in L2TP Transmit (TX) Speed AVP 24 when you use this feature.

Session Termination for Dynamic Speed Timeout

Under certain heavy load conditions, the router might be unable to obtain the dynamic-layer2 value for the transmit connect speed of the subscriber's access interface. In this situation, the LAC sends the LNS an L2TP Call-Disconnect-Notify (CDN) message to terminate the L2TP session.

For more information about supported L2TP terminate reasons, see *Appendix C, Application Terminate Reasons*.

Advisory Speed Precedence for VLANs over Bridged Ethernet

For interface columns that consist of an L2TP session over an Ethernet VLAN subinterface over a bridged Ethernet interface, the advisory transmit speed of the VLAN subinterface, if configured with the **vlan advisory-tx-speed** command, takes precedence over the physical port speed of the underlying layer 2 ATM 1483 interface. As a result, if the advisory transmit speed is configured for the VLAN subinterface, L2TP reports this value as the transmit connect speed regardless of the port speed of the ATM 1483 interface.

Using AAA Domain Maps to Configure the Transmit Connect Speed Calculation Method

To configure the transmit connect speed calculation method for a tunneled L2TP session associated with an AAA domain map:

1. Access Domain Map Tunnel Configuration mode.

```
host1(config)#aaa domain-map sunnyvale.com
host1(config-domain-map)#router-name lac
host1(config-domain-map)#tunnel 5
host1(config-domain-map-tunnel)#
```

For more information about how to map a domain to an L2TP tunnel from Domain Map Tunnel Configuration mode, see [Mapping a User Domain Name to an L2TP Tunnel](#) on page 224.

2. From Domain Map Tunnel Configuration mode, configure the calculation method for the transmit connect speed of the subscriber's access interface.

```
host1(config-domain-map-tunnel)#tx-connect-speed-method dynamic-layer2
```

3. (Optional) Use the **show aaa domain-map** command to verify configuration of the transmit connect speed calculation method.

```
host1(config-domain-map-tunnel)#run show aaa domain-map
```

```
Domain: sunnyvale.com; router-name: lac; ipv6-router-name: default
```

Tunnel Tag	Tunnel Peer	Tunnel Source	Tunnel Type	Tunnel Medium	Tunnel Password	Tunnel Id	Tunnel Client Name
5	<null>	<null>	l2tp	ipv4	<null>	<null>	<null>
Tunnel Tag	Server Name	Tunnel Preference		Tunnel Max Sessions	Tunnel RWS	Tunnel Virtual Router	
5	<null>	2000		0	system chooses	<null>	
Tunnel Tag	Failover Resync	Tunnel Switch Profile		Tunnel Tx Speed Method			
5	<null>	<null>		dynamic layer2			

tx-connect-speed-method

- Use from Domain Map Tunnel Configuration mode to configure the method that the router uses for calculating the transmit connect speed of the subscriber's access interface for a tunneled L2TP session associated with an AAA domain map.
- L2TP reports the transmit connect speed in L2TP Transmit (TX) Speed AVP 24.
- You must specify the calculation method for the transmit connect speed in one of the following ways:
 - For calculation based on statically configured settings for the underlying layer 2 interface, use the **static-layer2** keyword.
 - For calculation based on dynamically configured settings for the underlying layer 2 interface, use the **dynamic-layer2** keyword.
 - For calculation based on settings determined by QoS, use the **qos** keyword.
 - For calculation as the lesser of the **dynamic-layer2** value or the **qos** value, use the **actual** keyword.
- Example


```
host1(config-domain-map-tunnel)#tx-connect-speed-method qos
```
- Use the **no** version to remove configuration of the transmit connect speed calculation method from the AAA domain map.

Using AAA Tunnel Groups to Configure the Transmit Connect Speed Calculation Method

To configure the transmit connect speed calculation method for a tunneled L2TP session associated with an AAA tunnel group:

1. Access Tunnel Group Tunnel Configuration mode.

```
host1(config)#aaa tunnel-group boston
host1(config-tunnel-group)#tunnel 3
host1(config-tunnel-group-tunnel)#
```

For more information about how to map a domain to an L2TP tunnel from Tunnel Group Tunnel Configuration mode, see [Mapping a User Domain Name to an L2TP Tunnel](#) on page 224.

2. From Tunnel Group Tunnel Configuration mode, configure the calculation method for the transmit connect speed of the subscriber's access interface.

```
host1(config-tunnel-group-tunnel)#tx-connect-speed-method qos
```

3. (Optional) Use the **show aaa tunnel-group** command to verify configuration of the transmit connect speed calculation method.

```
host1(config-tunnel-group-tunnel)#run show aaa tunnel-group
```

```
Tunnel Group: boston
```

Tunnel Tag	Tunnel Peer	Tunnel Source	Tunnel Type	Tunnel Medium	Tunnel Password	Tunnel Id	Tunnel Client Name
3	<null>	<null>	l2tp	ipv4	<null>	<null>	<null>
Tunnel Tag	Tunnel Server Name	Tunnel Preference	Tunnel Max Sessions	Tunnel RWS		Tunnel Virtual Router	
3	<null>	2000	0	system chooses		<null>	
Tunnel Tag	Tunnel Failover Resync	Tunnel Switch Profile	Tunnel Tx Speed Method				
3	<null>	<null>	qos				

tx-connect-speed-method

- Use from Tunnel Group Tunnel Configuration mode to configure the method that the router uses for calculating the transmit connect speed of the subscriber's access interface for a tunneled L2TP session associated with an AAA tunnel group.
- For detailed information about how to use this command, see [tx-connect-speed-method](#) on page 275.
- Example

```
host1(config-tunnel-group-tunnel)#tx-connect-speed-method actual
```

- Use the **no** version to remove configuration of the transmit connect speed calculation method from the AAA tunnel group.

Using RADIUS to Configure the Transmit Connect Speed Calculation Method

On the LAC, the router can receive tunnel configuration attributes through a RADIUS authentication server. To use RADIUS to configure the transmit connect speed calculation method for a subscriber's access interface, you can configure RADIUS to include the Tunnel-Tx-Speed-Method RADIUS attribute (Juniper Networks VSA 26-94) in RADIUS Access-Accept messages.

Table 27 describes the Tunnel-Tx-Speed-Method RADIUS attribute. For more information about RADIUS Access-Accept messages, see [Chapter 2, Configuring RADIUS Attributes](#). For a description of the RADIUS attributes supported by JUNOS software, see [Appendix A, RADIUS Attribute Descriptions](#).

Table 27: Tunnel-Tx-Speed-Method RADIUS Attribute

Attribute Number	Attribute Name	Description	Length	Subtype Length	Value
[26-94]	Tunnel-Tx-Speed-Method	The method that the router uses to calculate the transmit connect speed of the subscriber's access interface	12	6	integer: <ul style="list-style-type: none"> ■ 1 = static-layer2; TX speed based on static layer 2 settings ■ 2 = dynamic-layer2; TX speed based on dynamic layer 2 settings ■ 3 = qos; TX speed based on QoS settings ■ 4 = actual; TX speed that is the lesser of the dynamic-layer2 value or the qos value

Using AAA Default Tunnel Parameters to Configure the Transmit Connect Speed Calculation Method

You can configure the transmit connect speed calculation method as a default AAA tunnel parameter by using the **aaa tunnel tx-connect-speed-method** command from Global Configuration mode. This command applies the specified calculation method to all tunneled L2TP sessions associated with a particular virtual router, and thereby alleviates the need for you to configure the transmit connect speed calculation method for each individual subscriber.

Configuring the calculation method as a default AAA tunnel parameter for a virtual router has lower precedence than using AAA domain maps, AAA tunnel groups, or RADIUS to configure the transmit connect speed calculation method. The router uses the calculation method specified with the **aaa tunnel tx-connect-speed-method** command if the tunnel attributes returned from an AAA domain map, an AAA tunnel group, or a RADIUS authentication server do not include the transmit connect speed calculation method.

To configure the transmit connect speed calculation method for all tunneled L2TP sessions associated with a particular virtual router:

1. Create the virtual router for which you want to configure the transmit connect speed calculation method.

```
host1(config)#virtual-router north
```

For more information about configuring and using virtual routers, see [JUNOS System Basics Configuration Guide, Chapter 12, Configuring Virtual Routers](#).

2. Configure the transmit connect speed calculation method in the context of this virtual router.

```
host1:north(config)#aaa tunnel tx-connect-speed-method qos
```

3. (Optional) Use the **show aaa tunnel-parameters** command to verify configuration of the transmit connect speed calculation method.

```
host1:north(config)#run show aaa tunnel-parameters
Tunnel password is <NULL>
Tunnel client-name is <NULL>
Tunnel nas-port-method is none
Tunnel switch-profile is boston
Tunnel tx-connect-speed-method is qos
Tunnel nas-port ignore disabled
Tunnel nas-port-type ignore disabled
Tunnel assignmentId format is assignmentId
Tunnel calling number format is fixed
```

aaa tunnel tx-connect-speed-method

- Use to configure the method that the router uses for calculating the transmit connect speed of the subscriber's access interface as a default AAA tunnel parameter for tunneled L2TP sessions associated with a particular virtual router.
- L2TP reports the transmit connect speed in L2TP Transmit (TX) Speed AVP 24.
- The router uses the calculation method specified with the **aaa tunnel tx-connect-speed-method** command if the tunnel attributes returned from an AAA domain map, an AAA tunnel group, or a RADIUS authentication server do not include the transmit connect speed calculation method.
- To specify the calculation method for the transmit connect speed, use one of the following keywords, as described in [tx-connect-speed-method](#) on page 275:
 - **static-layer2**
 - **dynamic-layer2**
 - **qos**
 - **actual**
- Example


```
host1:south(config)#aaa tunnel tx-connect-speed-method dynamic-layer2
```
- Use the **no** version to remove configuration of the transmit connect speed calculation method from the tunneled L2TP sessions associated with this virtual router.

PPP Accounting Statistics

JUNOS accounting for tunneled subscribers at the L2TP LAC counts the payload that PPP passes to or receives from L2TP for transport. At this stage in the protocol processing, any padding outside PPP, such as that for PPPoE, has been removed. Accounting includes the authentication acknowledgement packet, CHAP success packets, and PAP acknowledgment packets. Accounting ends when L2TP has been notified to terminate the session. The statistics are reported in the following RADIUS attributes:

Attribute Number	Attribute Name
42	Acct-Input-Octets
43	Acct-Output-Octets
47	Acct-Input-Packets
48	Acct-Output-Packets

Termination of a tunneled session can result from PPP termination, L2TP shutdown, subscriber logout, or lower layer down events. When the session is terminated through PPP, the software counts both the PPP terminate-request and the PPP terminate-acknowledgement packets.

- Accounting statistics reported in RADIUS octet counts (Acct-Input-Octets and Acct-Output-Octets) for tunneled PPP customers at the L2TP LAC include the following data:
 - All upper layer control traffic, including IPCP, IPCPv6, OSICP, and MPLSNCP
 - All data traffic, including IP, IPv6, MPLS, and OSI
 - PPP PAP or CHAP acknowledgments, and also retransmission of PAP or CHAP that take place after the session is active (even when proxy authentication is accepted)
 - All PPP PAP or CHAP negotiations in the case where proxy authentication is disabled or required to renegotiate at the LNS
 - All LCP traffic when proxy LCP is disabled or required to renegotiate at the LNS
 - All PPP LCP echo requests and their responses
 - PPP LCP terminate-request or terminate-acknowledgement packets from the client or LNS when PPP initiates termination of the session
 - If present, the two PPP header bytes (Address Field 0xFF and Control Field 0x03) as part of the L2TP payload

- Accounting statistics reported in RADIUS octet counts (Acct-Input-Octets and Acct-Output-Octets) for tunneled PPP customers at the L2TP LAC exclude the following data:
 - LCP when Proxy LCP is enabled and accepted at the LNS
 - Initial PPP PAP request
 - Initial PPP CHAP challenge and response
- Accounting statistics reported in RADIUS packet counts (Acct-Input-Packets and Acct-Output-Packets) for tunneled PPP customers at the L2TP LAC are based on packets delivered to or received from the L2TP session. These statistics exclude L2TP control traffic and L2TP hello messages.

For information on accounting statistics for terminated PPP sessions, see [PPP Accounting Statistics](#) in *JUNOS Link Layer Configuration Guide, Chapter 4, Configuring Point-to-Point Protocol*.

Monitoring L2TP

When you have configured L2TP on your E-series router, you can monitor the active tunnels and sessions.



NOTE: All of the commands in this section apply to both the LAC and the LNS.

show aaa domain-map

- Use to display the mapping between user domains and virtual routers.
- Field descriptions—The actual fields displayed depend on your configuration. See [show aaa domain-map](#) on page 90 for information about the field descriptions for this command.
- Example

```
host1#show aaa domain-map
```

```
Domain: lac-tunnel; router-name: lac; ipv6-router-name: default
```

Tunnel Tag	Tunnel Peer	Tunnel Source	Tunnel Type	Tunnel Medium	Tunnel Password	Tunnel Id
5	192.168.1.1	<null>	l2tp	ipv4	welcome	lac-tunnel

Tunnel Tag	Tunnel Client Name	Tunnel Server Name	Tunnel Preference	Tunnel Max Sessions	Tunnel RWS
5	lac	boston	5	0	4

Tunnel Tag	Tunnel Virtual Router	Tunnel Failover Resync	Tunnel Switch Profile	Tunnel Tx Speed Method
5	<null>	<null>	denver	qos

show aaa tunnel-group

- Use to display the currently configured tunnel groups.
- Field descriptions—The information displayed is almost identical to the tunnel information displayed using the **show aaa domain-map** command. See [show aaa domain-map](#) on page 90 for information about the field descriptions for this command.
- Example

```
host1#show aaa tunnel-group
```

```
Tunnel Group: boston
```

Tunnel Tag	Tunnel Peer	Tunnel Source	Tunnel Type	Tunnel Medium	Tunnel Password	Tunnel Id
3	192.168.1.1	<null>	l2tp	ipv4	msn	<null>

Tunnel Tag	Tunnel Client Name	Tunnel Server Name	Tunnel Preference	Tunnel Max Sessions	Tunnel RWS
3	msn.del.com	<null>	2000	0	4

Tunnel Tag	Tunnel Virtual Router	Tunnel Failover Resync	Tunnel Switch Profile	Tunnel Tx Speed Method
3	<null>	<null>	sanjose	qos

show aaa tunnel-parameters

- Use to display the configuration of tunnel parameters used for tunnel definitions.
- Field descriptions
 - Tunnel password—Default tunnel password
 - Tunnel client-name—Hostname that the LAC sends to the LNS when communicating about the tunnel
 - Tunnel nas-port-method—Default NAS port type
 - Tunnel switch profile is—Name of the default L2TP tunnel switch profile
 - Tunnel tx-connect-speed-method is—Method that the router uses to calculate the transmit connect speed of the subscriber's access interface: static layer2, dynamic layer2, qos, actual, not set
 - Tunnel nas-port ignore—Whether the router uses the tunnel peer's NAS-Port [5] attribute; enabled or disabled
 - Tunnel nas-port-type ignore—Whether the router uses the tunnel peer's NAS-Port-Type [61] attribute; enabled or disabled
 - Tunnel assignmentId format—Value of the tunnel assignment ID that is passed to PPP/L2TP

- Tunnel calling number format—Format configured for L2TP Calling Number AVP 22 generated by the LAC
- Tunnel calling number format fallback—Fallback format configured for L2TP Calling Number AVP 22 generated by the LAC
- Example

```
host1#show aaa tunnel-parameters
Tunnel password is 3&92k%b#q4
Tunnel client-name is <NULL>
Tunnel nas-port-method is none
Tunnel switch profile is boston
Tunnel tx-connect-speed-method is qos
Tunnel nas-port ignore disabled
Tunnel nas-port-type ignore disabled
Tunnel assignmentId format is assignmentId
Tunnel calling number format is descriptive
Tunnel calling number format fallback is fixed
```

show l2tp

- Use to display the global configuration and status for L2TP on E-series routers, including switched sessions.
- Field descriptions
 - Configuration:
 - L2TP administrative state—Status of L2TP on the router; enabled or disabled
 - Dynamic interface destruct timeout—Number of seconds that the router maintains dynamic destinations, tunnels, and sessions after they have terminated
 - Data packet checksums—Status of checking data integrity via UDP; enabled or disabled
 - Receive data sequencing—Whether the router processes or ignores sequence numbers in incoming data packets
 - Tunnel switching—Enabled or disabled
 - Retransmission retries for established tunnels—Number of retries configured for established tunnels
 - Retransmission retries for not-established tunnels—Number of retries configured for tunnels not established
 - Tunnel idle timeout—Length of the tunnel idle timeout, in seconds
 - Failover within a preference level—Enabled or disabled
 - Weighted load balancing—Enabled or disabled
 - Tunnel authentication challenge—Enabled or disabled
 - Calling number avp—Whether the E-series LAC sends Calling-Station-Id and Called-Station-Id AVPs in ICRQ packets, enabled or disabled
 - Reject remote transmit address change—Enabled or disabled for IP address, UDP port, or both

- ❑ Ignore remote transmit address change—Enabled or disabled for IP address, UDP port, or both
- ❑ Disconnect-cause avp generation—Enabled or disabled
- ❑ Default receive window size—Default L2TP RWS for a tunnel on both the LAC and the LNS; displays either the configured value or the default behavior, indicated by `system chooses`
- ❑ Rx speed avp when equal—Enabled or disabled
- ❑ Destination lockout timeout—Number of seconds that L2TP destinations remain in the lockout state after they become unavailable
- ❑ Destination lockout test—Status of the L2TP destination lockout test, enabled or disabled
- ❑ Failover resync—Global L2TP peer resynchronization configuration
- Sub-interfaces:
 - ❑ total—Number of destinations, tunnels, and sessions that the router created
 - ❑ active—Number of operational destinations, tunnels, and sessions
 - ❑ failed—Number of requests that did not reach an operational state
 - ❑ auth-errors—Number of requests that failed because the tunnel password was invalid

■ Example

host1#**show l2tp**

Configuration

```
L2TP administrative state is enabled
Dynamic interface destruct timeout is 600 seconds
Data packet checksums are disabled
Receive data sequencing is not ignored
Tunnel switching is disabled
Retransmission retries for established tunnels is 5
Retransmission retries for not-established tunnels is 5
Tunnel idle timeout is 60 seconds
Failover within a preference level is disabled
Weighted load balancing is disabled
Tunnel authentication challenge is enabled
Calling number avp is enabled
Reject remote transmit address change is enabled for ip address
Ignore remote transmit address change is disabled
Disconnect-cause avp generation is enabled
Default receive window size is system chooses
Rx speed avp when equal is enabled
Destination lockout timeout is 300 seconds
Destination lockout test is disabled
Failover resync is silent-failover
```

Sub-interfaces	total	active	failed	auth-errors
Destinations	0	0	0	n/a
Tunnels	0	0	0	0
Sessions	0	0	0	n/a
Switched-sessions	0	0	0	n/a

show l2tp destination

- Use to display detailed configuration information about specified destinations.
- Field descriptions
 - Configuration:
 - Administrative state—Configured status of the destination:
enabled—No restrictions on creation and operation of sessions and tunnels for this destination
disabled—Router disabled existing sessions and tunnels and will not create new sessions or tunnels for this destination
drain—Router will not create new sessions or tunnels for this destination
 - SNMP traps—Whether or not the router sends traps to SNMP for operational state changes
 - Destination address:
 - Transport—Method used to transfer traffic
 - Virtual router—Name of the virtual router on which the tunnel is configured
 - Local and peer addresses—Addresses of the local and remote interfaces
 - Destination status:
 - Effective administrative state—The more restrictive of the router and destination administrative states. This setting, rather than the administrative state of the destination, determines whether the router can create new sessions or tunnels and whether the sessions or tunnels are disabled for this destination.
 - Sub-interfaces:
 - total—Number of sessions or tunnels that the router created for this destination
 - active—Number of operational sessions or tunnels for this destination
 - failed—Number of requests that did not reach an operational state for this destination
 - auth-errors—Number of requests that failed because the tunnel password was invalid for this destination
 - Statistics—Information about the traffic sent and received

■ Example 1

```
host1#show l2tp destination ip 172.31.1.98
L2TP destination 1 is Up with 5 active tunnels and 64 active sessions
```

■ Example 2

```
host1#show l2tp destination detail 1
L2TP destination 1 is Up with 5 active tunnels and 64 active sessions
Configuration
  Administrative state is enabled
  SNMP traps are enabled
Destination address
  Transport ipUdp
  Virtual router default
```

```

Local address 192.168.1.230, peer address 172.31.1.98
Destination status
Effective administrative state is enabled
Sub-interfaces total active failed auth-errors
Tunnels      5      5      0      0
Sessions     64     64      0     n/a
Statistics   packets  octets  discards  errors
Control rx   69      3251    2         0
Control tx   195     23939  0         0
Data rx      68383456 68383456 0         0
Data tx      68383456 68383456 0         0

```

show l2tp destination lockout

- Use to display information about the L2TP destinations that are currently locked out.
- Field descriptions
 - L2TP destination waiting—Name of destination and its lockout status. The status indicates whether the destination is waiting for the lockout timeout to expire (and how much time is left), or waiting for the lockout test to start or finish
 - L2TP lockout destinations found—Number of destinations that are currently in lockout state
- Example

```

host1#show l2tp destination lockout
L2TP destination 36 is waiting for lockout timeout (45 seconds remaining)
L2TP destination 54 is waiting for lockout test start
L2TP destination 76 is waiting for lockout test complete
3 L2TP lockout destinations found

```

show l2tp destination profile

- Use to display either a list of configured L2TP destination profiles or the host profiles defined in a particular profile.
- If a nondefault L2TP RWS is configured for a particular host profile, the command displays the RWS setting as an attribute of that host profile. (See Example 2.)
- Field descriptions
 - Destination profile attributes:
 - Transport—Method used to transfer traffic
 - Virtual router—Name of the virtual router
 - Peer address—IP address of the LAC
 - Destination profile maximum sessions—Maximum number of sessions allowed for the destination profile
 - Destination profile current session count—Number of current sessions for the destination profile
 - Host profile attributes:
 - Remote host—Name of the remote host
 - Local hostname—Name of the local host

- ❑ Local IP address—IP address of the local host
- ❑ Bundled group id—Identifier for bundled sessions
- ❑ Tunnel password—Password for the tunnel
- ❑ Interface profile—Name of the host profile
- ❑ Proxy lcp—Status of proxy LCP for the remote host
- ❑ Proxy authenticate—Status of proxy authentication for the remote host
- ❑ mlppp upper binding type—Default upper binding type
- ❑ Disconnect-cause avp generation—Status of the disconnect cause generation
- ❑ Receive window size—Number of packets that the peer can transmit without receiving an acknowledgment from the router
- ❑ Maximum sessions—Maximum number of sessions allowed for the host profile
- ❑ Failover resync—L2TP peer resynchronization method for the host profile
- ❑ Current session count—Number of current sessions for the host profile

■ Example 1

```
host1#show l2tp destination profile
L2TP destination profile westford
1 L2TP destination type profile found
```

■ Example 2

```
host1#show l2tp destination profile westford
L2TP destination profile westford
Configuration
  Destination address
    Transport ipUdp
    Virtual router lns
    Peer address 192.168.1.99
  Destination profile maximum sessions is 5000
Statistics
  Destination profile current session count is 2
Host profile attributes
  Remote host is remhost22.xyz.com
  Configuration
    Tunnel password is 23erf5
    Interface profile is ebcints
    Bundled group id is 1
    Bundled group id override is enabled
    Maximum sessions is 400
    Failover resync is failover-protocol
  Statistics
    Current session count is 14
  Remote host is asciitext
  Configuration
    Bundled group id is 0
    Tunnel password is 222
    Interface profile is ascints
    Default upper binding type mlppp
    Maximum sessions is 250
    Failover resync is failover-protocol
```

```

Statistics
  Current session count is 2
Remote host is mexico
Configuration
  Local ip address is 10.10.2.2
  Proxy lcp is disabled
  Proxy authenticate is enabled
  mlppp upper binding type
  Disconnect-cause avp is enabled
  Receive window size is 4
  Maximum sessions is 500
  Failover resync is failover-protocol
Statistics
  Current session count is 14
4 L2TP host profiles found

```

show l2tp destination summary

- Use to display a summary of the configured and operational status of all L2TP destinations.
- Field descriptions
 - Administrative status:
 - enabled—No restrictions on creation and operation of sessions and tunnels for this destination
 - drain—Router will not create new sessions or tunnels for this destination
 - disabled—Router disabled existing sessions and tunnels and will not create new sessions or tunnels for this destination
 - Operational status:
 - up—Destination is available for tunnels
 - down—Destination is not available for tunnels
 - lower-down—Underlying transport is unavailable; for example, you removed the virtual router
 - not-present—Hardware supporting the destination is unavailable; for example, you removed a required line module
- Example

```

host1#show l2tp destination summary
Administrative status  enabled    drain      disabled
                      0          0          0
Operational status    up         down       lower-down not-present
                      0          0          0          0

```

show l2tp received-disconnect-cause-summary

- Use to display statistics for all information the LAC receives from an LNS about the cause of an L2TP session disconnection.

- Example

```
host1#show l2tp received-disconnect-cause-summary
```

Disconnect Cause (Code)	Global	Peer	Local
no info (0)	0	0	0
admin disconnect (1)	0	0	0
renegotiation disabled (2)	0	0	0
normal disconnect (3)	0	0	0
compulsory encryption refused (4)	0	0	0
lcp failed to converge (5)	0	0	0
lcp peer silent (6)	0	0	0
lcp magic number error (7)	0	0	0
lcp keepalive failure (8)	0	0	0
lcp mlppp endpoint discriminator mismatch (9)	0	0	0
lcp mlppp peer mrru not valid (10)	0	0	0
lcp mlppp peer ssn invalid (11)	0	0	0
lcp callback refused (12)	0	0	0
authenticate timed out (13)	0	0	0
authenticate mlppp name mismatch (14)	0	0	0
authenticate protocol refused (15)	0	0	0
authenticate failure (16)	0	0	0
ncp no negotiation completed (17)	0	0	0
ncp no ncps available (18)	0	0	0
ncp addresses failed to converge (19)	0	0	0
ncp negotiation inhibited (20)	0	0	0

show l2tp session

- Use to display detailed configuration information about specified sessions.
- Field descriptions
 - Configuration:
 - Administrative state—Configured status of the session
enabled—No restrictions on the operation of this session
disabled—Router terminated this session
 - SNMP traps—Whether or not the router sends traps to Simple Network Management Protocol (SNMP) for operational state changes
 - Session status:
 - Effective administrative state—Most restrictive of the following administrative states: router, destination, tunnel, and session. This setting, rather than the administrative state of the session, determines whether the router can maintain this session or not.
 - State—Status of the session: idle, connecting, established, or disconnecting
 - Local and peer session id—Names the router uses to identify the session locally and remotely
 - Statistics—Information about the traffic for this session
 - Session operational configuration—Information received from the peer when the session was created

- Example 1

```
host1#show l2tp session
L2TP session 1/1/1 is Up
1 L2TP session found
```

- Example 2

```
host1#show l2tp session detail
L2TP session 1/1/1 is Up
Configuration
  Administrative state is enabled
  SNMP traps are enabled
Session status
  Effective administrative state is enabled
  State is established
  Local session id is 25959, peer session id is 2
Statistics packets octets discards errors
Data rx  7      237    1      0
Data tx  6      160    0      0

Session operational configuration
  User name is 't1.s1@local'
  Tunneling PPP interface atm 0/0.1
  Call type is lacIncoming
  Call serial number is 0
  Bearer type is none
  Framing type is none
  Proxy LCP was provided
  Authentication method was chap
  Tunnel switch profile is chicago
```

show l2tp session summary

- Use to display a summary of the configured and operational status of all L2TP sessions.
- Field descriptions
 - Administrative status:
 - enabled—No restrictions on the creation of sessions
 - disabled—Router disabled these sessions
 - Operational status:
 - up—Session is available
 - down—Session is unavailable
 - lower-down—Session is unavailable because the tunnel supporting it is inaccessible
 - not-present—Session is unavailable because the hardware (such as a line module) supporting it is inaccessible
- Example

```
host1#show l2tp session summary
Administrative status  enabled    disabled
                      64         0
Operational status   up        down    lower-down  not-present
                      64         0         0         0
```

show l2tp switch-profile

- Use to display information about the L2TP switch profiles configured on the router.
- To display only the names of all L2TP tunnel switch profiles configured on the router, issue the command without specifying a profile name.
- To display information about the settings in a particular L2TP tunnel switch profile, issue the command with a profile name.
- Field descriptions
 - L2TP tunnel switch profile—Name of the L2TP tunnel switch profile
 - AVP *actionType* action is—Indicates the tunnel switching behavior or action type (for example, relay) configured for the specified L2TP AVP type
- Example 1—Displays the names of the L2TP tunnel switch profiles configured on the router

```
host1#show l2tp switch-profile
L2TP tunnel switch profile concord
L2TP tunnel switch profile myProfile
2 L2TP tunnel switch profiles found
```

- Example 2—Displays the tunnel switching behavior configured in the specified L2TP tunnel switch profile

```
host1#show l2tp switch-profile concord
L2TP tunnel switch profile concord
  AVP bearer type action is relay
  AVP calling number action is relay
  AVP Cisco nas port info action is relay
```

show l2tp tunnel

- Use to display detailed configuration information about specified tunnels.
- Field descriptions
 - Configuration:
 - Administrative state—Configured status of the tunnel
 - enabled—No restrictions on creation and operation of sessions for this tunnel
 - disabled—Router disabled existing sessions and will not create new sessions on this tunnel
 - drain—Router will not create new sessions on this tunnel
 - SNMP traps—Whether or not the router sends traps to SNMP for operational state changes
 - Tunnel address:
 - Transport—Method used to transfer traffic
 - Virtual router—Name of the virtual router on which the tunnel is configured
 - Local and peer addresses—IP addresses of the local and remote ends of the tunnel. If the router is set up to ignore address and port changes in SCCRP packets, both the transmit and receive addresses are listed for the peer.

- ❑ Local and peer UDP ports—UDP ports for the local and remote ends of the tunnel. If the router is set up to accept address and port changes in SCCRP packets, both the transmit and receive UDP ports are listed for the peer.
- Tunnel status:
 - ❑ Effective administrative state—Most restrictive of the following administrative states: E-series router, destination, and tunnel. This setting, rather than the administrative state of the tunnel, determines whether the router can create new sessions on a tunnel or whether the sessions on a tunnel are disabled or not.
 - ❑ State—Status of the tunnel: idle, connecting, established, or disconnecting
 - ❑ Local and peer tunnel id—Names the router used to identify the tunnel locally and remotely
- Sub-interfaces:
 - ❑ total—Number of sessions that the router has created on this tunnel
 - ❑ active—Number of operational sessions on the tunnel
 - ❑ failed—Number of requests that did not reach an operational state
- Statistics—Information about the traffic sent and received
- Control channel statistics:
 - ❑ Receive window size—Number of packets that the peer can transmit without receiving an acknowledgment from the router
 - ❑ Receive ZLB—Number of acknowledgments that the router has received from the peer
 - ❑ Receive out-of-sequence—Number of received control packets that were out of order
 - ❑ Receive out-of-window—Number of packets that arrived at the router outside the receiving window
 - ❑ Transmit window size—Number of packets that the router can transmit before receiving an acknowledgment from the peer
 - ❑ Transmit ZLB—Number of acknowledgments that the router has sent to the peer
 - ❑ Transmit queue depth—Number of packets that the router is waiting to send to the peer, plus the number of packets for which the peer has not yet acknowledged receipt
- Tunnel operation configuration—Information received from the peer when the tunnel was created
- Example 1


```
host1#show l2tp tunnel virtual router default ip 172.31.1.98
L2TP tunnel 1/xyz is Up with 13 active sessions
L2TP tunnel 1/aol.com is Up with 13 active sessions
L2TP tunnel 1/isp.com is Up with 13 active sessions
L2TP tunnel 1/msn.com is Up with 13 active sessions
L2TP tunnel 1/mv.com is Up with 12 active sessions
5 L2TP tunnels found
```

■ Example 2

```

host1#show l2tp tunnel detail 1/xyz
L2TP tunnel 1/xyz is Up with 13 active sessions
Configuration
  Administrative state is enabled
  SNMP traps are enabled
Tunnel address
  Transport ipUdp
  Virtual router default
  Local address 192.168.1.230, peer address 172.31.1.98
  Local UDP port 1701, peer UDP port: 1701
Tunnel status
  Effective administrative state is enabled
  State is established
  Local tunnel id is 14529, peer tunnel id is 34
Sub-interfaces      total    active    failed
Sessions            13      13        0
Statistics  packets      octets      discards    errors
Control rx   14          683          0          0
Control tx   41         4666          0          0
Data rx      67900944    67900944      0          0
Data tx      67900944    67900944      0          0
Control channel statistics
  Receive window size = 4
  Receive ZLB = 17
  Receive out-of-sequence = 0
  Receive out-of-window = 0
  Transmit window size = 4
  Transmit ZLB = 12
  Transmit queue depth = 0
  Retransmissions = 8
Tunnel operational configuration
  Peer host name is 'Juniper-POS'
  Peer vendor name is 'XYZ, Inc.'
  Peer protocol version is 1.1
  Peer firmware revision is 0x1120
  Peer bearer capabilities are digital and analog
  Peer framing capabilities are sync and async

```

show l2tp tunnel summary

- Use to display a summary of the configured and operational status of all L2TP tunnels.
- Field descriptions
 - Administrative status:
 - enabled—No restrictions on the creation and operation of sessions for this tunnel
 - drain—Router will not create new sessions for this tunnel
 - disabled—Router disabled existing sessions and will not create new sessions for this tunnel
 - Operational status:
 - up—Tunnel is available
 - down—Tunnel is unavailable
 - lower-down—Tunnel is unavailable because the destination supporting it is inaccessible
 - not-present—Tunnel is unavailable because the hardware (such as a line module) supporting the tunnel is inaccessible
- Example

```

host1#show l2tp tunnel summary
Administrative status  enabled  drain  disabled
                    5          0      0
Operational status    up      down  lower-down  not-present
                    5          0      0          0
  
```


Chapter 7

Configuring L2TP Dial-Out

This chapter describes the Layer 2 Tunneling Protocol (L2TP) dial-out feature on your E-series router. This chapter includes the following sections:

- [Overview](#) on page 295
- [Platform Considerations](#) on page 302
- [References](#) on page 302
- [Before You Configure L2TP Dial-Out](#) on page 303
- [Configuring L2TP Dial-Out](#) on page 303
- [Monitoring L2TP Dial-Out](#) on page 305

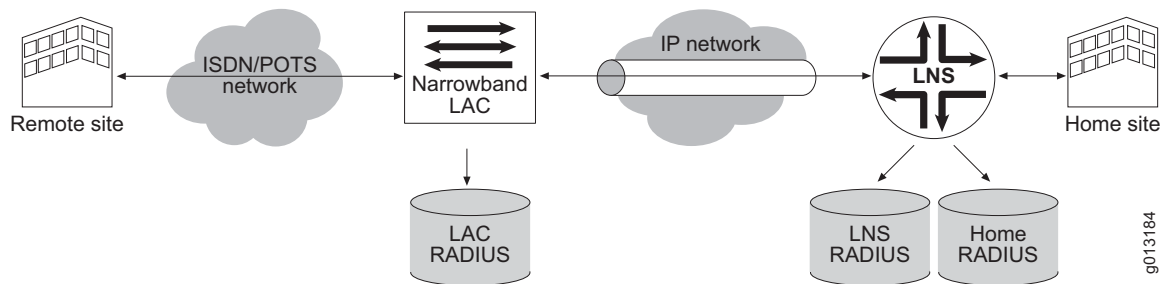
Overview

L2TP dial-out provides a way for corporate virtual private networks (VPNs) that use Broadband Remote Access Server (B-RAS) to dial out to remote offices that have only narrowband dial-up access. The L2TP network server (LNS) function is deployed in networks that have a combination of broadband and narrowband access.

A remote site can communicate on demand with the home site with a normal L2TP access concentrator (LAC) to LNS session. When the communication finishes, the remote site terminates the session. However, if the home site wishes to communicate with the remote site and no incoming call is currently established, the home site needs a method to dial out to the remote site. This method is L2TP dial-out, which uses the L2TP outgoing call support defined in [RFC 2661—Layer Two Tunneling Protocol “L2TP” \(August 1999\)](#).

Figure 10 shows the dial-out model in which the LNS initiates L2TP sessions and provides enough information to the narrowband LAC so that it can complete the dial-out from the home site to the remote site.

Figure 10: Network Model for Dial-Out



NOTE: The dial-out feature exists in the LNS only. It does not exist in the LAC.

Terms

Table 28 describes key terms used in L2TP dial-out.

Table 28: L2TP Dial-Out Terms

Term	Description
Dial-out trigger	IP packet that initiates a dial-out session
Dial-out session	Control entity for a triggered IP flow used to manage the establishment of an associated L2TP session for dial-out
Dial-out target	A virtual router context and an IP address prefix, for which the arrival of an IP packet (a dial-out trigger) initiates a dial-out session.
Dial-out route	Contains the dial-out target, as well as a domain name and profile. <ul style="list-style-type: none"> ■ The domain name is used in the initial Access-Request message. ■ The profile is used to create the IP/Point-to-Point Protocol (PPP) stack for the dial-out session.

Network Model for Dial-Out

In Figure 10, the home site connects to the Internet over a permanent leased line to the Internet service provider's (ISP's) E-series LNS. The ISP uses an IP network to connect the LNS to the narrowband access point of the network where the narrowband LAC exists. The narrowband LAC connects to a narrowband network (ISDN) that the remote site is also connected to.

The figure shows three RADIUS servers. The home site maintains the home server, and the other two servers are at the LNS and the LAC. The router accesses the home and LNS RADIUS servers. (The separation of the RADIUS servers is transparent to the router.)

Before any attempts at connectivity can take place from the home site to the remote site, an administrator must configure a dial-out route on the router. This route directs the router to start a dial-out operation. The route includes a dial-out target (the virtual router context and the IP address of the remote site). When the router receives a packet destined for the target, it triggers a dial-out session to the target. The route is associated with a profile that holds parameters for the interface stack that the router builds as a result of the dial-out.

Dial-Out Process

The following is the dial-out process used in the [Figure 10](#) network:

1. The router receives a trigger packet.
2. The router builds a RADIUS Access-Request message and sends it to the RADIUS server that is associated with the virtual router on which the dial-out route is defined—typically, the RADIUS home server.
3. The RADIUS server's response to the Access-Request is similar to the response used for LAC incoming calls. Notable differences are that the IP addresses of the peer are interpreted as LAC addresses instead of LNS addresses. In addition, narrowband details, such as calling numbers, are returned.
4. The LNS makes the outgoing call using a load-balancing or round-robin mechanism identical to the one that the E-series LAC uses for incoming calls. The LAC may also employ the LAC RADIUS in tunnel authentication.
5. Once the LNS successfully completes a control connection and session with the LAC, the LAC performs the actual narrowband dial-out operation to the remote site using the information passed by the LNS during session setup.
6. A PPP session is started on the remote customer premises equipment (CPE), and mutual PPP authentication is performed at the remote CPE and the LNS as follows:
 - a. The LNS uses the LNS RADIUS server to validate the remote CPE's PPP session, while the CPE can use its own RADIUS server to validate the LNS's PPP session.
 - b. The LNS uses the username and password that is returned in the first Access-Accept message.
7. Once authentication is successful, an IP interface is built on top of the PPP interface at the LNS. Internet Protocol Control Protocol (IPCP) is negotiated, and the framed route that RADIUS returns as a result of the PPP authentication supersedes the dial-out route.

IP traffic can now flow freely between the home and remote sites.

Dial-Out Operational States

The dial-out state machine is a control process within the router that manages the dial-out function for each IP flow. The dial-out state machine has four levels of control: the router chassis, virtual router, targets, and sessions. This section describes the operational states of each of these levels.

Chassis

[Table 29](#) describes the operational states of the chassis.

Table 29: Chassis Operational States

State	Description
inService	Dial-out service is operational at the chassis level.
initializationFailed	Dial-out service could not obtain enough system resources for basic operation. All configuration commands fail, and the dial-out service does not function.

Virtual Router

[Table 30](#) describes the operational states of the virtual router.

Table 30: Virtual Router Operational States

State	Description
inService	Dial-out service is operational for the virtual router.
initPending	Dial-out service is waiting for the virtual router to be operational. Targets defined within the virtual router are not functional.
down	The dial-out interface for this virtual router is down. Targets defined within the virtual router are not functional.

Targets

[Table 31](#) describes the operational states of the targets.

Table 31: Target Operational States

State	Description
inService	Dial-out route is up and operational.
inhibited	Dial-out service cannot obtain sufficient resources to handle triggers, and all triggers are discarded. When resources become available, a target can transition from inhibited to inService. Note that sessions within an inhibited target that are already in the process of connecting or are in the inService state are not affected by this condition.
down	There are insufficient resources to support the creation of a dial-out route for the target. When resources become available, the target can transition to inService. Note that sessions within a down target that are already in the process of connecting or are in the inService state are not affected by this condition.

Sessions

Table 32 describes operational states of the sessions.

Table 32: Session Operational States

State	Description
authenticating	<p>New sessions start in the authenticating state. In this state, the dial-out state machine has received a valid trigger and is waiting for authentication, authorization, and accounting (AAA) to complete the initial authentication.</p> <p>On getting a grant from AAA, the session transitions to the connecting state. Alternatively, on getting a deny from AAA, the session transitions to the inhibited state.</p>
connecting	<p>Sessions enter the connecting state when authentication is complete. In this state, the dial-out state machine has initiated an outgoing L2TP call. On entering this state, the session-connecting timer is set to the chassis-wide trigger timer value. The session stays in this state until either the outgoing call is successful or the connecting timer expires. Any new trigger packets received for this session when it is in the connecting state are discarded.</p>
inService	<p>A session enters the inService state from the connecting state on successful completion of the dial-out call request. The session stays in this state until the outgoing call is closed.</p>
inhibited	<p>A session enters the inhibited state from the connecting state when the connecting timer expires (that is, the outgoing call was unsuccessful). This state prevents the router from thrashing on an outgoing call that cannot be completed. When in this state, the router discards all trigger packets received for the session.</p> <p>The inhibited timer controls the amount of time spent in this state. The setting of the inhibited timer varies depending on whether the session is entering the inhibited state for the first time or is reentering the state.</p> <ul style="list-style-type: none"> ■ If it is the first time, the inhibited timer is initialized to the chassis-wide trigger value. ■ If it is reentering the state, the inhibited timer is initialized to 2 times the previous value of the inhibited timer, up to a maximum of 8 times the chassis-wide trigger value. For example, if the chassis-wide trigger value is 30 seconds, the setting of the inhibited timer within the session (on subsequent immediate reentries; see postInhibited state) is 30, 60, 120, 240. Since 240 is 8 x 30, the inhibited timer for this session is never set larger than 240 seconds.
postInhibited	<p>A session enters the postInhibited state after completion of an inhibited state. The inhibited timer is reused to control the amount of time the session stays in postInhibited state. In this state the timer repeatedly times out and reduces the inhibited timer by a factor of 2 on each iteration. Once the inhibited timer reaches zero, the session transitions to dormant. The receipt of a trigger in this state results in a transition to the authenticating state.</p>
dormant	<p>A session enters the dormant state after completion of a postInhibited state. The dormant timer is initialized to the chassis-wide dormant timer value, minus the time the session spent in the postInhibited state. Receipt of a new trigger packet transitions the session to the authenticating state. If the dormant timer expires, the session is deleted. The dormant state exists to allow analysis of a dial-out session before it is deleted.</p>

Table 32: Session Operational States (continued)

State	Description
pending	A session enters the pending state when a valid trigger is received but there already are the maximum number of connecting sessions in the router. The router discards all subsequent trigger packets until other sessions transition out of the connecting state. When this happens, pending sessions can transition to the dormant state.
failed	<p>A session enters the failed state when the router detects a configuration error that prevents the successful operation of the session. Specifically, one of the final steps in a dial-out request is mutual PPP authentication at the LNS. A side-effect of authentication is the installation of an access route for the outgoing call. If the access route does not correspond to the trigger packet (that is, the trigger packet cannot be routed successfully by the new access route), the router detects this discrepancy as a configuration error because trigger packets that arrive are not forwarded into the outgoing call; rather, they are buffered or discarded.</p> <p>The only way to exit the failed state is with the l2tp dial-out session reset command.</p>

Outgoing Call Setup Details

This section details the process described in [Dial-Out Process](#) on page 297.

Access-Request Message

To create the username in the authentication request, the router uses the trigger, dial-out route, domain name, and optional Multiprotocol Label Switching (MPLS) route distinguisher (RD). The username is constructed as follows:

[MPLS RD]/[trigger destination address]@domain-name

For example, given a dial-out route with an IP prefix of 10.10.0.0/16, a domain name of L2TP-dial-out.de.dt, and an MPLS RD of 0.0.0.0:65000, if a trigger packet arrives with a destination IP address of 10.10.1.1, the router creates the following username:

0.0.0.0:65000/10.10.1.1@L2TP-dial-out.de.dt

No password is offered, and the authentication request is passed to the S-series AAA server for normal authentication processing.

Using the above example, the AAA domain map processes the L2TP-dial-out.de.dt domain as for any other domain. If RADIUS authentication is configured for the authenticating virtual router (VR) context, AAA passes the authentication request to the E-series RADIUS client. The RADIUS authentication request is consistent with other requests, except that the Service-Type attribute is set to outbound (value of 5).

Access-Accept Message

The router expects RADIUS attributes that define a tunnel to be returned with the additions in [Table 33](#). If tunnel attributes are excluded from the Access-Accept message or the returned Service-Type attribute is not set to outbound, the dial-out session is denied.

Table 33: Additions to RADIUS Attributes in Access-Accept Messages

Attribute Number	Attribute Name	Content
6	Service-Type	Outbound
67	Tunnel-Server-Endpoint	IP address of LAC
Juniper VSA 26-35	Tunnel-Dialout-Number	L2TP dial-out number
Juniper VSA 26-36	PPP-Username	Username used in PPP L2TP dial-out sessions at the LNS
Juniper VSA 26-37	PPP-Password	Password used in PPP L2TP dial-out sessions at the LNS
Juniper VSA 26-38	PPP-Protocol	Authentication protocol used for L2TP sessions. 0 = none 1 = PAP 2 = CHAP 3 = PAP-CHAP 4 = CHAP-PAP
Juniper VSA 26-39	Tunnel-Min-Bps	Minimum line speed; passed to LAC (not interpreted by the LNS)
Juniper VSA 26-40	Tunnel-Max-Bps	Maximum line speed; passed to LAC (not interpreted by the LNS)
Juniper VSA 26-41	Tunnel-Bearer-Type	Bearer capability required: 0 = name; 1 = analog; 2 = digital. Passed to LAC (not interpreted by the LNS).

Outgoing Call

After receiving a valid tunnel definition from AAA, the E-series LNS initiates an outgoing call. The router follows the same load-sharing mechanisms as for incoming calls. See [Failover Between Preference Levels](#) in [Chapter 6, Configuring L2TP](#).

After an outgoing call is successfully signaled, the router dynamically creates a PPP interface. The profile in the dial-out route definition specifies any PPP configuration options. Both the L2TP session and the PPP interface exist on a Tunnel Service module, identical to the LNS operation for incoming calls.

Once the PPP interface is created, Link Control Protocol (LCP) and IPCP are negotiated.

Mutual Authentication

Mutual authentication takes place in LCP, where the LNS validates the PPP interface on the remote CPE and vice-versa. LNS takes the same actions to authenticate the peer as it does on incoming calls.

The LNS obtains the PPP username and password from the initial Access-Accept message. It then provides this information to the remote CPE for authentication.

Route Installation

Once authentication is complete, the router creates a new access route. This route directs the forwarding of IP packets related to the original trigger packet to the newly created interface. The route does not need to be identical to the one specified in the dial-out route, but it must be able to forward packets that have the same destination address as the trigger packet. However, if the access route does not encompass the dial-out route definition, any other trigger packets initiate a new dial-out session.

The dial-out state machine verifies that the trigger packet can be forwarded over the route.

- If the verification is unsuccessful, the dial-out session is put into the failed state.
- If the verification is successful, the dial-out session is put into the inService state.

Platform Considerations

L2TP dial-out is supported on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

References

For more information about L2TP, see [RFC 2661—Layer Two Tunneling Protocol “L2TP” \(August 1999\)](#).

Before You Configure L2TP Dial-Out

Create a profile that the router uses to create the dynamic PPP and IP interfaces on the LNS. The profile specifies parameters that are common to all dial-out sessions that use the profile. The following is an example of a typical profile configuration.

1. Create a profile.

```
host1(config)#profile dialOut
host1(config-profile)#
```

2. Specify the interface used for dialout.

```
host1(config-profile)#ip unnumbered loopback 0/0
```

3. Specify the virtual router for the dial-out user's IP interface.

```
host1(config-profile)#ip virtual-router lns
```

4. Specify the authentication mechanism.

```
host1(config-profile)#ppp authentication chap
```

Configuring L2TP Dial-Out

To configure L2TP dial-out:

1. Enable the creation of a dial-out session.

```
host1(config)#l2tp dial-out target 10.10.0.0 255.255.0.0 L2TP-dial-out.de.dt
profile dialOut
```

2. (Optional) Set the maximum time allowed for successful establishment of an L2TP dial-out session.

```
host1(config)#l2tp dial-out connecting-timer-value 30
```

3. (Optional) Set how long the dial-out session stays in the dormant state waiting for a new trigger after the associated L2TP outgoing call ends.

```
host1(config)#l2tp dial-out dormant-timer-value 300
```

4. (Optional) Set the maximum number of trigger packets held in buffer while the dial-out session is being established.

```
host1(config)#l2tp dial-out max-buffered-triggers 50
```

You can also:

- Manually delete a dial-out session.

```
host1#l2tp dial-out session delete 10.10.0.0
```

- Reset a dial-out session by forcing it to the dormant state.

```
host1#l2tp dial-out session reset 10.10.0.0
```

l2tp dial-out connecting-timer-value

- Use to set the maximum time allowed for attempts to establish L2TP dial-out sessions.
- If the session fails to be established before the connecting timer expires, subsequent attempts to establish the dial-out session to the same destination are inhibited temporarily.
- The range is 30–3600 seconds.
- Example
host1(config)#**l2tp dial-out connecting-timer-value 30**
- Use the **no** version to set the connecting timer to the default, 30 seconds.

l2tp dial-out dormant-timer-value

- Use to set how long the dial-out session waits in the dormant state for a new trigger after the associated L2TP outgoing call ends.
- If no trigger is received before the dormant timer expires, the dial-out session is deleted.
- The range is 0–3600 seconds.
- Example
host1(config)#**l2tp dial-out dormant-timer-value 300**
- Use the **no** version to set the dormant timer to the default, 300 seconds (5 minutes).

l2tp dial-out max-buffered-triggers

- Use to set the maximum number of buffered trigger packets held for any dial-out session pending the successful establishment of the L2TP session. Once the session is established, the buffered trigger packets are transmitted.
- Trigger packets received when the maximum number of triggers are already buffered are discarded.
- The range of values is 0–50.
- Example
host1(config)#**l2tp dial-out max-buffered-triggers 50**
- Use the **no** version to set the number of trigger buffers to the default, 0.

l2tp dial-out session delete

- Use to delete a dial-out session.
- Closes any L2TP outgoing call associated with the dial-out session.
- Example
host1#**l2tp dial-out session delete 10.10.0.0**
- There is no **no** version.

I2tp dial-out session reset

- Use to force the dial-out session to the dormant state where it remains until the dormant timer expires or it receives a new trigger.
- Closes any L2TP outgoing call associated with the dial-out session.
- Example

```
host1#I2tp dial-out session reset 10.10.0.0
```
- There is no **no** version.

I2tp dial-out target

- Use to define an L2TP dial-out target. When the router receives packets destined for the target, it creates a dial-out session.
- When you create a target, you must specify the following:
 - *ipAddress*—IP address of the target
 - *ipAddressMask*—IP address mask of the target
 - *domainName*—Domain name used in the outgoing call Access-Request message
 - *profileName*—Name of profile used to create the interface stack
- Example

```
host1(config)#I2tp dial-out target 10.10.0.0 255.255.0.0 L2TP-dial-out.de.dt profile dialOut
```
- Use the **default** version to remove the L2TP dial-out route.
- Use the **no** version to remove the L2TP dial-out route or target.

Monitoring L2TP Dial-Out

This section presents the commands used to display L2TP dial-out configuration, status, and statistics.

The **show** commands display aspects of the dial-out state machine and details about the dial-out routes themselves. This section presents sample output. The actual output on your router may differ significantly. For detailed information about states, see [Dial-Out Operational States](#) on page 298.

You can use several keywords to tailor the output of the **show I2tp dial-out** commands:

- **summary**—Displays aggregate counts for the subject of the command in each of the possible operational and administrative states.
- **detail**—Displays configuration, state, and statistics.

- **state**—Limits the output to subjects of the command in the specified operational or administrative state.
- **allVirtualRouters**—Displays dial-out information across all virtual routers.



NOTE: The level of a user's permission determines the use of the **allVirtualRouters** option. For example, if you have permission to view only the current virtual router, then that is all that is displayed when you enter a command.

show l2tp dial-out

- Use to display the chassis-wide configuration, operational state, and statistics for L2TP dial-out.
- Field descriptions
 - Operational status—Current operational status of the chassis
 - Connecting timer value—Configuration of the connecting timeout
 - Dormant timer value—Configuration of the dormant timeout
 - Dial-out Chassis Statistics—Statistics at the chassis level
 - Current sessions—Total number of session currently active on the chassis
 - Maximum sessions—Highest value of current sessions recorded on the chassis since the last router restart
 - Current sessions in the process of connecting—Sessions currently in the connecting state
 - Maximum sessions connecting at one time—Highest number of sessions recorded on the chassis at the same time since the last router restart
 - Current sessions pending—Sessions in the pending state
 - Maximum sessions pending—Highest number of sessions recorded in the pending state since the last router restart
 - Current targets inhibited—Targets currently in the inhibited state
 - Maximum targets inhibited—Highest value of targets recorded in the inhibited state since the last router restart
 - Authentication grant for nonexistent session—Number of authentication requests granted to nonexistent sessions
 - Authentication deny for nonexistent session—Number of authentication requests denied to nonexistent sessions
 - Dial-out Virtual router statistics—Statistics at the virtual router level
 - Virtual routers active—VRs in use by the state machine
 - Virtual routers created—VRs that have been used by the state machine
 - Virtual routers removed—VRs no longer used by the state machine

- ❑ Virtual routers in init-pending state—VRs in the initializationPending state
- ❑ Virtual routers in init-failed state—VRs in the initializationFailed state
- ❑ Virtual routers in down state—VRs in the down state
- ❑ Virtual routers in in-service state—VRs in the inService state
- ❑ IP Discarded trigger frames—Trigger frames that IP discarded
- ❑ Trigger frames received for unknown route—Trigger frames received for an unknown route
- ❑ Sessions in dormant state—Sessions on the VR that are in the dormant state
- ❑ Sessions in pending state—Sessions on the VR that are in the pending state
- ❑ Sessions in authenticating state—Sessions on the VR that are in the authenticating state
- ❑ Sessions in connecting state—Sessions on the VR that are in the connecting state
- ❑ Sessions in in-service state—Sessions on the VR that are in the inService state
- ❑ Sessions in inhibited state—Sessions on the VR that are in the inhibited state
- ❑ Sessions in post-inhibited state—Sessions on the VR that are in the postInhibited state
- ❑ Sessions in failed state—Sessions on the VR that are in the failed state
- Dial-out target statistics—Statistics at the route target level
 - ❑ Targets active—Current active targets
 - ❑ Targets created—All targets created
 - ❑ Targets removed—Targets deleted
 - ❑ Targets in down state—Targets in the down state
 - ❑ Targets in inhibited state—Targets in the inhibited state
 - ❑ Targets in in-service state—Targets in the inService state
 - ❑ Triggers discarded—Trigger packets discarded
- Dial-out session statistics—Statistics at the session level
 - ❑ Sessions active—Currently active sessions
 - ❑ Sessions created—All sessions created
 - ❑ Sessions removed—Sessions deleted
 - ❑ Sessions reset—Sessions reset using the **l2tp dial-out session reset** command
 - ❑ Triggers received—Triggers received for dial-out sessions
 - ❑ Triggers enqueued—Triggers that have been put into the queue
 - ❑ Triggers discarded—Trigger packets discarded

- ❑ Triggers forwarded—Trigger packets forwarded
- ❑ Triggers max enqueued—Maximum number of triggers that have been enqueued simultaneously since the last router reset
- ❑ Authentication requests—Authentication requests received
- ❑ No resources for authentication—Authentication requests not processed because of insufficient resources
- ❑ Authentication grants—Authentication requests granted
- ❑ Authentication Denies—Authentication requests denied
- ❑ Dial-outs requested—Outgoing calls requested for sessions
- ❑ Dial-outs rejected—Outgoing call requests that were rejected
- ❑ Dial-outs established—Successful outgoing calls before the connecting timer expired
- ❑ Dial-outs timed out—Number of times the connecting timer expired
- ❑ Dial-outs torn down—Successful outgoing calls that were terminated

■ Example 1

```
host1#show l2tp dial-out
Operational status: inService
Connecting timer value: 30 seconds
Dormant timer value: 300 seconds
```

■ Example 2

```
host1#show l2tp dial-out detail
Dial-out Chassis Configuration and Operational Status
Chassis operational status : inService
Dormant timeout           : 30 seconds
Connecting timeout        : 30 seconds

Dial-out Chassis Statistics
Current sessions:                0
Maximum sessions:               0
Current sessions in the process of connecting: 0
Maximum sessions connecting at one time: 0
Current sessions pending:        0
Maximum sessions pending:        0
Current targets inhibited:        0
Maximum targets inhibited:        0
Authentication grant for nonexistent session: 0
Authentication deny for nonexistent session: 0

Dial-out Virtual router statistics
Virtual routers active:          0
Virtual routers created:         0
Virtual routers removed:         0
Virtual routers in init-pending state: 0
Virtual routers in init-failed state: 0
Virtual routers in down state:    0
Virtual routers in in-service state: 0
IP Discarded trigger frames:     0
Trigger frames received for unknown route: 0
Sessions in dormant state:        0
Sessions in pending state:        0
```

```

Sessions in authenticating state:      0
Sessions in connecting state:         0
Sessions in in-service state:         0
Sessions in inhibited state:          0
Sessions in post-inhibited state:     0
Sessions in failed state:             0

Dial-out target statistics
Targets active:                       0
Targets created:                     0
Targets removed:                     0
Targets in down state:               0
Targets in inhibited state:          0
Targets in in-service state:         0
Triggers discarded:                  0

Dial-out session statistics
Sessions active:                     0
Sessions created:                    0
Sessions removed:                    0
Sessions reset:                      0
Triggers received:                   0
Triggers enqueued:                   0
Triggers discarded:                   0
Triggers forwarded:                  0
Triggers max enqueued:               0
Authentication requests:             0
No resources for authentication:      0
Authentication grants:               0
Authentication Denies:               0
Dial-outs requested:                 0
Dial-outs rejected:                  0
Dial-outs established:               0
Dial-outs timed out:                 0
Dial-outs torn down:                 0

```

■ Example 3

```

host1#show l2tp dial-out summary
Virtual routers in init pending state :      0
Virtual routers in init failed state :      0
Virtual routers in down state :             0
Virtual routers in inService state :         0
Targets in down state :                     0
Targets in inhibited state :                 0
Targets in inService state :                 0
Sessions in dormant state :                  0
Sessions in pending state :                  0
Sessions in authenticating state :           0
Sessions in connecting state :               0
Sessions in inService state :                0
Sessions in inhibited state :                0
Sessions in postInhibited state :            0
Sessions in failed state :                   0

```

show l2tp dial-out session

- Use to display the status of dial-out sessions.
- If you do not include any options, the command displays all sessions within the current virtual router context.
- To limit the display to detailed information about a particular session, enter the trigger IP address for the session.
- Field descriptions
 - Session—IP address of the session
 - Status—Current status of the session
 - Operational status—Current operational status of session

■ Example 1

```
host1#show l2tp dial-out session
Session           Status
-----
10.10.1.1         connected
10.10.2.1         dormant
```

■ Example 2

```
host1#show l2tp dial-out session 10.1.1.1
Session 10.1.1.1
Operational status: dormant
```

show l2tp dial-out target

- Use to display configured dial-out targets within the current virtual router context.
- If you do not include any options, the command displays general information for all targets within the virtual router.
- To limit the display to detailed information about a target, enter the target IP address and mask.
- Field descriptions
 - Target—Address of the target
 - Status—Status of the connection to the target
 - Active Sessions—Currently active session to the target
 - Total triggers—Trigger packets received for the target
 - Failed sessions—Sessions that are currently in the failed state
 - Connected sessions—Sessions that are currently in the connected state

■ Example 1

```
host1:dialout#show l2tp dial-out target
Target           Status      Active Sessions
-----
10.10.1.1/16     up         14
10.1.1.0/24     up         10
```

- Example 2

```
host1:dialout#show l2tp dial-out target 10.1.1.0/24
Target 10.1.1.0/24
Operational status: up
Active sessions: 10
Total triggers: 127
Failed sessions: 2
Connected sessions: 8
```

show l2tp dial-out virtual-router

- Use to display dial-out state machine operational status and statistics within the current VR context.
- Field descriptions
 - Virtual router—Name of VR
 - Virtual router operational status—Operational status of the VR
 - Maximum trigger buffers per session—Maximum number of trigger packets held in buffer while the dial-out session is being established
- Example

```
host1#show l2tp dial-out virtual-router
Dial-out Virtual Router Configuration and Operational Status
Virtual router host1:
Virtual router operational status: inService
Maximum trigger buffers per session: 0
```


Chapter 8

Configuring DHCP

The Dynamic Host Configuration Protocol (DHCP) provides a mechanism through which computers using Transmission Control Protocol/IP (TCP/IP) can obtain protocol configuration parameters automatically from a DHCP server on the network.

The following sections describe how to configure your E-series router to provide DHCP support:

- [Overview](#) on page 314
- [Platform Considerations](#) on page 314
- [References](#) on page 315
- [Configuring the DHCP Access Model](#) on page 316
- [Configuring DHCP Proxy Clients](#) on page 316
- [Configuring DHCP Relay and BOOTP Relay](#) on page 318
- [Configuring DHCP Relay Proxy](#) on page 338
- [Configuring DHCP Local Server](#) on page 340
- [Configuring DHCP External Server Application](#) on page 364
- [Using Option 60 Strings to Forward Client Traffic to Specific DHCP Servers](#) on page 368
- [Viewing and Deleting DHCP Client Bindings](#) on page 371
- [Logging DHCP Packet Information](#) on page 372
- [Monitoring DHCP](#) on page 373

Overview

The most important configuration parameter carried by DHCP is the IP address. A computer must be initially assigned a specific IP address that is appropriate to the network to which the computer is attached and that is not assigned to any other computer on that network. If you move a computer to a new network, it must be assigned a new IP address for that new network. You can use DHCP to manage these assignments automatically.

An IP client contacts a DHCP server for configuration parameters. The DHCP server is typically centrally located and operated by the network administrator. Because the server is run by a network administrator, DHCP clients can be reliably and dynamically configured with parameters appropriate to the current network architecture.

You can configure the E-series router to support the following DHCP features:

- DHCP access model
- DHCP proxy client
- DHCP relay
- DHCP relay proxy
- DHCP local server
- DHCP external server

Service Deployment System

The Service Deployment System (SDX) is a component of Juniper Networks management products. The SDX application provides a Web-based interface that allows subscribers to access services, such as the Internet, an intranet, or an extranet.

When a DHCP subscriber logs in, the SDX can authorize the address request and select the DHCP address pool on the router from which the DHCP address is selected. The SDX can also control the number of IP addresses that are given to a particular retailer or subscriber and control the lease time of IP addresses assigned to DHCP subscribers.

Platform Considerations

For information about modules that support DHCP on the ERX-7xx models, ERX-14xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, ERX Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support DHCP.

For information about modules that support DHCP on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Module and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support DHCP.

References

For more information about DHCP, consult the following resources:

- [DSL Forum Technical Report \(TR\)-101—Migration to Ethernet-Based DSL Aggregation \(April 2006\)](#)
- [RFC 2131—Dynamic Host Configuration Protocol \(March 1997\)](#)
- [RFC 2132—DHCP Options and BOOTP Vendor Extensions \(March 1997\)](#)
- [RFC 3046—DHCP Relay Agent Information Option \(January 2001\)](#)
- [RFC 3315—Dynamic Host Configuration Protocol for IPv6 \(DHCPv6\) \(July 2003\)](#)
- [RFC 3633—IPv6 Prefix Options for Dynamic Host Configuration Protocol \(DHCP\) Version 6 \(December 2003\)](#)
- [RFC 4243—Vendor-Specific Information Suboption for the Dynamic Host Configuration Protocol \(DHCP\) Relay Agent Option \(December 2005\)](#)



NOTE: IETF drafts are valid for only 6 months from the date of issuance. They must be considered as works in progress. Please refer to the IETF Web site at <http://www.ietf.org> for the latest drafts.

For information about supported accounting attributes, see [Chapter 2, Configuring RADIUS Attributes](#) and [Appendix A, RADIUS Attribute Descriptions](#)

Configuring the DHCP Access Model

The E-series router provides a DHCP access model, which enables you to integrate the router into an existing RADIUS-based operation support system (OSS). In the DHCP access model, a DHCP local server or DHCP external service is configured, but the E-series router does not have direct interaction with an OSS or a policy server, such as the SDX application. The router passes the client's DHCP options, client's media access control (MAC) address and, if appropriate, the DHCP relay's IP address in RADIUS requests for authentication.

To configure the DHCP access model to pass the client's information in RADIUS requests, you enable the DHCP options feature, then specify the client information to be passed to RADIUS. You can specify that the client's MAC address be included in the request. You can also specify that the DHCP relay's IP address be sent, if appropriate. For descriptions of the RADIUS attributes used with the DHCP access model, see [Chapter 2, Configuring RADIUS Attributes](#).

Configuring DHCP Proxy Clients

DHCP proxy client support enables the router to obtain an IP address from a DHCP server for a remote PPP client. Each virtual router (acting as a DHCP proxy client) can query up to five DHCP servers.

For PPP users, the router acts as a DHCP client to obtain an address for the user. This is referred to as DHCP proxy.

The process for PPP users is as follows:

1. The remote user dials in, and the client requests RADIUS authentication.
2. The AAA server on the router sends a request to the DHCP proxy client on the router for an IP address to be assigned to the remote user's host.
3. The proxy client assumes the role of DHCP client and sends a discovery message to each DHCP server.
4. One or more of the DHCP servers responds with an offer message containing an IP address.
5. The proxy client determines which offer to accept and sends a message to that DHCP server requesting that IP address.
6. The DHCP server responds to the proxy client with an acknowledgment message.
7. The proxy client passes the IP address to the authentication, authorization, and accounting (AAA) server on the router, and the AAA server returns the address to PPP. PPP then assigns the address to the remote host. The new IP address is included when the router next updates its routing table.

Dynamic IP addresses are *leased* to the remote host for a specific period of time, which can range from minutes to days. At the halfway point in the lease period, the proxy client requests an extension from the DHCP server on behalf of the remote host. The lease is extended for a period specified in the acknowledgment (ACK) message returned by the DHCP server—typically equal to the original lease. If the DHCP server returns a negative acknowledgment (NAK) message to the proxy client, the proxy client notifies the server on the router that the extension has been denied. The AAA server logs out the remote host and frees the IP address for reuse.

When a remote host disconnects, the AAA server notifies the proxy client that the IP address is available for reuse. The proxy client informs the DHCP server, which can now reassign that IP address.

For additional information on managing client bindings, see [Viewing and Deleting DHCP Client Bindings](#) on page 371.

To configure a proxy client from Global Configuration mode:

1. Specify one or more DHCP servers.

```
host1(config)#ip dhcp-server 10.6.128.10
```

2. Direct the router to request IP addresses for remote users from the DHCP server(s).

```
host1(config)#ip address-pool dhcp
```

ip address-pool

- Use to specify to the router where to get an IP address for the remote user.
- In this case, select the **dhcp** option to get the address from a DHCP server.
- Example

```
host1(config)#ip address-pool dhcp
```
- Use the **no** version to set the default, local.

ip dhcp-server

- Use to specify the address of a DHCP server that will provide IP addresses for remote hosts.
- When you issue this command, the router adds the IP address to the list of DHCP servers (up to five).
- Example

```
host1(config)#ip dhcp-server 10.6.128.10
```
- Use the **no** version to remove the specified DHCP server or all DHCP servers.

Configuring DHCP Relay and BOOTP Relay

The DHCP relay feature relays a request from a remote client to a DHCP server for an IP address. When the router receives a DHCP request from an IP client, it forwards the request to the DHCP server and passes the response back to the IP client.

Configuring DHCP relay also enables bootstrap protocol (BOOTP) relay. The router relays any BOOTP requests it receives to the same set of servers that you configured for DHCP relay. A DHCP server can respond to the BOOTP request only if it is also a BOOTP server. The router relays any BOOTP responses it receives to the originator of the BOOTP request. If you do not configure DHCP relay, then BOOTP relay is disabled.

The router must wait for an acknowledgment from the DHCP server that the assigned address has been accepted. The IP client must accept an IP address from one of the servers. When the DHCP server sends an acknowledgment message back to the DHCP client via the router, the router updates its routing table with the IP address of the client.

If a DHCP relay request is received on an unnumbered interface, the router determines the loopback address for that interface and passes that IP address to the server.

DHCP carries other important configuration parameters, such as the subnet mask, default router, and DNS server. You can also use the DHCP relay agent information option (option 82) to add information to the DHCP packets sent to DHCP servers—the additional information, in the form of suboptions to the option 82 value, helps you to manage the IP address and service level assignments granted to your subscribers. For example, you can add the E-series hostname or the virtual router name to the front of the Agent Circuit ID suboption (suboption 1) of the DHCP relay agent information option (option 82). See [Configuring Relay Agent Information Option \(Option 82\) Suboption Values](#) on page 328.

Trust-All Method

By default, the DHCP relay treats all packets destined for DHCP servers as if the packets originated at an untrusted source; if the packets have a gateway IP address (giaddr) of 0 and if option 82 information is present, these packets are dropped. However, you can use the **set dhcp relay trust-all** command to enable the trust-all method on the DHCP relay. In the trust-all method, the DHCP relay treats the packets as if they are from trusted sources and forwards the packets to the DHCP server.

Assigning the Giaddr to Source IP Address

As a security measure, DHCP servers typically use the giaddr included in DHCP packets to ensure that the packets come from a recognized DHCP gateway. The servers verify that the giaddr in the DHCP packet matches the source IP address in the IP packet header. You can use the **set dhcp relay assign-giaddr-source-ip** command to specify that the DHCP relay and DHCP relay proxy assign the giaddr to the source IP packet header of packets they send to DHCP servers—the DHCP servers can then compare the giaddr in the IP packet header to the giaddr in the DHCP packets.

Protecting Against Spoofed Giaddr and Relay Agent Option Values

DHCP relay includes an override feature that provides enhanced security to protect against spoofed giaddr and relay agent option (option 82) values in packets destined for DHCP servers.

DHCP relay can detect spoofed giaddrs when the giaddr value is equal to a local IP address on which the DHCP relay can be accessed; otherwise, DHCP relay does not detect spoofed giaddrs. Also, DHCP relay does not detect spoofed relay agent option values.

Spoofed giaddrs are a concern when the DHCP relay is used if the giaddr value in received DHCP packets is different from the local IP address on which the DHCP relay is accessed. In this situation, DHCP relay always honors the giaddr. To configure DHCP relay to override all giaddrs (including valid giaddrs) that are received from downstream network elements, use the **set dhcp relay override giaddr** command. DHCP relay then takes control of the client, adding its own giaddr to the packets before forwarding the packets to the DHCP server.

Spoofed relay agent options are a concern if the giaddr is not null, or if it is null and the DHCP relay is operating in the trust-all method. In these two situations, DHCP relay always honors the relay agent option value in received DHCP packets. To protect against spoofed relay agent option values, use the **set dhcp relay override agent-option** command. DHCP relay then overrides all relay agent option values that are received from downstream network elements, performing one of the following actions:

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

Using the Giaddr to Identify the Primary Interface for Dynamic Subscriber Interfaces

When creating dynamic subscriber interfaces, the router builds the dynamic interfaces on the associated primary interface. By default, the router identifies the primary interface based on the interface on which DHCP client discover packets are received. The router then builds all dynamic interfaces on that primary interface.

In some cases you might want more control over the determination of the primary interface and you might not want to use the primary interface that is determined by the default behavior. The JUNOS software enables you to configure DHCP relay to use information in the giaddr in DHCP ACK messages to specify which interface is to be used as the primary interface. This capability allows you to build dynamic interfaces on the primary interface of your choice.

DHCP Relay Configuration and ARP Spoof Checking

The Address Resolution Protocol (ARP) performs spoof checking on all incoming ARP requests by default. For each incoming packet, ARP does a route lookup on the source IP address to determine the interface on which that IP address was routed. ARP then verifies that the interface on which the packet was received matches the routed interface. If the interface on which the packet was received does not match the routed interface, the router drops the packet.

When you configure applications such as DHCP relay that automatically install routes, you must ensure that the routes are correctly installed for your configuration. DHCP relay installs host routes by default, which is required in certain configurations to enable address renewals from the DHCP server to work properly. However, the default installation of host routes might cause a conflict when you configure DHCP relay with static subscriber interfaces. To avoid these configuration conflicts, use the **set dhcp relay inhibit-access-route-creation** command to prevent DHCP relay from installing host routes by default.

Example This example describes a sample procedure for configuring multiple subscribers over a particular static subscriber interface (ip53001 in this example)—you might use commands similar to the following to create demultiplexer table entries and a subnet route that points to the static subscriber interface.

In the example, the host routes are associated with the primary IP interface on Gigabit Ethernet 1/0. Because the host routes are statically configured with the subscriber interface, there is no need for the router to install DHCP host routes. Therefore, in step 7, the **set dhcp relay inhibit-access-route-creation** command is used to prevent DHCP relay from installing host routes.

1. Create a shared IP interface.

```
host1(config)#interface ip ip53001
```

2. Associate the shared IP interface with a static layer 2 interface.

```
host1(config-if)#ip share-interface gigabitEthernet 1/0
```

3. Make the shared interface an unnumbered interface.

```
host1(config-if)#ip unnumbered loopback 53
```

4. Specify the source addresses that the subscriber interface uses to demultiplex traffic.

```
host1(config-if)#ip source-prefix 10.10.10.0 255.255.255.252
```

5. Exit Interface Configuration mode.

```
host1(config-if)#exit
```

6. Create a static route that sends traffic for destination address 10.10.10.0 to subscriber interface ip53001.

```
host1(config)#ip route 10.10.10.0 255.255.255.252 ip ip53001
```

7. Prevent DHCP relay from installing host routes—this avoids a conflict that can cause undesirable ARP behavior.

```
host1(config)#set dhcp relay inhibit-access-route-creation
```

In the example, if you do not prevent DHCP relay from installing host routes, the ARP spoof-checking mechanism associates the ARP traffic with the primary IP interface (Gigabit Ethernet 1/0), although packets actually arrive on the subscriber interface (ip53001), causing the router to detect a spoof and drop the packet.

Including Relay Agent Option Values in the PPPoE Remote Circuit ID

You can enable the router to capture and format a vendor-specific tag containing a PPPoE remote circuit ID value transmitted from a digital subscriber line access multiplexer (DSLAM) device. The router can then send this value to a Remote Authentication Dial-In User Service (RADIUS) server or to a Layer 2 Tunneling Protocol (L2TP) network server (LNS) to uniquely identify subscriber locations.

By default, the router formats the captured PPPoE remote circuit ID to include only the agent-circuit-id suboption (suboption 1) of the DHCP relay agent information option (option 82). You can use the **radius remote-circuit-id-format** command to configure the following nondefault formats for the PPPoE remote circuit ID value:

- Include either or both of the agent-circuit-id (suboption 1) and agent-remote-id (suboption 2) suboptions of the DHCP relay agent information option, with or without the NAS-Identifier [32] RADIUS attribute.
- Append the agent-circuit-id suboption value to an interface specifier that is consistent with the recommended format in the [DSL Forum Technical Report \(TR\)-101—Migration to Ethernet-Based DSL Aggregation \(April 2006\)](#).

For information about configuring the PPPoE remote circuit ID, see [Using the PPPoE Remote Circuit ID to Identify Subscribers](#) and [Configuring PPPoE Remote Circuit ID Capture](#) in *JUNOS Link Layer Configuration Guide, Chapter 7, Configuring Point-to-Point Protocol over Ethernet*.

Configuring Layer 2 Unicast Transmission Method for Reply Packets to DHCP Clients

By default, DHCP relay and relay proxy broadcast DHCP Offer reply packets and DHCP ACK and NAK reply packets to DHCP clients during the discovery process. In some environments, this default broadcast method might be a security concern because all clients can receive packets intended for all other clients.

You use the **set dhcp relay layer2-unicast-replies** command in Global Configuration mode to configure the optional layer 2 unicast and layer 3 broadcast transmission method for DHCP relay and DHCP relay proxy. This method uses the client's layer 2 (MAC) address and layer 3 (IP) broadcast address to provide secure transmission of DHCP Offer reply packets and ACK and NAK reply packets. The optional layer 2 unicast method enables reply packets to be broadcast through the layer 3 network but received only by the specified client.

There are exceptions to this behavior for DHCP relay proxy when the DHCP client is already bound to an IP address or is renewing the lease on its IP address. For information, see [DHCP Relay Proxy Behavior for Bound Clients and Address Renewals](#) on page 324.

To display whether the layer 2 unicast method is currently on or off on the router, use the **show dhcp relay** command. For information, see [show dhcp relay](#) on page 376.

The dhcpRelayGeneral logging event category uses the debug severity level to log DHCP reply packets that are transmitted to clients using a layer 2 unicast address and a layer 3 broadcast address.

The **set dhcp relay broadcast-flag-replies** command configures the router to use the setting of the broadcast flag in DHCP request packets to control the transmission of DHCP reply packets. The **set dhcp relay layer2-unicast-replies** command and the **set dhcp relay broadcast-flag-replies** command are mutually exclusive. For more information, see [Interaction with Layer 2 Unicast Transmission Method](#) on page 323.



NOTE: When you enable the layer 2 unicast transmission feature, the DHCP relay and DHCP relay proxy instance must be the next hop from the DHCP clients. Otherwise, the DHCP reply packets might be discarded.

The layer 2 unicast transmission method is not supported on non-ASIC line modules.

Using the Broadcast Flag Setting to Control Transmission of DHCP Reply Packets

Each DHCP request packet includes a broadcast flag that, if set, specifies how to transmit DHCP Offer reply packets and DHCP ACK and NAK reply packets to DHCP clients during the discovery process. To configure DHCP relay and DHCP relay proxy to use the setting of the broadcast flag to control the transmission of DHCP Offer, DHCP ACK, and DHCP NAK reply packets, use the **set dhcp relay broadcast-flag-replies** command from Global Configuration mode.

When you issue the **set dhcp relay broadcast-flag-replies** command, the method that DHCP relay and DHCP relay proxy use to transmit DHCP Offer reply packets and ACK and NAK reply packets depends on whether the broadcast flag in the DHCP request packet is set or not set, as follows:

- If the broadcast flag is set in the DHCP request packet, using the **set dhcp relay broadcast-flag-replies** command causes DHCP relay and DHCP relay proxy to broadcast DHCP reply packets to clients.
- If the broadcast flag is not set in the DHCP request packet, using the **set dhcp relay broadcast-flag-replies** command causes DHCP relay and DHCP relay proxy to use the layer 2 unicast transmission method to send DHCP reply packets using the client's layer 2 (MAC) address and layer 3 (IP) unicast address.

There are exceptions to this behavior for DHCP relay proxy when the DHCP client is already bound to an IP address or is renewing the lease on its IP address. For information, see [DHCP Relay Proxy Behavior for Bound Clients and Address Renewals](#) on page 324.

To display whether support for broadcast flag replies is currently on or off on the router, use the **show dhcp relay** command. For information, see [show dhcp relay](#) on page 376.

To troubleshoot applications that use this feature, you can use the dhcpCapture system event log category. For information about how to log system events, see [JUNOS System Event Logging Reference Guide, Chapter 1, System Logging Overview](#).

Interaction with Layer 2 Unicast Transmission Method

As described in [Configuring Layer 2 Unicast Transmission Method for Reply Packets to DHCP Clients](#) on page 321, you can use the **set dhcp relay layer2-unicast-replies** command to configure DHCP relay and DHCP relay proxy to use the layer 2 unicast and layer3 broadcast transmission method to send DHCP Offer reply packets and DHCP ACK and NAK reply packets to clients.

The **set dhcp relay broadcast-flag-replies** command and the **set dhcp relay layer2-unicast-replies** command are mutually exclusive. If you attempt to issue the **set dhcp relay broadcast-flag-replies** command when the **set dhcp relay layer2-unicast-replies** command is already in effect, the operation fails and the router displays the following message:

```
% layer2-unicast-replies and broadcast-flag-replies are mutually exclusive
```

If this message appears, you must first issue the **no set dhcp relay layer2-unicast-replies** command to disable layer 2 unicast replies, and then issue the **set dhcp relay broadcast-flag-replies** command again to enable broadcast flag replies.

[Table 34](#) summarizes how the configuration of the **set dhcp relay broadcast-flag-replies** command and the **set dhcp relay layer2-unicast-replies** command interacts with the setting of the broadcast flag in DHCP request packets to control how the router transmits DHCP reply packets to clients during the discovery process. Because these commands are mutually exclusive, broadcast flag replies and layer 2 unicast replies cannot both be enabled on the router at the same time.

Table 34: Effect of Router Configuration on Transmission of DHCP Reply Packets

Broadcast Flag Replies	Layer 2 Unicast Replies	Router Behavior if Broadcast Flag Set	Router Behavior if Broadcast Flag Not Set
Enabled (on)	Disabled (off)	DHCP relay and DHCP relay proxy broadcast DHCP reply packets to clients.	DHCP relay and DHCP relay proxy use layer 2 unicast and layer 3 unicast transmission to send DHCP reply packets to clients.
Disabled (off)	Enabled (on)	DHCP relay and DHCP relay proxy use layer 2 unicast and layer 3 broadcast transmission to send DHCP reply packets to clients.	DHCP relay and DHCP relay proxy use layer 2 unicast and layer 3 broadcast transmission to send DHCP reply packets to clients.
Disabled (off)	Disabled (off)	DHCP relay and DHCP relay proxy broadcast DHCP reply packets to clients. For information about exceptions to this behavior for DHCP relay proxy, see DHCP Relay Proxy Behavior for Bound Clients and Address Renewals on page 324.	DHCP relay and DHCP relay proxy broadcast DHCP reply packets to clients. For information about exceptions to this behavior for DHCP relay proxy, see DHCP Relay Proxy Behavior for Bound Clients and Address Renewals on page 324.

DHCP Relay Proxy Behavior for Bound Clients and Address Renewals

When a DHCP client is already bound to an IP address or is renewing the lease on its IP address, DHCP relay proxy unicasts DHCP ACK and DHCP NAK replies to the client regardless of the current configuration of the **set dhcp relay layer2-unicast-replies** command or the **set dhcp relay broadcast-flag-replies** command.

This behavior applies only to DHCP relay proxy; it does not apply to DHCP relay because DHCP relay does not maintain a list of active clients or receive address renewal requests from clients.

For information about using the **set dhcp relay layer2-unicast-replies** command, see [Configuring Layer 2 Unicast Transmission Method for Reply Packets to DHCP Clients](#) on page 321. For information about using the **set dhcp relay broadcast-flag-replies** command, see [Using the Broadcast Flag Setting to Control Transmission of DHCP Reply Packets](#) on page 322.

set dhcp relay

- Use to create and enable DHCP relay in the current virtual router.
- Use this command without an IP address to create the DHCP relay independent of any DHCP servers. Use this version of the command when configuring support for DHCP vendor-option strings (option 60). For information about configuring option 60 support, see [Using Option 60 Strings to Forward Client Traffic to Specific DHCP Servers](#) on page 368.
- Use with the IP address variable to enable DHCP relay and BOOTP relay and to specify an IP address for the DHCP server.
- The router relays any BOOTP requests it receives to the same set of servers that you configured for DHCP relay.
- When you issue this command with the IP address of a DHCP server, the router adds the IP address to the list of DHCP servers (up to five) and forwards all request packets to all configured servers.
- Issuing this command also enables relay of BOOTP requests to the configured DHCP servers. If one of the DHCP servers is also a BOOTP server and responds, the router relays the response to the request originator.
- You can use the **inhibit-access-route-creation** keyword to specify that the DHCP relay does not install access routes. (See [DHCP Relay Configuration and ARP Spoof Checking](#) on page 319.)
- You can use the **discard-access-routes** keyword to remove existing access routes for an interface from routing tables and nonvolatile storage (NVS).
- Example 1

```
host1(config)#set dhcp relay
```
- Example 2

```
host1(config)#set dhcp relay 192.168.29.10
```

- Use the **no** version without specifying an IP address to explicitly delete the DHCP relay from the current virtual router. Use the **no** version with an IP address to remove the specified DHCP server.



NOTE: When this feature is configured, the client bypasses the DHCP relay component and communicates directly with the DHCP server to request address renewal or to release the address. The DHCP relay component has no role in determining when or whether to remove the installed host route.

set dhcp relay assign-giaddr-source-ip

- Use to configure DHCP relay and DHCP relay proxy to assign the giaddr to the source IP address of traffic that they send to DHCP servers. The DHCP servers can then use the giaddr to verify that the incoming traffic is from the DHCP relay or DHCP relay proxy.
- Example

```
host1(config)#set dhcp relay assign-giaddr-source-ip
```
- The **no** version of the command restores the default in which the DHCP relay and DHCP relay proxy do not assign the giaddr to the source IP address.

set dhcp relay broadcast-flag-replies

- Use to configure DHCP relay and DHCP relay proxy to use the setting of the broadcast flag in the DHCP request packet to control the transmission of DHCP Offer and DHCP ACK and NAK reply packets to DHCP clients during the discovery process.
- If the broadcast flag is set in the request packet, DHCP relay and DHCP relay proxy broadcast DHCP reply packets to clients.
- If the broadcast flag is not set in the request packet, DHCP relay and DHCP relay proxy use the layer 2 unicast transmission method to send DHCP reply packets using the client's layer 2 (MAC) address and layer 3 (IP) unicast address.
- The **set dhcp relay broadcast-flag-replies** command and the **set dhcp relay layer2-unicast-replies** command are mutually exclusive. For more information, see [Interaction with Layer 2 Unicast Transmission Method](#) on page 323.
- Example

```
host1(config)#set dhcp relay broadcast-flag-replies
```
- Use the **no** version to cause the router not to use the broadcast flag setting and restore the default behavior, which broadcasts DHCP Offer reply packets and ACK and NAK reply packets to all clients during the discovery process.

set dhcp relay giaddr-selects-interface

- Use to configure DHCP relay to use information in the giaddr in DHCP server-destined packets to identify the primary interface on which dynamic subscriber interfaces are built.
- Example

```
host1(config)#set dhcp relay giaddr-selects-interface
```

- Use the **no** version to restore the default in which DHCP relay builds dynamic subscriber interfaces on the IP interface that is used for DHCP server-destined messages.

set dhcp relay layer2-unicast-replies

- Use to configure DHCP relay and DHCP relay proxy to use the optional layer 2 unicast and layer 3 broadcast transmission feature to transmit DHCP Offer reply packets and ACK and NAK reply packets to DHCP clients during the discovery process.
- The **set dhcp relay layer2-unicast-replies** command and the **set dhcp relay broadcast-flag-replies** command are mutually exclusive. For more information, see *Interaction with Layer 2 Unicast Transmission Method* on page 323.
- Example

```
host1(config)#set dhcp relay layer2-unicast-replies
```
- Use the **no** version to restore the default method that broadcasts DHCP Offer reply packets and ACK and NAK reply packets to all DHCP clients during the discovery process.

set dhcp relay options

- Use to configure the relay agent option 82 information. This is information that the router adds to DHCP packets before it relays the packets to the DHCP server.
- Use one of the following keywords to add either the hostname or virtual router name to the front of the Circuit-Id field:
 - **hostname**—Adds the router's hostname to the front of the Circuit-Id field; a colon separates the hostname from the circuit information
 - **vrname**—Adds the router's virtual router name to the front of the Circuit-Id field; a colon separates the virtual router name from the circuit information
- The last option specified is the one in use; that is, specifying either hostname or virtual router name turns off the other selection.
- Use the **exclude-subinterface-id** to strip the subinterface ID from the Interface-Id field. When the interface ID is constructed, it contains the slot/port numbers, the subinterface ID, and the VPI/VCI for ATM interfaces or the VLAN ID for Ethernet interfaces. Use this keyword to remove the subinterface ID from the Interface-Id field.
- Example

```
host1(config)#set dhcp relay options hostname
```
- Use the **no** version to return to the default, no additional information is added to the Circuit-Id field, and the subinterface ID is not stripped from the Interface-Id field.

set dhcp relay override

- Use to configure the DHCP relay to override the relay agent option (option 82) or the giaddr information in packets destined for a DHCP server.
- Use one of the following keywords to override either the option 82 or the giaddr information:
 - **agent-option**—The DHCP relay ignores the relay agent option information and performs one of the following actions:
 - If the DHCP relay is configured to add relay agent option 82 to the packets, it clears the existing option 82 values and inserts the new values.
 - If the DHCP relay is not configured to add relay agent option 82, it clears the existing option values, but does not add any new values.
 - **giaddr**—The DHCP relay clears the giaddr, then adds its own giaddr to the packet and forwards the packet to the DHCP server.
- Example

```
host1(config)#set dhcp relay override giaddr
```
- Use the **no** version to return to the default, in which the information is not overridden.

set dhcp relay preserve-trusted-client-option

- Use to enable DHCP relay or DHCP relay proxy to preserve option 82 information for trusted clients, in which DHCP relay and DHCP relay proxy prevent option 82 information from being stripped off packets destined for a trusted client. A trusted client has a giaddr value of 0. If DHCP relay is configured not to remove option 82 and the giaddr field is 0, option 82 information remains in the packets.
- Example

```
host1(config)#set dhcp relay preserve-trusted-client-option
```
- Use the **no** version to restore the default, in which DHCP relay strips the packets.

set dhcp relay trust-all

- Use to enable the DHCP relay trust-all method, in which the DHCP relay treats all server-destined DHCP packets as if the packets are from trusted sources.
 - If the DHCP packets contain option 82 and a giaddr field of 0, the DHCP relay inserts its giaddr into the packets and then forwards the packets.
 - If the DHCP relay is configured to add option 82, it does not add an additional option 82 if one is already present in the DHCP packets.
- Example

```
host1(config)#set dhcp relay trust-all
```
- Use the **no** version to restore the default, in which the DHCP relay treats the packets as if they are from an untrusted source; packets that contain option 82 and a giaddr field of 0 are dropped.

Configuring Relay Agent Information Option (Option 82) Suboption Values

The DHCP relay agent information option (option 82) enables you to include additional useful information in the client-originated DHCP packets that the DHCP relay forwards to a DHCP server.

When the DHCP relay agent information option is enabled, the DHCP relay adds the option 82 information to packets it receives from clients, then forwards the packets to the DHCP server. The DHCP server uses the option 82 information to decide which IP address to assign to the client—the DHCP server might also use information in the option 82 field for additional purposes, such as determining which services to grant to the client. The DHCP server sends its reply back to the DHCP relay, which removes the option 82 information field from the message, and then forwards the packet to the client.

The option 82 information is made up of a sequence of suboptions. JUNOS software supports the following DHCP relay agent information suboptions.

- Agent Circuit ID (suboption 1)—An ASCII string that identifies the interface on which a client DHCP packet is received.
- Agent Remote ID (suboption 2)—An ASCII string assigned by the relay agent that securely identifies the client.
- Vendor-Specific (suboption 9)—The JUNOS software data field, which contains the Internet Assigned Numbers Authority (IANA) enterprise number (4874) used by JUNOS software and either or both the layer 2 circuit ID and the user packet class.
 - Layer 2 Circuit ID (type 1)—The hexadecimal representation of the layer 2 identifier in the Agent Circuit ID (suboption 1) value (for example, the ATM VPI/VCI or Ethernet SVLAN/VLAN ID.) You can configure this suboption type without the Agent Circuit ID.
 - User Packet Class (type 2)—The hexadecimal representation of the user packet class field, whose value is assigned by the layer 2 policy application. The layer 2 policy application can be used to map the DHCP packet or message IEEE 802.1p value to the user packet class field. See the [JUNOS Policy Management Configuration Guide](#) for information about layer 2 policies.

The Agent Circuit ID suboption (suboption 1) and the Agent Remote ID suboption (suboption 2) are typically determined by the client network access device and depend on the network configuration. The Vendor-Specific suboption (suboption 9) is more flexible and can be used by administrators to associate specific data with the DHCP messages relayed between the DHCP relay and the DHCP server. For example the Vendor-Specific suboption can include the client's IEEE 802.1p value, which identifies the client's user priority.



NOTE: The DHCP relay agent replaces any existing Vendor-Specific value in the client packet with the relay agent's value.

The JUNOS software provides two commands that you can use to configure DHCP relay agent information suboptions.

- The **set dhcp relay agent sub-option** command—Enables you to configure option 82 to include any combination of the supported suboptions, including the Vendor-Specific suboption.
- The **set dhcp relay agent** command—Enables you to configure option 82 to include either or both the Agent Circuit ID suboption (suboption 1) and Agent Remote ID suboption (suboption 2). The command does not support the Vendor-Specific suboption (suboption 9).



NOTE: The **set dhcp relay agent** command is a legacy command, which JUNOS software continues to support to provide backward-compatibility for existing scripts. We recommend that all new configurations use the **dhcp relay agent sub-option** command.

The **set dhcp relay agent sub-option** command enables you to manage specific option 82 suboptions without impacting the configuration of other suboptions. The legacy **set dhcp relay agent** command, however, changes the configuration of suboptions in some cases.

Table 35 indicates the effect each command has on enabling or disabling relay agent information suboptions.

Table 35: Effect of Commands on Option 82 Suboption Settings

Command	Suboption and Status		
	Agent Circuit ID	Agent Remote ID	Vendor-Specific
set dhcp relay agent sub-option circuit-id	Enable	No change	No change
set dhcp relay agent sub-option remote-id	No change	Enable	No change
set dhcp relay agent sub-option vendor-specific <i>suboption-type</i>	No change	No change	Enable specified suboption type
no set dhcp relay agent sub-option circuit-id	Disable	No change	No change
no set dhcp relay agent sub-option remote-id	No change	Disable	No change
no set dhcp relay agent sub-option vendor-specific <i>suboption-type</i>	No change	No change	Disable specified suboption type
set dhcp relay agent	Enable	Enable	Not supported
set dhcp relay agent circuit-id-only	Enable	Disable	Not supported
set dhcp relay agent remote-id-only	Disable	Enable	Not supported
no set dhcp relay agent	Disable	Disable	Disable

Example 2—The Vendor-Specific suboption for a VLAN ID of 135-2468 (0x87-0x09a4, format <SVLAN ID> - <VLAN ID>) and a UPC of 5 is formatted as follows:

```
09 0e 00 00 13 0a 09 01 04 00 87 09 a4 02 01 05  
| | | | | | | | | | | | | |  
| | | | | | | | | | | | | | UPC val: 5  
| | | | | | | | | | | | | | UPC len: 1 byte  
| | | | | | | | | | | | | | UPC type: 2  
| | | | | | | | L2 Circuit ID val: 00 87 09 a4  
| | | | | | | | L2 Circuit ID len: 4 bytes  
| | | | | | | | L2 Circuit ID type: 1  
| | | | | | JUNOSE data len: 9 bytes  
| | | JUNOSE IANA: 13 0a  
| subopt 9 len: 14 bytes  
subopt code: 9
```

Example 3—The Vendor-Specific suboption for a VPI/VCI of 123.45678 (0x7b.0xb26e, format <VPI> . <VCI>) and a UPC of 5 is formatted as follows:

[illegible]

```
set dhcp relay agent
```

- Use to enable support for DHCP relay agent option, which includes the option 82 suboptions—Agent Circuit ID (suboption 1) and Agent Remote ID (suboption 2). This command does not support the Vendor-Specific option (suboption 9).



NOTE: This command, when used to configure option 82 suboptions is a legacy command, which JUNOS software continues to support to provide backward-compatibility for existing scripts. We recommend that you use the **dhcp relay agent sub-option** command for new option 82 suboption configurations.

- The suboptions include information from the DHCP relay agent that the DHCP server can use to implement parameter assignment policies. The DHCP server echoes the suboptions when it replies to the client—the DHCP relay agent can optionally strip the option 82 information before relaying the packets to the client. (Use the CLI command **set dhcp relay preserve-trusted-client-option** to configure this behavior for trusted clients.)
- When you issue the **set dhcp relay agent** command, the router adds the configured DHCP relay agent information suboptions to every packet it relays from a DHCP client to a DHCP server.

- The **circuit-id-only** keyword specifies the Agent Circuit ID suboption, which contains the following information, based on interface type. This keyword disables support for the Agent Remote ID suboption.
 - ATM interfaces

`< interface type > < slot > / < port > . < sub-if > : < vpi > : < vci >`

For example: `atm4/1.2:0.101`
 - VLAN interfaces

`< interface type > < slot > / < port > . < sub-if > : < vlan id >`

For example: `gigabitEthernet1/2.3:4`
 - Stacked VLAN interfaces

`< interface type > < slot > / < port > . < sub-if > : < svlan id > - < vlan id >`

For example: `gigabitEthernet1/2.3:4-5`
- The **remote-id-only** keyword specifies the Agent Remote ID suboption, which contains a value only when (1) the interface is a dynamic ATM interface and (2) the **subscriber** command is used to configure a username and domain name for the interface. If both conditions are met, the suboption contains a string with the username and domain name in the format: *username@domainname*. The **remote-id-only** keyword disables support for the Agent Circuit ID suboption.
- If you do not explicitly specify the **circuit-id-only** or **remote-id-only** keyword, both suboptions are used.
- Example


```
host1(config)#set dhcp relay agent circuit-id-only
```
- Use the **no** version to disable the addition of the DHCP relay agent information.

set dhcp relay agent sub-option

- Use to enable support for a specific DHCP relay agent option 82 suboption—Agent Circuit ID (suboption 1), Agent Remote ID (suboption 2), and Vendor-Specific (suboption 9).



NOTE: We recommend that you use the **set dhcp relay agent sub-option** command for new option 82 suboption configurations. However, JUNOS software continues to support the **set dhcp relay agent** command, with option 82 suboptions, to provide backward-compatibility for existing scripts.

- When you issue this command and certain conditions are met, the router adds the DHCP relay agent information suboptions to every packet it relays from a DHCP client to a DHCP server.
- The suboptions include information from the DHCP relay agent that the DHCP server can use to implement parameter assignment policies. The DHCP server echoes the suboptions when it replies to the DHCP client, but the DHCP relay strips the suboptions before relaying the packets to the client.

- The Agent Circuit ID suboption identifies the interface on which the DHCP Discover or Request packet was received. This suboption contains the following information, based on interface type:
 - ATM interfaces

`< interface type > < slot > / < port > . < sub-if > : < vpi > : < vci >`

For example: `atm4/1.2:0.101`
 - VLAN interfaces

`< interface type > < slot > / < port > . < sub-if > : < vlan id >`

For example: `gigabitEthernet1/2.3:4`
 - Stacked VLAN interfaces

`< interface type > < slot > / < port > . < sub-if > : < svlan id > - < vlan id >`

For example: `gigabitEthernet1/2.3:4-5`
- The Agent Remote ID suboption contains a value only when (1) the interface is a dynamic ATM interface and (2) the **subscriber** command is used to configure a username and domain name for the interface. If both conditions are met, the suboption contains a string with the username and domain name in the format: *username@domainname*.
- The Vendor-Specific suboption contains a value that includes a JUNOS data field. You can configure the data field to support one or both of the following values:
 - **layer2-circuit-id** (type 1)—The hexadecimal representation of the layer 2 identifier in the Agent Circuit ID (suboption 1) value (for example, the ATM VPI/VCI or Ethernet SVLAN/VLAN ID). You can configure this suboption type without the Agent Circuit ID.
 - **user-packet-class** (type 2)—The hexadecimal representation of the user packet class field, whose value is assigned by the layer 2 policy application. The layer 2 policy application can be used to map the DHCP packet or message IEEE 802.1p value to the user packet class field. See the [JUNOS Policy Management Configuration Guide](#) for information about layer 2 policies.
- Example 1

`host1(config)#set dhcp relay agent sub-option circuit-id`
- Example 2

`host1(config)#set dhcp relay agent sub-option vendor-specific user-packet-class`
- Use the **no** version to disable the addition of the specified DHCP option 82 suboption.

Configuration Example—Using DHCP Relay Option 82 to Pass IEEE 802.1p Values to DHCP Servers

Using the DHCP relay agent option 82 feature, you can configure an environment in which a customized DHCP server assigns an IP address that provides the desired service to the DHCP client.

The DHCP server uses information based on the IEEE 802.1p values, which are extracted from the DHCP packets using JUNOS software layer 2 policies, to determine the appropriate IP address to assign to the client.

This type of environment, which is illustrated in [Figure 11](#), includes the following components:

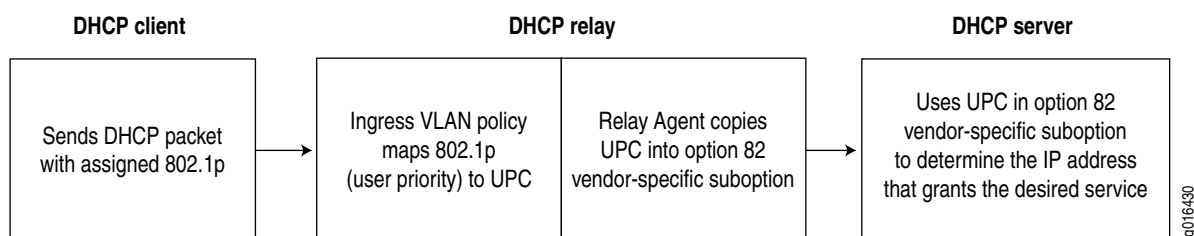
- Layer 2 policy on the ingress interface (that is, the interface that receives the client's DHCP packet) that maps the 802.1p value from the packet to a user packet class (UPC.)



NOTE: To ensure optimal performance when mapping 802.1p values to UPCs, order the classifier groups in the VLAN policy list with the most often used UPC values listed first.

- DHCP relay agent option 82 configuration that enables Vendor-Specific suboption type 2 (User Packet Class) support and maps the Layer 2 policy user packet class to the option 82 user packet class suboption.
- Customized DHCP server configuration that assigns IP addresses based on the option 82 user packet class suboption. The IP address is associated with the appropriate quality, type, or class of service for the user packet class specified in the option 82 suboption.

Figure 11: Passing 802.1p Values to the DHCP Server



The following example describes a sample procedure that creates an environment that passes 802.1p values to the DHCP server, which then assigns an IP address that enables the desired service to the DHCP client.

1. Configure a layer 2 policy that maps 802.1p values to user packet class values for a VLAN interface.

```

host1(config)# vlan classifier-list dot1p0 user-priority 0
host1(config)# vlan classifier-list dot1p1 user-priority 1
host1(config)# vlan classifier-list dot1p2 user-priority 2
host1(config)# vlan classifier-list dot1p3 user-priority 3
host1(config)# vlan classifier-list dot1p4 user-priority 4
host1(config)# vlan classifier-list dot1p5 user-priority 5
  
```

```

host1(config)# vlan classifier-list dot1p6 user-priority 6
host1(config)# vlan classifier-list dot1p7 user-priority 7
host1(config)# vlan policy-list dot1pToUpc
host1(config-policy-list)# classifier-group dot1p0
host1(config-policy-list-classifier-group)# user-packet-class 0
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)# classifier-group dot1p1
host1(config-policy-list-classifier-group)# user-packet-class 1
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)# classifier-group dot1p2
host1(config-policy-list-classifier-group)# user-packet-class 2
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)# classifier-group dot1p3
host1(config-policy-list-classifier-group)# user-packet-class 3
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)# classifier-group dot1p4
host1(config-policy-list-classifier-group)# user-packet-class 4
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)# classifier-group dot1p5
host1(config-policy-list-classifier-group)# user-packet-class 5
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)# classifier-group dot1p6
host1(config-policy-list-classifier-group)# user-packet-class 6
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)# classifier-group dot1p7
host1(config-policy-list-classifier-group)# user-packet-class 7
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
host1(config)# profile atm1483BaseProfile
host1(config-profile)# vlan policy input dot1pToUpc statistics enabled
host1(config-profile)#exit
host1(config)#

```

2. (Optional) Verify the policy list configuration.

```

host1(config)# run show policy-list dot1pToUpc

```

```

Policy Table
-----
VLAN Policy dot1pToUpc
Administrative state: enable
Reference count: 1
Classifier control list: dot1p0, precedence 100
user-packet-class 0
Classifier control list: dot1p1, precedence 100
user-packet-class 1
Classifier control list: dot1p2, precedence 100
user-packet-class 2
Classifier control list: dot1p3, precedence 100
user-packet-class 3
Classifier control list: dot1p4, precedence 100
user-packet-class 4
Classifier control list: dot1p5, precedence 100
user-packet-class 5
Classifier control list: dot1p6, precedence 100
user-packet-class 6
Classifier control list: dot1p7, precedence 100
user-packet-class 7

Referenced by interface(s):
None

```

Referenced by profile(s):

atm1483BaseProfile input policy, statistics enabled

Referenced by merged policies:

None

3. Configure the DHCP relay to use the option 82 suboptions. This configuration includes the command that specifies the mapping of the user packet class values from the layer 2 policy to the user-packet-class type in the option 82 Vendor-Specific suboption.

```
host1(config)# set dhcp relay 192.168.32.1 proxy
host1(config)# set dhcp relay 192.168.32.2
host1(config)# set dhcp relay agent sub-option circuit-id
host1(config)# set dhcp relay agent sub-option remote-id
host1(config)# set dhcp relay agent sub-option vendor-specific
user-packet-class
host1(config)# set dhcp relay agent sub-option vendor-specific
layer2-circuit-id
host1(config)# set dhcp relay options hostname
host1(config)# set dhcp relay options exclude-subinterface-id
host1(config)# set dhcp relay inhibit-access-route-creation
host1(config)# set dhcp relay trust-all
host1(config)# set dhcp relay override agent-option
```

4. (Optional) Verify the DHCP Relay configuration.

```
host1(config)# run show dhcp relay

DHCP Relay Configuration
-----
Mode: Proxy
  Restore Client Timeout: 72
  Inhibit Access Route Creation: off
  Assign Giaddr to Source IP: off
  Layer 2 Unicast Replies: off
  Giaddr Selects Interface: off
  Relay Agent Information Option (82):
    Override Giaddr: off
    Override Option: on
    Trust All Clients: on
    Preserve Option From Trusted Clients: off
    Circuit-ID Sub-option (1): on
      select - hostname
      select - exclude-subinterface-id
    Remote-ID Sub-option (2): on
    Vendor-Specific Sub-option (9): on
      select - layer2-circuit-id
      select - user-packet-class

DHCP Server Addresses
-----
192.168.32.1
192.168.32.2
```


Configuring DHCP Relay Proxy

The DHCP relay proxy is an enhancement to the E-series router's DHCP relay component. The DHCP relay proxy manages host routes for DHCP clients, and determines which offer to use when there are multiple DHCP servers configured.

After you are in DHCP relay proxy mode, all **set dhcp relay** commands are supported. The relay proxy also enables you to set timeout values related to handling DHCP client host routes after a reboot and to display related **show** command statistics.



NOTE: The E-series router configured as a DHCP relay proxy must be the first hop from the DHCP client. If it is not the first hop, the router defaults to the DHCP relay configuration.

Managing Host Routes

The DHCP relay proxy feature enables the E-series router to efficiently manage host routes for DHCP clients, including:

- Installing routes when DHCP clients are configured
- Removing routes when DHCP clients release their DHCP-assigned addresses or when the addresses expire

When a DHCP client sends a request to an external DHCP server, the relay proxy receives the request and forwards it to the external DHCP server. The relay proxy then sends the DHCP server's response back to the client. This process is similar to that used by the DHCP relay component. The DHCP client views the relay proxy as a DHCP server, and the DHCP server sees the relay proxy as a DHCP relay agent.

To DHCP clients, there is no difference when they use a DHCP relay or a DHCP relay proxy. However, the DHCP relay proxy differs from the DHCP relay in how client address renewals and releases are handled:

- With the DHCP relay proxy, DHCP clients communicate with the relay proxy to renew and release addresses.
- With the DHCP relay, DHCP clients communicate directly with the DHCP server to renew and release addresses.

A major benefit of the relay proxy configuration is that the E-series router is kept informed of the status of a DHCP client's address. When addresses are released by clients, the router removes the installed host route for that client. In the DHCP relay configuration, the router does not know when addresses have been renewed or released; the host routes that are no longer needed are still unavailable.

For additional information on managing client bindings, see [Viewing and Deleting DHCP Client Bindings](#) on page 371.

Selecting the DHCP Server Response

Similar to the DHCP relay, the DHCP relay proxy enables you to specify up to five DHCP servers to provide address and configuration information for a DHCP client. As an added benefit over the relay, when using multiple DHCP external servers, you can configure how the DHCP relay proxy determines which offer to send to the DHCP client. You can configure the DHCP relay proxy to use either the single best offer or the first offer it receives from the DHCP servers.

If there are multiple offers, the DHCP relay proxy selects the final offer based on the following priorities:

1. The offer that contains the IP address requested by the DHCP client.
2. The offer that contains an IP address on the same subnetwork as the requested IP address.
3. The offer that has the longest lease time.

If you have enabled the optional select-first-offer feature, the DHCP relay proxy immediately uses the first offer that it receives from any DHCP server.

Behavior for Bound Clients and Address Renewals

When a DHCP client is already bound to an IP address or is renewing the lease on its IP address, DHCP relay proxy unicasts DHCP ACK and DHCP NAK replies to the client regardless of the current configuration of the **set dhcp relay layer2-unicast-replies** command or the **set dhcp relay broadcast-flag-replies** command. These commands control the transmission method used for DHCP reply packets.

This behavior applies only to DHCP relay proxy; it does not apply to DHCP relay because DHCP relay does not maintain a list of active clients or receive address renewal requests from clients.

For information about using the **set dhcp relay layer2-unicast-replies** command, see [Configuring Layer 2 Unicast Transmission Method for Reply Packets to DHCP Clients](#) on page 321. For information about using the **set dhcp relay broadcast-flag-replies** command, see [Using the Broadcast Flag Setting to Control Transmission of DHCP Reply Packets](#) on page 322.

set dhcp relay proxy

- Use to enable DHCP relay proxy and to specify an IP address for the DHCP server. After you are in DHCP relay proxy mode, all **set dhcp relay** commands are supported.
- When you issue this command, the router adds the IP address to the list of DHCP servers (up to five) and forwards all request packets to all configured servers.
- Example

```
host1(config)#set dhcp relay 192.168.29.10 proxy
```
- Use the **no** version to remove the specified DHCP server or to remove all servers if no IP address is specified.

set dhcp relay proxy send-first-offer

- Use to specify that the DHCP relay proxy uses the first offer it receives from any configured DHCP server and sends that offer to the DHCP client.
- Example

```
host1(config)#set dhcp relay proxy send-first-offer
```
- Use the **no** version to restore the default setting, in which the DHCP relay proxy sends the most appropriate offer it receives from the configured DHCP servers to the DHCP client.

set dhcp relay proxy timeout

- Use to set the amount of time, in the range 1–168 hours, that the DHCP relay proxy waits for a renewal message from DHCP clients after a router reboot or switchover occurs. If no renewal message is received before the timeout expires, the relay proxy declares the client no longer active and removes the client's host route.



NOTE: DHCP relay proxy does not remove a DHCP client's host route when the lease for the client's IP address expires. DHCP relay proxy will instead remove the host route when the relay proxy timeout expires. To prevent a host route from remaining long after lease expiration, modify the relay proxy timeout from its default setting of 72 hours to a setting close to, but not less than the lease time.

- A renewal message from a DHCP client is required when a router reboot or switchover occurs.
- Example

```
host1(config)#set dhcp relay proxy timeout 8
```
- Use the **no** version to restore the default setting, 72 hours (3 days).

Configuring DHCP Local Server

You can use DHCP to configure the router to allow remote access to non-PPP clients. DHCP-based access is also an alternative to PPP in environments such as Public Wireless LANs (PWLANS). In PWLANS, a user scans for available broadband networks, then is redirected to a web-based authentication mechanism to request service.

DHCP provides address assignment information for users. Authentication, authorization, and accounting are separate processes, and are up to the Internet service provider (ISP) to define.

The DHCP local server can configure a client with the following DHCP options:

- Default router
- DNS server
- Domain name
- Lease time

- Grace period for address lease
- NetBIOS name server
- NetBIOS node type
- Subnet mask

For additional information on managing client bindings, see [Viewing and Deleting DHCP Client Bindings](#) on page 371.



NOTE: You cannot configure both the DHCP local server and one of the following in the same virtual router: DHCP external server, DHCP relay, or DHCP relay proxy. If you issue the **set dhcp relay** command when a local server has been configured, the local server is deactivated.

DHCP Local Server Modes

The router offers an embedded DHCP server, known as the DHCP local server. The DHCP local server has two modes: equal-access and standalone.



NOTE: E-series routers also support an embedded DHCP version 6 (DHCPv6) local server. The DHCPv6 local server provides a subset of the features of the DHCP local server. For information about configuring the DHCPv6 local server, see [DHCPv6 Local Server](#) on page 341.

- In equal-access mode, the DHCP local server works with the Juniper Networks SDX software to provide an advanced subscriber configuration and management service.
- In standalone mode, the DHCP local server provides a basic DHCP service, and also allows you to configure AAA authentication for incoming DHCP clients. Also, after successful authentication, the DHCP local server uses the information in the client's AAA subscriber record together with the client's DHCP parameters to select the IP address pool used for address assignment.

DHCP local server also supports RADIUS accounting, including interim accounting, in standalone mode. This feature allows you to use RADIUS start and stop attributes to track user events such as the lifetime of an IP address.

DHCPv6 Local Server

In addition to the embedded DHCP local server that is used for IP version 4 (IPv4) address support, E-series routers includes an embedded DHCPv6 local server. This server enables the router to function as a server for the DHCP protocol for IP version 6 (IPv6). The DHCPv6 local server sends and receives packets via IPv6 and informs IPv6 of the routing requirements of the router clients.

The DHCPv6 local server provides the following IPv6 address support:

- Delegates IPv6 prefixes to client routers; each client can have one prefix; prefixes and DNS information can be locally configured or derived from RADIUS via AAA.
- Provides DNS server information to directly connected router clients.



NOTE: You must add a vendor-specific attribute to RADIUS to enable E-series routers to retrieve IPv6 Domain Name System (DNS) addresses.

Equal-Access Mode

In equal-access mode, the router enables access to non-PPP users. Non-PPP equal access requires the use of the router’s DHCP local server and SDX software, which communicates with a RADIUS server.

The DHCP local server performs the following functions in equal-access mode:

- Communicates with SDX software.
- Assigns an IP address that enables the subscriber to access services.

Local Pool Selection and Address Allocation

The DHCP local server selects a DHCP pool from which to allocate an address using the framed IP address or pool name parameters. The router compares the parameters with the local DHCP pools in the order presented in Table 36. When the router finds a match, it selects a pool based on the match and does not examine other parameters.

Table 36: Local Pool Selection in Equal-Access Mode

Field	How the DHCP Local Server Uses the Field
Framed IP address	The client’s RADIUS entry can be configured with a framed IP address, which the DHCP local server can get from the SDX software. If the router selects a pool using a framed IP address, the DHCP local server attempts to allocate the framed IP address from the pool. If the framed IP address is not available, then the server allocates the next available address in the pool to the client.
Pool name	Each DHCP local pool has a pool name. The client’s RADIUS entry can also be configured with a pool name, which the DHCP local server can get from the SDX software. The SDX software must be configured to send RADIUS attributes to DHCP.
Domain name	You can use a domain name as the name of a DHCP local pool. If the client logs onto the SDX application and RADIUS authenticates the client using a domain name, the DHCP local server receives the domain name from the SDX software. If the client’s domain name does not match the name of the DHCP local pool, the router attempts to match the client’s domain name to the domain name field within the pool.
Giaddr	A DHCP local pool is configured with a network address. A gateway IP address (giaddr), which indicates a client’s subnet, can be presented to the DHCP local server in the client’s DHCP request message. The giaddr field in the DHCP request message usually contains the IP address of a DHCP relay server. The router attempts to match the giaddr address in the DHCP request message with the network address of a DHCP local pool.

The Connection Process

The following sequence describes how the subscriber connects to the network for the first time using equal-access mode. Figure 12 illustrates the process.

1. The subscriber's computer boots and issues a DHCP request.
2. The DHCP local server uses the SDX client to issue a COPS request to retrieve address pool information.
3. After standard DHCP negotiations, the DHCP local server supplies an IP address to the subscriber's computer from a local address pool, as described in the previous section.

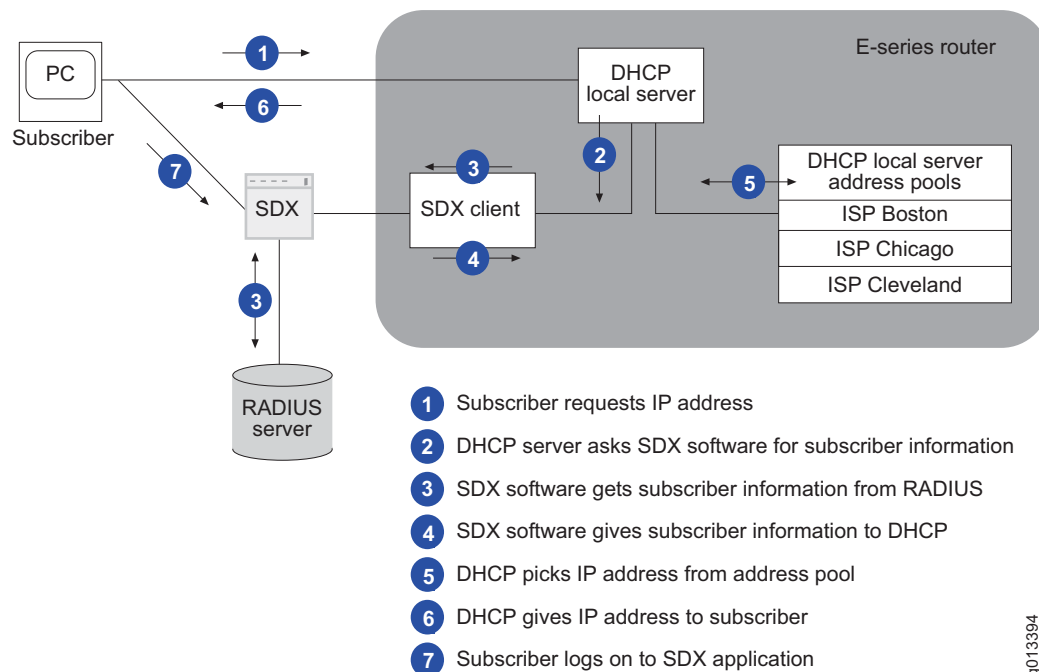
The router maintains a host route that maps the IP address to the router's interface associated with the subscriber's computer.

4. The subscriber's computer retains the IP address until the subscriber turns off the computer.



NOTE: If a DHCP client attempts to renew its address and the DHCP server receives the request on a different interface than the interface that the client originally used, the DHCP server sends a NAK message to the client, forcing the client to begin the DHCP connection process again.

Figure 12: Non-PPP Equal Access via the Router



g013394

Standalone Mode

In standalone mode, the DHCP local server operates as a basic DHCP server. Clients are not authenticated by default; however, you can optionally configure the DHCP local server to use AAA authentication for the incoming clients. The DHCP local server receives DHCP client requests for addresses, selects DHCP local pools from which to allocate addresses, distributes addresses to the clients, and maintains the resulting DHCP bindings in a server management table.

Local Pool Selection and Address Allocation

In standalone mode, the DHCP local server selects a pool to allocate an address for a client; the SDX application is never notified or queried. The process used depends on whether AAA authentication is configured.

- If AAA authentication is not configured, the DHCP local server selects a pool by matching the local pool network address to the giaddr or the received interface IP address. The router first attempts to match the giaddr to a local pool network address. If it does not find a match, the router attempts to match the received interface IP address to a local pool network address.
 - Giaddr—A giaddr, which indicates a client's subnetwork, can be presented to the DHCP local server in the client DHCP REQUEST message. The giaddr field in the DHCP request message usually contains the IP address of a DHCP relay server. The router attempts to match the giaddr address in the DHCP request message with the network address of a DHCP local pool. If it finds a match, the router uses the matching DHCP local pool.
 - Received interface IP address—The router uses the IP address of the interface on which the DHCP packet is being processed.

After the router selects a DHCP local pool, the DHCP local server first tries to find a reserved IP address for the client in the selected pool. If no reserved address is available, the router attempts to allocate a client's requested IP address. If the requested IP address is not available, the router allocates the next available address in the pool. If a grace period is configured for the pool, the router assigns the grace period to the allocated address.

- If AAA authentication is configured (as described in [Configuring AAA Authentication for DHCP Standalone Mode](#) on page 356) and the authentication is successful, the local server selects an IP address pool based on the following precedence:
 1. If AAA specifies an IP address, the DHCP local server finds the address pool containing the address, then allocates that address.
 2. If AAA specifies an address pool name, the local server finds the pool with the matching name and allocates an address from that pool.
 3. The local server finds the address pool whose name matches the client's domain.
 4. The local server finds the address pool whose domain name matches the client's domain.

5. The local server finds the address pool whose IP network matches the client's DHCP giaddr.
6. The local server finds the address pool whose interface matches the interface on which the client's DHCP request was received.

Server Management Table

For each client that makes requests of the DHCP local server, the router keeps an entry in the server management table. The entry defines client-specific information and state information. The router uses this table to identify clients when it receives subsequent messages and to maintain the state of each client within the DHCP protocol. In addition, the table contains information that may be transferred to and from the SDX software.

Linking Local Address Pools

In both equal-access mode and standalone mode, you can link a DHCP local pool to another local pool. The linked pool serves as a backup pool. If no addresses are available in a pool, the DHCP local server attempts to allocate an address from the linked pool. The address pools that are linked are viewed as a group.

DHCP Local Server Event Logs

To troubleshoot and monitor your DHCP local server, use the following system event logs:

- dhcpLocalClients—DHCP local server client events and duplicate MAC address detection
- dhcpLocalGeneral—DHCP local server infrastructure-related events and number of client threshold events



NOTE: The dhcpLocalGeneral category replaces the dhcpLocalServerGeneral category.

- dhcpLocalHighAvailability—DHCP high availability events
- dhcpLocalPool—DHCP local address pool events, including normal, linked, and shared pools
- dhcpLocalProtocol—DHCP local server protocol events

See the [JUNOS System Event Logging Reference Guide](#) for additional information about the DHCP local server logs.

DHCP Local Server SNMP Traps

The DHCP local server supports configurable global SNMP traps that monitor events related to the DHCP local server and local SNMP traps that are related to address pool utilization.

The DHCP local server's global SNMP trap generates severity level 1 (alert), 2 (critical), and 3 (error) events. This trap helps administrators monitor DHCP local server general health, error statistics, address lease status, and protocol events.

The DHCP local server's global SNMP trap generates a severity level 4 (warning) event when a duplicate MAC address is detected.

Use the following command to enable the global SNMP traps for DHCP local server.

```
host1(config)#ip dhcp-local snmpTraps
```

The global SNMP trap information is captured in the dhcpLocalGeneral logging category.

SNMP also traps events related to address pool utilization. You use the **warning** command to define the maximum and minimum threshold values and the **snmpTrap** command to generate traps when utilization occurs above or below the defined values.

```
host1(config-dhcp-local)#warning 50 40
host1(config-dhcp-local)#snmpTrap
```

For linked or shared pools, SNMP treats the members of the pool as a group, and uses the values configured for the first pool in the chain as the group's threshold.

The address pool utilization SNMP trap information is captured in the dhcpLocalPool logging category.



NOTE: You must configure your SNMP management client to read the MIB objects, and your SNMP trap collector must be capable of decoding the new traps. For information about setting up SNMP, see [JUNOS System Basics Configuration Guide, Chapter 4, Configuring SNMP](#).

Before You Configure DHCP Local Server

Before you configure DHCP local server, you need to configure interfaces. You can configure ATM or Ethernet interfaces for DHCP local server. These interfaces can be numbered or unnumbered. Because subscribers connect to the router from different subnetworks, you must configure an IP address for each subnetwork on the interface. This action provides connectivity between the subnetwork and the router.

To configure a numbered IP address for DHCP local server:

1. Select an ATM or Ethernet interface.
2. Assign the primary IP address for one subnetwork to this interface.
3. Assign secondary IP addresses for all other subnetworks to this interface.

To configure an unnumbered IP address for DHCP local server:

1. Specify a loopback interface.
2. Assign the primary IP address for one subnet to the loopback interface.
3. Assign secondary IP addresses for all other subnets to the loopback interface.
4. Select an ATM or Ethernet interface.
5. Configure an unnumbered IP address associated with the loopback interface on the ATM or Ethernet interface.

For information about defining IP addresses, see [JUNOS IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP](#).

Configuration Tasks

This section covers the configuration tasks for equal-access and standalone modes. Perform the appropriate procedure:

1. For both equal-access and standalone modes, configure the DHCP local server. See [Configuring the DHCP Local Server](#) on page 347 for a sample configuration.
2. For standalone mode, optionally configure the router to use AAA authentication for DHCP requests from subscribers. See [Configuring AAA Authentication for DHCP Standalone Mode](#) on page 356 for a sample configuration.
3. For non-PPP equal access, configure the router to work with the SDX application. See [Configuring the Router to Work with the SDX Application](#) on page 361 for a sample configuration.

Configuring the DHCP Local Server

To configure the DHCP local server:

1. Enable the DHCP local server for either equal-access or standalone mode.

```
host1(config)#service dhcp-local equal-access
host1(config)#service dhcp-local standalone
```

2. (Optional) Specify the maximum number of IP addresses that the DHCP local server can supply to each VPI/VCI, VLAN, Ethernet subnetwork, or to a particular interface or subinterface.

```
host1(config)#ip dhcp-local limit ethernet 6
```

3. Specify any addresses that the DHCP local server must not assign.

```
host1(config)#ip dhcp-local excluded-address 10.10.3.4
```

4. (Optional) Enable general DHCP local server traps.

```
host1(config)#ip dhcp-local snmpTraps
```

5. For both equal-access and standalone modes, configure the DHCP local server to supply IP addresses to subscribers who want to access a domain.

- a. Access DHCP Local Pool Configuration mode for the local address pool.

```
host1(config)#ip dhcp-local pool ispBoston
host1(config-dhcp-local)#
```

- b. Specify the IP addresses that the DHCP local server can assign from the local address pool.

```
host1(config-dhcp-local)#network 10.10.0.0 255.255.0.0
```

- c. (Optional) Specify a DNS server.

```
host1(config-dhcp-local)#dns-server 10.10.1.1
```

- d. (Optional) Specify a NetBIOS server.

```
host1(config-dhcp-local)#netbios-name-server 10.10.1.1 10.10.1.2
```

- e. (Optional) Define threshold values for local address pool utilization.

```
host1(config-dhcp-local)#warning 50 40
```

- f. (Optional) Enable SNMP traps for local address pool utilization.

```
host1(config-dhcp-local)#snmpTrap
```

- g. Specify the router that will forward traffic from these IP addresses to destinations on other subnets.



NOTE: The default router must be on the same subnetwork as the local server pool IP addresses.

```
host1(config-dhcp-local)#default-router 10.10.1.3
```

- h. Specify the lease time for IP addresses.

```
host1(config-dhcp-local)#lease 0 0 24
```

- i. (Optional) Configure the grace period for addresses allocated from this local pool.

```
host1(config-dhcp-local)#grace-period 25 12
```

- j. (Optional) Specify that the grace period is also used for addresses that are explicitly released by clients.

```
host1(config-dhcp-local)#use-release-grace-period
```

- k. (Optional) Specify the type of NetBIOS server.

```
host1(config-dhcp-local)#netbios-node-type b-node
```

- l. (Optional) Specify a domain name that can be returned to the subscriber if requested.

```
host1(config-dhcp-local)#domain-name ispBoston
```

- m. (Optional) For DHCP standalone mode, reserve an IP address for a specific MAC address.

```
host1(config-dhcp-local)#reserve 10.10.13.8 0090.1a10.0552
```

- n. For DHCP standalone mode, set the DHCP server address that is sent to DHCP clients.

```
host1(config-dhcp-local)#server-address 10.10.20.8
```

6. (Optional) For both equal-access and standalone modes, link the local address pool to a backup address pool.

- a. Access DHCP Local Pool Configuration mode for the local address pool.

```
host1(config)#ip dhcp-local pool ispBoston  
host1(config-dhcp-local)#
```

- b. Link the current local address pool to another local address pool.

```
host1(config-dhcp-local)#link ispChicago
```

default-router

- Use to specify the IP address of the router for the subscriber's computer to use for traffic destined for locations beyond the local subnetwork.
- The default router must be on the same subnetwork as the local server pool IP addresses that you configure with the **network** command.
- Specify the IP address of a primary server, and optionally, specify the IP address of a secondary server.
- Example

```
host1(config-dhcp-local)#default-router 10.10.1.1
```

- Use the **no** version to remove the association between the address pool and the router.

dns-server

- Use to assign a DNS server to an address pool.
- Some DHCP clients request the DHCP local server to assign a DNS server.
- Example

```
host1(config-dhcp-local)#dns-server 10.10.1.1
```

- Use the **no** version to remove the association between the address pool and the DNS server.

domain-name

- Use to specify a domain name that can be returned to the subscriber if requested.
- The name of the domain must match the name you specified for the RADIUS vendor-specific attribute (VSA) and for authentication, authorization, accounting, and address assignment (AAAA).
- Example

```
host1(config-dhcp-local)#domain-name ispBoston
```
- Use the **no** version to remove the association between the address pool and the domain name.

ip dhcp-local auto-configure agent-circuit-identifier

- Use to configure the DHCP local server to support the creation of dynamic subscriber interfaces built over dynamic VLANs that are based on the agent-circuit-id option (suboption 1) of the option 82 field in DHCP messages.

The use of the option 82 field enables you to stack an IP interface that is associated with a particular subscriber over a dynamically created VLAN; the VLAN is dynamically created based on the agent-circuit-id option (suboption 1) that is contained in the DHCP option 82 field.

For information about configuring agent-circuit-id–based dynamic VLAN subinterfaces, see [JUNOS Link Layer Configuration Guide, Chapter 13, Configuring Dynamic Interfaces Using Bulk Configuration](#).
- Use this command within a specific virtual router context.
- This command requires that the user's DHCP control traffic and data traffic traverse the same client-facing ingress port on the E-series router.
- Example

```
host1(config)#ip dhcp-local auto-configure agent-circuit-identifier
```
- Use the **no** version to disable the autoconfigure feature.

ip dhcp-local excluded-address

- Use to specify IP addresses that you do not want the DHCP local server to supply from the default address pool because those addresses are already used by devices on the subnetwork.
- Specify a single IP address or a start-of-range IP address and an end-of-range IP address.
- Example

```
host1(config)#ip dhcp-local excluded-address 10.10.1.1
```
- Use the **no** version to enable the local server to supply the specified IP address.

ip dhcp-local limit

- Use to specify the maximum number of IP addresses that the DHCP local server can supply to each VPI/VCI, VLAN, Ethernet subnetwork, or to a particular interface or subinterface.
- You can set global limits for a given interface type, ATM, Ethernet, or VLAN. When you set a limit for any of these interface types, all interfaces of that type that are subsequently created, whether dynamically or statically, inherit that limit value.

You can also set an individual interface limit for a specific interface and override the global limit configured for that interface type. For example, suppose the VLAN interface type limit is five. You can specify a limit of 10 for the VLAN interface FastEthernet 1/0.100. All other VLAN interfaces retain the global limit of five.

The global limits for interface types and the individual interface limits set on static interfaces are kept in NVS. These values are restored during a switchover or a reload.

When you assign an individual limit to a dynamic interface, that limit is in force only until either a switchover or reload takes place. After the switchover or reload, if the action that caused the dynamic interface to be created occurs again, a new dynamic interface is created. The new dynamic interface then inherits the limit set by the global values based on the type of interface that is created.

- Example 1
host1(config)#**ip dhcp-local limit ethernet 6**
- Example 2
host1(config)#**ip dhcp-local limit interface atm 3/1 15**
- Use the **no** version to restore the default value as the maximum number of IP addresses that the DHCP local server can supply to each VPI/VCI, VLAN, Ethernet subnetwork, or to a particular interface or subinterface.



NOTE: Limits that you specify on dynamic interfaces are not restored after a switchover or reboot.

ip dhcp-local pool

- Use to access DHCP Local Pool Configuration mode.
- The DHCP local server uses pool names other than the default to maintain configuration information for subscribers to a particular domain.
- Example
host1(config)#**ip dhcp-local pool ispBoston**
- Use the **no** version to prevent the DHCP local server from supplying IP addresses from the specified pool.

ip dhcp-local snmpTraps

- Use to enable SNMP traps for DHCP local server general health, error statistics, address lease status, client per-interface thresholds, and protocol events.
- Traps are generated for severity level 1 (alert), 2 (critical), and 3 (error) events.



NOTE: You must configure your SNMP management client to read the MIB objects, and your SNMP trap collector must be capable of decoding the new traps. For information about setting up SNMP, see [JUNOS System Basics Configuration Guide, Chapter 4, Configuring SNMP](#).

- Example
host1(config)#**ip dhcp-local snmpTraps**
- Use the **no** version to disable SNMP traps for DHCP local server.

lease

- Use to specify the time period for which the supplied IP address is valid.
- Specify the number of days, and optionally, the number of hours, minutes, and seconds.
- Specify the keyword **infinite** to specify a lease that does not expire.
- Example
host1(config-dhcp-local)#**lease 0 0 24**
- Use the **no** version to restore the default lease time, one day.

link

- Use to link the DHCP local address pool being configured to another local address pool. If no addresses are available in the local pool, the DHCP local server attempts to allocate an address from the linked pool. The linked pools form a group.
- Example
host1(config-dhcp-local)#**link ispChicago**
- Use the **no** version to remove the link.

netbios-name-server

- Use to assign a NetBIOS server for subscribers.
- Specify the IP address of a primary server and, optionally, the address of a secondary server.
- Some DHCP clients request the DHCP local server to assign a NetBIOS server.
- Example
host1(config-dhcp-local)#**netbios-name-server 10.10.1.1 10.10.1.2**
- Use the **no** version to remove the association between the address pool and the NetBIOS server.

netbios-node-type

- Use to specify a NetBIOS node type.
- Specify one of the following types of NetBIOS servers:
 - **b-node**—Broadcast
 - **p-node**—Peer-to-peer
 - **m-node**—Mixed
 - **h-node**—Hybrid
- Example
`host1(config-dhcp-local)#netbios-node-type b-node`
- Use the **no** version to restore the default, in which the node type is unspecified.

network

- Use to specify the IP addresses that the DHCP local server can provide from an address pool.
- Example
`host1(config-dhcp-local)#network 10.10.1.0 255.255.0.0`
- Use the **no** version to remove the network address and mask.
- Specify the **force** keyword with the **no** version to delete the address pool even if the pool is in use.

reserve

- For standalone mode, use to reserve an IP address for a specific MAC address.
- Example
`host1(config-dhcp-local)#reserve 10.10.13.8 0090.1a10.0552`
- Use the **no** version to remove the reservation.

server-address

- For standalone mode, use to set the DHCP server address that is sent to DHCP clients.
- Example
`host1(config-dhcp-local)#server-address 10.10.20.0`
- Use the **no** version to remove the server address.

service dhcp-local

- Use to enable the DHCP local server to operate in either equal-access mode or standalone mode.
- Example
`host1(config)#service dhcp-local equal-access`
- Use the **no** version to disable the DHCP local server.

snmpTrap

- Use to enable Simple Network Management Protocol (SNMP) traps for local address pool utilization, including normal, linked, and shared address pools. Traps are generated based on threshold values for utilization. You can define threshold values by using the **warning** command.
- Example
host1(config-dhcp-local)#**snmpTrap**
- Use the **no** version to disable the SNMP traps for DHCP local pool utilization.

warning

- Use to define the maximum and minimum threshold values for local address pool utilization, including normal, linked, and shared pools. If you issue the **snmpTrap** command, SNMP traps are generated when utilization occurs above or below the specified threshold values.
- Example
host1(config-dhcp-local)#**warning 50 40**
- Use the **no** version to restore the default threshold values for DHCP local address pool utilization.

Configuring Grace Periods for Address Leases

The JUNOS software enables you to configure a grace period for a particular local address pool—the grace period is applied to all address leases associated with the address pool. The grace period is the amount of time that a client continues to retain its address lease after the lease expires or is released. An address cannot be assigned to any other client during the grace period. When the grace period expires, the address is released back to the address pool.

Grace periods help to ensure that a DHCP client retains its previously assigned IP address in situations that might normally cause a lease termination followed by a new address assignment. For example, if a client loses its lease due to a network disruption, the grace period enables the client to be reassigned the same address when the client requests an address after the network stabilizes. Grace periods are also useful during client reboots and in cases where a non-compliant or unreliable DHCP implementation triggers a lease renewal.

You configure a grace period for a local address pool. The grace period is immediately applied to all addresses that are allocated from the pool, including previously allocated addresses that are currently active—the new grace period takes precedence over a previously configured grace period for the address pool.



NOTE: Configuring a new grace period that is shorter than the address pool current grace period immediately terminates any existing address leases that are in the grace period state and that have already exceeded the length of the new grace period.

NOTE: An address continues to be counted against the address pool resources while in a grace period. For example, if the address pool is exhausted, a new address cannot be assigned to other clients.

Client address leases enter the grace period in two ways—the lease might expire or the address can be explicitly released by the client. In both cases the address remains unavailable to other clients and can only be reapplied to the original client during the grace period. The address is released back to the address pool if the grace period expires before the address is reapplied to the original client.

When you configure a grace period, by default it is applied to address leases that *expire*, but not to addresses that are *released* by clients. However, you can optionally apply the grace period to released addresses.

grace-period

- Use to configure a grace period for address leases allocated from the current DHCP local address pool.
- When the address lease expires, the address enters the *expired* state for the duration of the grace period. During the grace period, the address can only be reassigned to the original client and is unavailable to other clients.
- This command applies only to address leases that expire. Use the **use-release-grace-period** command to also apply the configured grace period to the local pool addresses that are explicitly released by clients.
- Specify the number of days and, optionally, the number of hours, minutes, and seconds in the grace period.
- Example

```
host1(config-dhcp-local)#grace-period 0 12
```
- Use the **no** version to restore the default, in which no grace period is associated with address allocated from the local address pool.

use-release-grace-period

- Use to apply the grace period configured for the DHCP local address pool to addresses that have been explicitly released by clients. By default, the grace period is applied only to addresses leases that expire, not to addresses that have been released.
- When a client releases an address, the address enters the *released* state for the duration of the grace period. During the grace period, the address can only be reassigned to the original client and is unavailable to other clients.
- Example

```
host1(config-dhcp-local)#use-release-grace-period
```
- Use the **no** version to restore the default, which disables the use of the grace period for released addresses.

Configuring AAA Authentication for DHCP Standalone Mode

The DHCP local server enables you to optionally configure AAA-based authentication of standalone mode DHCP clients. In addition to providing increased security, AAA authentication also provides RADIUS-based input to IP address pool selection for standalone mode clients. By default, clients are not authenticated in standalone mode.

Typically, an incoming DHCP client does not provide a username—therefore, the DHCP local server constructs a username based on the user's attachment parameters and optional DHCP parameters. AAA uses the constructed username to authenticate the incoming client and create the AAA subscriber record for the client. The information in the AAA subscriber record is then used to determine the IP address pool from which to assign the address for the DHCP client. You can include the following elements in the username:

Attachment Parameters	DHCP Parameters
domain	circuit ID
user prefix	circuit type
–	MAC address
–	option 82
–	virtual router name



NOTE: The nondomain portion of a constructed username must contain at least one character. Otherwise, the DHCP local server rejects the DHCP client without performing the AAA authentication request.

When using authentication, AAA accepts the DHCP client as a subscriber—this enables you to use **show** commands to monitor configuration information and statistics about the client. You can also use the **logout subscriber** command to manage subscribers.

To configure AAA-based authentication for DHCP local server standalone mode clients:



CAUTION: Configuring authentication on the DHCP local server requires that you first disable the DHCP local server for standalone mode. Doing so removes your entire DHCP local server configuration. Therefore, if you want to configure authentication, do so before you have otherwise configured the DHCP local server.

1. Disable the DHCP local server for standalone mode.

```
host1(config)#no service dhcp-local standalone
```

2. Enable authentication.

```
host1(config)#service dhcp-local standalone authenticate
```

3. Specify the password.

```
host1(config)#ip dhcp-local auth password to4tool8
```

4. Specify the elements to be included in the username.

```
host1(config)#ip dhcp-local auth domain ISP1.com
host1(config)#ip dhcp-local auth user-prefix ERX4-Boston
host1(config)#ip dhcp-local auth include virtual-router-name
host1(config)#ip dhcp-local auth include circuit-type
host1(config)#ip dhcp-local auth include circuit-identifier
```

5. (Optional) Verify your authentication configuration.

```
host1(config)#show ip dhcp-local auth config
```

DHCP Local Server Authentication Configuration

```
User-Prefix      : ERX4-Boston
Domain           : ISP1.com
Password         : to4Tool8
Virtual Router   : included
Circuit Type     : included
Circuit ID       : included
MAC Address      : excluded
Option 82        : excluded
```

ip dhcp-local auth domain

- Use to specify the domain for a username that is locally configured for a DHCP standalone mode client. The locally configured username is presented to AAA in an authentication request.

- Example

```
host1(config)#ip dhcp-local auth domain ISP1.com
```

- Use the **no** version to remove the domain.

ip dhcp-local auth include

- Use to include optional information as part of the locally configured username for a DHCP standalone mode client. The optional information becomes part of the AAA subscriber record, and is then used to determine the IP address pool from which to assign the address for the DHCP client.

- Use the following keywords to include specific information:

- **circuit-identifier**—Specifies the circuit identifier of the interface on which the DHCP client's request was received.
- **circuit-type**—Specifies the circuit type of the interface on which the DHCP client's request was received.
- **mac-address**—Specifies the DHCP client's MAC address.
- **option82**—Specifies the DHCP client's option 82 value.
- **virtual-router-name**—Specifies the DHCP local server's virtual router name.

- Example

```
host1(config)#ip dhcp-local auth include circuit-identifier
host1(config)#ip dhcp-local auth include circuit-type
host1(config)#ip dhcp-local auth include option82
```
- Use the **no** version to remove the specified optional information.

ip dhcp-local auth password

- Use to assign a password that authenticates a locally configured DHCP standalone mode client. In DHCP standalone mode, the password is presented to AAA in an authentication request.
- Example

```
host1(config)#ip dhcp-local auth password to4tooL8
```
- Use the **no** version to remove the password.

ip dhcp-local auth user-prefix

- Use to specify the user-prefix for a username that is locally configured for a DHCP standalone mode client. The locally configured username is presented to AAA in an authentication request.
- Example

```
host1(config)#ip dhcp-local auth user-prefix ERX4-Boston
```

Use the **no** version to remove the user-prefix.

service dhcp-local authenticate

- Use to enable the enable AAA-based authentication for DHCP local server standalone mode clients.
- Example

```
host1(config)#service dhcp-local standalone authenticate
```
- Use the **no** version to disable the DHCP local server authentication.

Differentiating Between Clients with the Same Client ID or Hardware Address

The JUNOS software includes an RFC-compliant feature that enables the DHCP local server to create unique client IDs to support roaming clients and to manage situations in which two clients in the network have the same hardware address.



NOTE: This feature replaces the previous DHCP local server client roaming and duplicate address support. The previously used **ip dhcp-local inhibit-roaming** command is deprecated and has no effect on the DHCP local server. The command is replaced by the **ip dhcp-local unique-client-ids** command.

You can configure the method DHCP local server uses when the router receives a DISCOVER or REQUEST packet that contains a client ID or hardware address that matches the ID or address of a currently bound client on another subnet.

In the default configuration, the DHCP local server uses the unique subnet portion of each client's DHCP client table key to support client roaming. When a new client, with a duplicate ID or hardware address, requests an address lease, DHCP assigns that client a new address and lease—the existing client's lease is unchanged.

In the optional configuration, you use the **ip dhcp-local unique-client-ids** to disable the use of subnet information to differentiate between clients with duplicate client IDs or hardware addresses. When DHCP receives the request from a duplicate ID or address, DHCP terminates the address lease for the existing client and returns the address to its original address pool. DHCP then assigns a new address and lease to the new client.

ip dhcp-local unique-client-ids

- Use to specify the method that DHCP local server uses to differentiate between two clients that have the same client ID or hardware address.
- We recommend that you enable this command only when duplicate client IDs and hardware addresses do not exist in your network.
- When this command is enabled and the router receives a DHCP DISCOVER or REQUEST packet with the same client ID or hardware address as a currently bound client, the request is always considered to be from a roaming client. The DHCP server terminates the currently bound client's lease, and assigns a new address to the requesting client.
- When this command is disabled, the router's default configuration provides an RFC-compliant method—DHCP local server uses the subnet portion of the client table key to differentiate between two clients that use the same client ID or hardware address. The DHCP server processes client requests in a standard manner.
- This command replaces the deprecated **ip dhcp-local inhibit-roaming** command.
- Any changes you make have no effect on currently bound clients.
- Example

```
host1(config)# ip dhcp-local unique-client-ids
```
- Use the **no** version to restore the RFC-compliant default behavior, which uses subnet information to differentiate between clients with duplicate client IDs or hardware addresses.

Logging Out DHCP Local Server Subscribers

You can use the **logout subscribers** command to log out DHCP local server subscribers. For example, you might use this feature if you want to force a user to request a new lease or if you want to recover functional resources. The **logout subscribers** command, unlike the **clear ip address binding** command (described in [Clearing an IP DHCP Local Server Binding](#) on page 360), does not terminate the subscriber's user session or management representation.

logout subscribers

- Use to log out DHCP local server subscribers.
- This command applies to DHCP local server local-access and standalone clients, as well as to PPP users.
- From Privileged Exec mode, you can log out **all** subscribers, or log out subscribers by **username**, **domain**, **virtual-router**, or **port**.
- Example

```
host1#logout subscribers username user195@isp1.com
```
- There is no **no** version.

Clearing an IP DHCP Local Server Binding

You can use the **clear ip dhcp-local binding** command to force the removal of a connected user's IP address lease and associated route configuration. Using this command enables you to:

- Recover functional resources from a user who has not explicitly terminated connectivity and whose lease is unexpired.
- Discontinue connectivity to a user, prompting or forcing the user to request a new lease in order to reestablish network connectivity.

clear ip dhcp-local binding

- Use to force the removal of a connected user's IP address lease and associated route configuration.



NOTE: This command is deprecated and might be removed completely in a future release. The function provided by this command has been replaced by the **dhcp delete-binding** command.

- Example

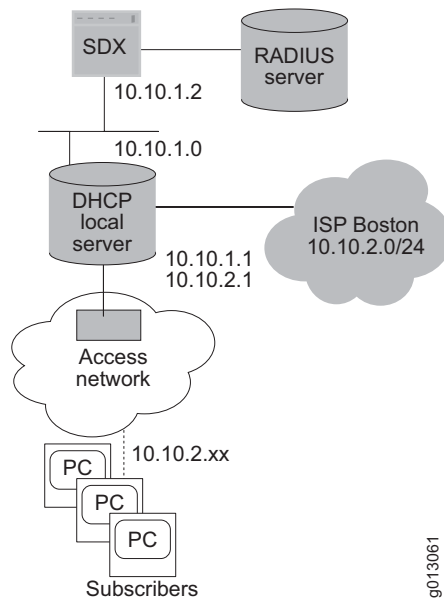
```
host1(config)#clear ip dhcp-local binding 10.10.20.41
```
- There is no **no** version.

Configuring the Router to Work with the SDX Application

E-series routers have an embedded SDX client that interacts with the SDX application. For information about configuring the SDX client, see [Configuring the SDX Client](#) in *Chapter 1, Configuring Remote Access*.

Configuration Example Figure 13 shows the scenario for this example. Subscribers obtain access to ISP Boston via a router. Subscribers log in through the SDX application, and a RADIUS server provides authentication.

Figure 13: Non-PPP Equal-Access Configuration Example



The following steps describe how to configure this scenario.

1. Configure interfaces on the router.

```
host1(config)#interface loopback 0
host1(config-if)#ip address 10.10.1.1 255.255.255.0
host1(config-if)#ip address 10.10.2.1 255.255.255.0 secondary
host1(config-if)#exit
host1(config)#interface fastEthernet 2/0
host1(config-if)#ip unnumbered loopback 0
```

2. Configure the parameters to enable the router to forward authentication requests to the RADIUS server.

```
host1(config)#radius authentication server 10.10.1.2
host1(config)#udp-port 1645
host1(config)#key radius
```


3. Specify the authentication method.

```
host1(config)#aaa authentication ppp default radius
```

Or

```
host1(config)#aaa authentication ppp default none
```

4. Enable the DHCP local server.

```
host1(config)#service dhcp-local
```

5. Specify the IP addresses that are in use, so that the DHCP local server cannot assign these addresses.

```
host1(config)#ip dhcp-local excluded-address 10.10.1.1
host1(config)#ip dhcp-local excluded-address 10.10.1.2
```

6. Configure the DHCP local server to provide IP addresses to subscribers of ISP Boston.

```
host1(config)#ip dhcp-local pool ispBoston
host1(config-dhcp-local)#network 10.10.2.0 255.255.255.0
host1(config-dhcp-local)#domain-name ispBoston
host1(config-dhcp-local)#default-router 10.10.2.1
host1(config-dhcp-local)#lease 0 0 10
host1(config-dhcp-local)#ip dhcp-local limit atm 5
```

7. Configure the SDX client.

```
host1(config)#sscc primary address 10.10.1.2 port 3310
host1(config)#sscc enable
host1(config)#sscc retryTimer 200
```

Configuring the DHCPv6 Local Server

To configure the DHCPv6 local server, you enable the service on the router. The router can then delegate IPv6 prefixes to client routers and provide DNS server information to directly connected router clients.

service dhcpv6-local

- Use to enable the DHCPv6 local server.
- Example


```
host1(config)#service dhcpv6-local
```
- Use the **no** version to disable the DHCPv6 local server.

ipv6 dhcpv6-local delegated-prefix

- Use to specify the IPv6 prefix and lifetime that are to be delegated to the DHCPv6 client. The specified prefix is delegated by the DHCPv6 local server when requested by the client.
- Use the **lifetime** keyword to specify the time period for which the prefix is valid. This lifetime overrides the default lifetime that is set in Global Configuration mode. If no lifetime is specified, the default lifetime is assigned.
 - Specify the number of days and, optionally, the number of hours, minutes, and seconds. You cannot specify a lifetime of zero (that is, you cannot set the days, hours, minutes, and seconds fields all to zero).
 - Use the keyword **infinite** to specify a lifetime that does not expire.
- Example


```
host1(config-if)#ipv6 dhcpv6-local delegated-prefix 2001:db8:17::/48 lifetime infinite
```
- Use the **no** version to remove the IPv6 prefix from the interface.

ipv6 dhcpv6-local dns-domain-search

- Use to specify the name of a DNS domain for DHCPv6 clients in the current virtual router to search.
- Specify a maximum of four DNS domains for a DHCPv6 local server's search list.
- Example


```
host1(config-if)#ipv6 dhcpv6-local dns-domain-search xyzcorporation.com
host1(config-if)#ipv6 dhcpv6-local dns-domain-search xyzcorp.com
```
- Use the **no** version to remove the specified DNS domain from the search list.

ipv6 dhcpv6-local dns-server

- Use to specify the IPv6 address of the DNS server and to assign the server to the DHCPv6 clients in the current virtual router.
- Specify a maximum of four DNS servers.
- Example


```
host1(config-if)#ipv6 dhcpv6-local dns-server 2001:db8:18::
```
- Use the **no** version to delete the specified DNS server.

ipv6 dhcpv6-local prefix-lifetime

- Use to set the default lifetime for which a prefix delegated by this DHCPv6 local server is valid. This default is overridden by an interface-specific lifetime.
 - Specify the number of days and, optionally, the number of hours, minutes, and seconds. You cannot specify a lifetime of zero (that is, you cannot set the days, hours, minutes, and seconds fields all to zero).
 - Use the keyword **infinite** to specify a lifetime that does not expire.

- Example

```
host1(config-if)#ipv6 dhcpv6-local prefix-lifetime infinite
```
- Use the **no** version to restore the default lifetime to 1 day.

Configuring DHCP External Server Application

You can configure the E-series router to provide support for an external DHCP server. This enables the router, which is not running DHCP relay or DHCP proxy server, to monitor DHCP packets and to keep information for subscribers based on their IP address and MAC address. When the E-series router's DHCP external server application is used, all DHCP traffic to and from the external server is monitored by the router.



NOTE: You cannot configure both the DHCP local server and one of the following in the same virtual router: DHCP external server, DHCP relay, or DHCP relay proxy. If you issue the **set dhcp relay** command when a local server has been configured, the local server is deactivated.

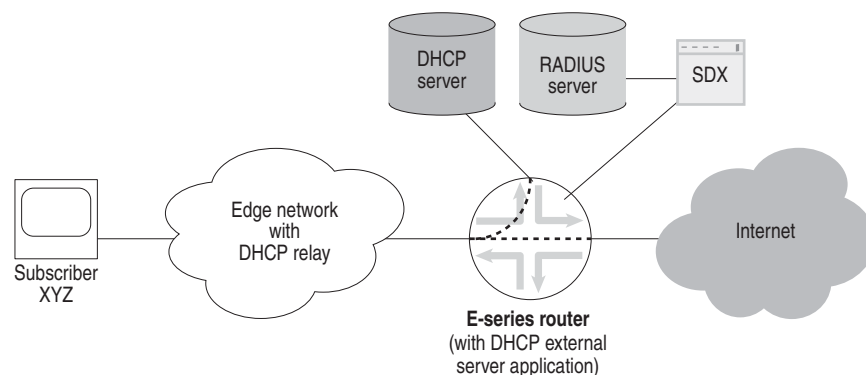
The services provided by integrating the E-series router's DHCP external server application with SDX software are similar to those provided when the DHCP local server is integrated with SDX software. The router's DHCP external application is used together with other features of the router to provide subscriber management. For additional information, see [Chapter 9, Configuring Subscriber Management](#).



NOTE: To ensure that DHCP external server with DHCP relay proxy processes unicast reply packets (such as renewal ACK and NAK packets), you must configure DHCP external server with the IP address of the DHCP relay proxy's giaddr. This configuration ensures that DHCP external server processes renewal ACK packets, which in turn enables the updating of client leases.

[Figure 14](#) shows a network that includes an external DHCP server and the E-series router.

Figure 14: DHCP External Server



g013393

In [Figure 14](#), the subscriber requests an address from the DHCP server through the E-series router. All communication between the subscriber and the DHCP server is monitored by the E-series router. After the subscriber receives an IP address, the subscriber is able to access the Internet and use the value-added services provided by the E-series router and by the SDX software. For this to occur, the edge network must be using a DHCP relay function.

When the subscriber requests an IP address from the DHCP server, the E-series router performs the following actions:

- Identifies the subscriber's IP address, MAC address, giaddr, and client identifier
- Extracts the lease time, creates a shadow lease, and starts its own lease timer that is associated with the subscriber

The E-series router views the subscriber as active once the subscriber sends a packet. The router then performs the following actions:

- Processes the subscriber's IP address by using a route map
- Extracts the dynamic subscriber interface profile (optional)
- Creates the subscriber's dynamic subscriber interface

If the SDX software is configured, the router also performs the following actions:

- Alerts the SDX program that the dynamic subscriber interface exists
- Alerts the SDX program that the subscriber's address exists and provides DHCP options

The SDX software then provides its enhanced services to the subscriber.

The E-series router monitors all traffic between the subscriber and the DHCP server, and resets the shadow lease by monitoring the DHCP server/client lease renewal. When the subscriber disconnects, the shadow lease will eventually expire. The E-series router then performs the following actions:

- Deletes the subscriber's dynamic subscriber interface
- Alerts the SDX software that the dynamic subscriber interface has been deleted
- Alerts the SDX software that the subscriber's address has been deleted

For additional information on managing client bindings, see [Viewing and Deleting DHCP Client Bindings](#) on page 371.

Interoperating with Ethernet DSLAMs

The DHCP external application uses the giaddr it receives in DHCP server–destined packets to determine the next hop for a subscriber’s access routes. However, when interoperating with Ethernet digital subscriber line access multiplexers (DSLAMs), using the giaddr sent by the DSLAM can result in traffic being dropped. To ensure that traffic is forwarded properly, you can configure the DHCP external application to disregard the DSLAM’s giaddr and learn the subscriber’s correct next-hop address.

The dropped traffic situation can occur because of the way some DSLAMs create the giaddr that is sent to the DHCP external application. Some Ethernet DSLAMs use a DHCP relay implementation that inserts giaddr values and relay agent options in DHCP packets that are received from end users. The intent is that this information is provided to a DHCP server, which uses the values to determine the configuration parameters for the subscriber.

However, when the DHCP external application receives the giaddr from an Ethernet DSLAM, the application installs the subscriber access route with the Ethernet DSLAM’s IP address as the next hop. This operation results in the subscriber–destined traffic being incorrectly sent to the Ethernet DSLAM, which cannot process the traffic.

To avoid dropping the traffic in this situation, use the **ip set dhcp-external disregard-giaddr-next-hop** command to configure the DHCP external application to ignore the giaddr when determining the next hop for the subscriber access routes. The E-series router then uses Address Resolution Protocol (ARP) to discover the subscriber’s IP address and sends the traffic to the learned IP address.

Configuring DHCP External Server Support

To configure the E-series router to support an external DHCP server, you enable the service on the router. If you are using DHCP packet detection, you must also specify each external DHCP server that determines which packets are monitored. The E-series router monitors all DHCP traffic between subscriber clients and the DHCP server.

dhcp-external delete-binding

- Use to delete clients from a virtual router’s DHCP binding table.



NOTE: This command is deprecated and might be removed completely in a future release. The function provided by this command has been replaced by the **dhcp delete-binding** command.

- Use the binding ID to delete a specific client from the table. Use the **all** keyword to delete all clients.
- Example

```
host1#dhcp-external delete-binding binding-id 3972819365
```
- There is no **no** version.

ip dhcp-external auto-configure

- Use to configure the DHCP external server to support the creation of dynamic subscriber interfaces.
- Use this command within a specific virtual router context.
- Use the **agent-circuit-identifier** keyword to configure the DHCP external server to support the creation of dynamic subscriber interfaces built over dynamic VLANs that are based on the agent-circuit-id option (suboption 1) of the option 82 field in DHCP messages.

The use of the option 82 field enables you to stack an IP interface that is associated with a particular subscriber over a dynamically created VLAN; the VLAN is dynamically created based on the agent-circuit-id option (suboption 1) that is contained in the DHCP option 82 field.

For information about configuring agent-circuit-id-based dynamic VLAN subinterfaces, see [JUNOS Link Layer Configuration Guide, Chapter 13, Configuring Dynamic Interfaces Using Bulk Configuration](#).

- This command requires that the user's DHCP control traffic and data traffic traverse the same client-facing ingress port on the E-series router.
- Examples

```
host1(config)#ip dhcp-external auto-configure
host1(config)#ip dhcp-external auto-configure agent-circuit-identifier
```

- Use the **no** version to disable the autoconfigure feature.

ip dhcp-external disregard-giaddr-next-hop

- Use to configure the DHCP external server application to disregard the giaddr when determining the next hop for a subscriber's access route.
 - Example
- ```
host1(config)#ip set dhcp-external disregard-giaddr-next-hop
```
- Use the **no** version to return to the default, in which the giaddr is not disregarded.

***ip dhcp-external server-address***

- Use to specify the IP address of the external DHCP server. The E-series router will monitor DHCP packets between the specified server and remote clients.
- You can configure a maximum of four DHCP servers.
- Example

```
host1(config)#ip dhcp-external server-address 10.10.10.1
host1(config)#ip dhcp-external server-address 10.20.10.1
```

- Use the **no** version to remove the specified DHCP server.

***ip dhcp-external server-sync***

- Use to create subscriber state information based on lease renewals.
- Use this command when the external DHCP server is unsynchronized with the E-series router. For example, an unsynchronized condition might occur when you first enable the DHCP external server application.
- Example  

```
host1(config)#ip dhcp-external server-sync
```
- Use the **no** version to disable this feature.

***service dhcp-external***

- Use to enable the DHCP external server application on the E-series router.
- Example  

```
host1(config)#service dhcp-external
```
- Use the **no** version to disable the DHCP external server application.

## Using Option 60 Strings to Forward Client Traffic to Specific DHCP Servers

---

The DHCP functionality supports the DHCP vendor class identifier option (option 60). This support allows DHCP relay to compare option 60 strings in received DHCP client packets against strings that you configure on the router. You can use the DHCP relay option 60 feature when providing converged services in your network environment—option 60 support enables DHCP relay to direct client traffic to the specific DHCP server (the vendor-option server) that provides the service that the client requires. Or, as another option, you can configure option 60 strings to direct traffic to the DHCP local server in the current virtual router.

For example, you might have an environment in which some DHCP clients require only Internet access, while other clients require IPTV service. The clients that need Internet access get their addresses assigned by the DHCP local server on the E-series router (in equal-access mode). Clients requiring IPTV must be relayed to a specific DHCP server that provides the service. To support both types of clients, you configure two option 60 strings on the DHCP relay. Now, when any DHCP client packets are received with option 60 strings configured, the strings are matched against all strings configured on the DHCP relay. If the client string matches the first string you configured, that client is directed to the DHCP local server and gains Internet access. Client traffic with an option 60 string that matches your second string is relayed to the DHCP server that provides the IPTV service. In addition, you can configure a default action, which DHCP relay performs when a client option 60 string does not match any strings you have configured—for example, you might specify that all clients with non-matching strings be dropped.

**set dhcp vendor-option**

- Use to configure vendor-option (option 60) strings to control DHCP client traffic. Create DHCP vendor-option servers by configuring DHCP relay to match DHCP option 60 strings and to specify what action to use for the traffic.
- Use the **equals** or **starts-with** keywords to specify a unique string to match, and to configure the action to take for traffic with a matching string:
  - **equals**—The DHCP client string is an exact match of the specified string
  - **starts-width**—The DHCP client string is a partial match, from left-to-right, of the specified string. For example, a client string of **day** matches a **starts-width** configured string of **daytime**.

Use the following keywords to configure actions for matching strings:

- **local-server**—Forward packets to the DHCP local server
- **relay**—Forward packets to the DHCP server with the specified IP address
- Use the **default** keyword to set the default action to take when the option 60 string does not match a configured vendor-option string. Use the following keywords to configure actions for nonmatching strings:
  - **drop**—Discard traffic
  - **local-server**—Forward packets to the DHCP local server
  - **proxy-client**—Forward traffic to the DHCP proxy client server
  - **relay**—Forward packets to the DHCP server with the specified IP address
  - **relay-server-list**—Forward traffic to all non-vendor option DHCP servers. The relay-server-list consists of all non-vendor option servers. Non-vendor option servers are those servers that are configured with the **set dhcp relay** command but not with the **set dhcp vendor-option** command.
  - When you configure the first DHCP vendor-option and no default action is specified for a configured DHCP application, the router chooses the default action according to the preference of the DHCP applications. The order of preference from first to last is DHCP local server, DHCP relay, and DHCP proxy client.
- You can map multiple strings to the same DHCP server, and you can map a single string to multiple servers. However, mapping one string to more than five DHCP vendor-option servers might impact performance.
- You can configure a maximum of 100 option 60 strings per DHCP relay. Strings can contain a maximum of 255 characters.
- Client packets that have option 60 configured but have no string specified (a string of 0 length) are treated as nonmatching strings and handled accordingly.
- Example 1—Configuring an exact match  

```
host1(config)#set dhcp vendor-option equals myword relay 192.168.7.7
```
- Example 2—Configuring a partial match  

```
host1(config)#set dhcp vendor-option starts-with abcd local-server
```
- Example 3—Configuring the default action  

```
host1(config)#set dhcp vendor-option default drop
```



- Example 4—Removing a configuration  
`host1(config)#no set dhcp vendor-option starts-with abcd local-server`
- Use the **no** version to remove the specified configuration.

**Configuration Example—Using DHCP Relay Option 60 to Specify Traffic Forwarding**

You use the DHCP relay option 60 feature to specify the action performed on DHCP client traffic. The DHCP relay uses the option 60 string in the client traffic to determine what action to take with the incoming traffic.

The following example describes a sample procedure that creates three actions for incoming DHCP client traffic, depending on the traffic’s option 60 string.

1. Enable the DHCP relay. Do not specify an IP address when you configure DHCP relay to support vendor-option strings.

```
host1(config)#set dhcp relay
```

2. Configure the action DHCP relay takes when the incoming traffic has an exact option 60 string of myword. DHCP relay forwards this traffic to the DHCP server with an IP address of 192.168.7.7.

```
host1(config)#set dhcp vendor-option equals myword relay 192.168.7.7
```

3. Configure the action DHCP relay takes when the incoming traffic has a partial match, from left-to-right, with an option 60 string you have configured. For this command, matching strings include a, ab, abc, and abcd. DHCP relay forwards matching traffic to the DHCP server with IP address 192.168.15.2.

```
host1(config)#set dhcp vendor-option starts-with abcd relay 192.168.15.2
```

4. Configure the default option 60 action. DHCP relay takes this action when the incoming traffic has an option 60 string that does not match any of the option 60 strings that you have configured. In this example, the traffic is sent to the DHCP local server.

```
host1(config)#set dhcp vendor-option default local-server
```

5. (Optional) View your DHCP relay vendor-option configuration.

```
host1(config)#run show dhcp vendor-option
Codes:
* - the configured vendor-string is an exact-match
default - all DHCP client packets not matching a configured vendor-string
implied - the DHCP application is configured but has not been enabled
 with the vendor-option command
drop - the DHCP application responsible for the action has not been
 configured yet therefore all packets for this application
 will be dropped
Total 3 entries.
```

| Vendor-option | Action                            |
|---------------|-----------------------------------|
| abcd          | relay to 192.168.15.2 (rx: 0)     |
| default(*)    | local-server (rx: 0, no-match: 0) |
| myword(*)     | relay to 192.168.7.7 (rx: 0)      |

## Configuring Cable Modem DHCP Relay

You use the DHCP vendor class identifier option (option 60) to configure DHCP relay to relay DHCP packets that originate from a cable modem to an external DHCP server that provides the cable modem with the configuration it requests.

Configure the vendor class identifier option to match the string used by cable modems—DHCP relay then forwards the packets to each DHCP server that you configured with the **set dhcp vendor-option** command (these servers are also considered to be cable-modem DHCP servers).

- Example:

```
host1(config)#set dhcp relay
host1(config)#service dhcp-local equal-access
host1(config)#set dhcp vendor-option equals docsis relay 192.168.1.1
host1(config)#set dhcp vendor-option equals cablemodem relay 192.168.1.1
```

Use the **show dhcp summary** and **show dhcp vendor-option** commands to display information about the cable modem DHCP relay configuration. See [show dhcp vendor-option](#) on page 383.

Use the **no** versions of the **set dhcp vendor-option** commands to disable the relay of DHCP messages from cable modems to the external DHCP server.

## Viewing and Deleting DHCP Client Bindings

The JUNOS software provides commands that enable you to manage your router's DHCP external server, DHCP local server, and DHCP relay proxy client bindings. A client binding associates an IP address with a DHCP client, and describes both the client (for example hardware address and state) and the IP address (for example subnet and lease time).

The commands enable you to view information about current DHCP bindings, and to remove current bindings that are no longer needed. Use the **show dhcp binding** command to display information for current client bindings and track lease times and status. Use the **dhcp delete-binding** command to delete a connected user's IP address lease and the associated route configuration. When you delete a client binding, the lease is removed on the router. You might delete client bindings to:

- Recover functional resources from a user who has not explicitly terminated connectivity and whose lease is unexpired.
- Discontinue connectivity to a user, prompting or forcing the user to request a new lease in order to reestablish network connectivity.

You can use the **dhcp delete-binding** command to delete leases that are granted by DHCP external server, DHCP local server, and DHCP relay proxy.

**dhcp delete-binding**

- Use to force removal of client leases from the router's DHCP binding table.
- This command replaces the **clear ip dhcp-local binding** and **dhcp-external delete-binding** commands, which are deprecated and might be removed in a future release.
- Use the following keywords:
  - **all**—Specifies all DHCP local server, DHCP external server, and DHCP relay proxy client bindings
  - **all-local**—Specifies all DHCP local server client bindings
  - **all-external**—Specifies all DHCP external server client bindings
  - **all-relay-proxy**—Specifies all DHCP relay proxy client bindings
  - **binding-id**—Specifies a particular binding ID
- Example 1  
host1#**dhcp delete-binding all-external**
- Example 2  
host1#**dhcp delete-binding binding-id 3972819365**
- There is no **no** version.

**Logging DHCP Packet Information**

The JUNOS software enables you to collect and log DHCP packet information for all JUNOS DHCP access models on a per-interface basis. To log packets for a specific DHCP application, you enable DHCP packet logging on the interface that serves the application. JUNOS software supports per-interface DHCP packet logging on a maximum of 16 interfaces. Per-interface DHCP packet logging is disabled by default.

You can specify which packets are logged—receive, transmit, or all. You can optionally assign low or high priority to the logged packets. Packets are assigned a low priority by default, which does not interfere with router DHCP packet processing. The logged packets are output to the dhcpCapture event logging category.

You can configure per-interface DHCP packet logging on statically configured and dynamically created IP interfaces. However, configuration information for dynamic interface configurations is lost after a cold restart. Both static and dynamic interface configuration information is maintained after a warm restart.

**ip dhcp-capture**

- Use to enable DHCP packet logging for all DHCP applications, on the interface.
- You can specify DHCP packet logging on a maximum of 16 interfaces.
- Use the **receive**, **transmit**, and **all** keywords to specify the type of DHCP packets that is logged.

- Use the optional **priority** keyword to assign a **low** or **high** priority to logged packets. By default, logged packets have a low priority and do not interfere with the router's DHCP packet processing.
- Example  
host1(config-if)#**ip dhcp-capture all**
- Use the **no** version to restore the default setting, which disables DHCP packet logging on the interface.

## Monitoring DHCP

---

This section describes the **show** commands for monitoring DHCP support on E-series routers.

You can set a statistics baseline by using the **baseline** commands. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline when you retrieve baseline-relative statistics.

### **baseline dhcp relay**

- Use to set a baseline for DHCP relay and DHCP relay proxy statistics.
- Use the **delta** keyword with the **show dhcp relay statistics** command and the **show dhcp relay proxy statistics** command to display baselined statistics.
- Example  
host1#**baseline dhcp relay**
- There is no **no** version.

### **baseline dhcp server**

- Use to set a baseline for DHCP proxy server statistics.
- Use the **delta** keyword with the **show dhcp server statistics** command to display baselined statistics.
- Example  
host1#**baseline dhcp server**
- There is no **no** version.

### **baseline ip dhcp-external**

- Use to set a baseline for DHCP external server statistics.
- The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.
- Example  
host1#**baseline ip dhcp-external**
- There is no **no** version.

**baseline ip dhcp-local****baseline ipv6 dhcpv6-local**

- Use to set a baseline for DHCP or DHCPv6 local server statistics.
- The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.
- Use the optional **interface** keyword with the **baseline ip dhcp-local** command to specify the type of interface and interface specifier. The following types of interfaces are supported for this command:
  - ATM
  - Fast Ethernet
  - Gigabit Ethernet
- Use the **delta** keyword with the **show ip dhcp-local statistics** command to show baselined statistics.
- Examples
 

```
host1#baseline ip dhcp-local atm 3/1

host1#baseline ipv6 dhcpv6-local
```
- There is no **no** version.

**show dhcp binding**

- Use to display DHCP client binding information.
- This command replaces the **show ip dhcp-external binding**, **show ip dhcp-external binding-id**, and **show ip dhcp-local binding** commands, which are deprecated and might be removed completely in a future release.
- Use the following keywords to qualify the binding information you want to display. All bindings are displayed if you do not specify an optional keyword.
  - **external**—Displays DHCP external server bindings
  - **local**—Displays DHCP local server bindings
  - **relay-proxy**—Displays DHCP relay proxy bindings
  - **detail**—Shows detailed information for the specified DHCP bindings
  - **binding-id**—Displays information for the specified DHCP binding
- Field descriptions
  - BindingId—Client binding ID
  - HwAddress—MAC address of client
  - IpSubnet—For DHCP local server bindings, the subnet of the IP address assigned to the client; 0.0.0.0 for DHCP external server and DHCP relay proxy bindings
  - IpAddress—IP address assigned to client
  - State—State of the DHCP client binding
  - Type—Binding type; external (DHCP external server), local (DHCP local server), or relay-p (DHCP relay proxy)

- Server—IP address of the DHCP server that allocated the client IP address
- Giaddr—For DHCP relay proxy the IP address of the DHCP relay proxy; for DHCP local server bindings, the IP address of the DHCP relay that sent the packet or 0.0.0.0 if the packet comes from the client; for DHCP external server bindings, the giaddr from the DHCP packet
- Lease—Total time for which the IP address is available, in seconds
- Remaining—Time remaining on the current lease, in seconds
- IpInterface—IP interface that is associated with the client
- ClientId—DHCP Option 61 received from the client
- Interface—Subinterface for DHCP local server bindings; does not apply to DHCP external server and DHCP relay proxy
- Relay Agent—Indicates Relay Agent Information option (option 82)
- Agent Circuit Id—Suboption 1 of the DHCP Relay Agent information option
- Agent Remote Id—Suboption 2 of the DHCP relay agent information option
- Vendor Specific—Suboption 9 of the DHCP relay agent information option
- Example 1

```
host1#show dhcp binding 3070230530
```

```
BindingId: 3070230530
HwAddress: 7000.0002.9365
IpSubnet: 0.0.0.0
IpAddress: 192.168.0.90
State: bound
Type: relay-p
Server: 192.168.15.1
Giaddr: 192.168.0.1
Lease: 3600
Remaining: 2079
IpInterface: GigabitEthernet1/0/1.101
ClientId: 45-41-48-00-01-70-00-00-02-93-65
Interface:
Relay Agent:
```

```
Agent Circuit Id: test circuit id
Agent Remote Id: test remote id
Vendor Specific: 01-02-03-04-05-06-07-08-09-0a-0b-0c-0d-0e-0f-10
Unrecognized: 11-12-13-14-15-16-17-18-19-1a-1b-1c-1d-1e-1f-20
```

■ Example 2

```

host1#show dhcp binding
BindingId HwAddress IpSubnet IpAddress Type State

3053453401 7000.0002.9365 0.0.0.0 192.168.0.90 external bound
3053453402 7000.0003.9365 0.0.0.0 192.168.0.91 external bound
3053453403 7000.0004.9365 0.0.0.0 192.168.0.92 external bound
3053453404 7000.0005.9365 0.0.0.0 192.168.0.93 external bound
3053453405 7000.0006.9365 0.0.0.0 192.168.0.94 external bound
3053453406 7000.0007.9365 0.0.0.0 192.168.0.95 external bound
3053453407 7000.0008.9365 0.0.0.0 192.168.0.96 external bound
3053453408 7000.0009.9365 0.0.0.0 192.168.0.97 external bound
3053453409 7000.000a.9365 0.0.0.0 192.168.0.98 external bound
3053453410 7000.000b.9365 0.0.0.0 192.168.0.99 external bound
3053453411 7000.000c.9365 0.0.0.0 192.168.0.100 external bound
3053453412 7000.000d.9365 0.0.0.0 192.168.0.101 external bound
3070230529 7000.0001.9365 0.0.0.0 192.168.0.2 relay-p bound
3070230530 7000.0002.9365 0.0.0.0 192.168.0.90 relay-p bound
3070230531 7000.0003.9365 0.0.0.0 192.168.0.91 relay-p bound
3070230532 7000.0004.9365 0.0.0.0 192.168.0.92 relay-p bound
3070230533 7000.0005.9365 0.0.0.0 192.168.0.93 relay-p bound
3070230534 7000.0006.9365 0.0.0.0 192.168.0.94 relay-p bound

```

**show dhcp relay**

- Use to display DHCP relay configuration information and the IP addresses of the configured DHCP servers.
- Field descriptions
  - Mode—DHCP relay mode; either Standard (DHCP relay mode) or Proxy (DHCP relay proxy mode)
    - Restore Client Timeout—(DHCP relay proxy mode only) number of hours
    - Send First Offer—On or off
  - Inhibit Access Route Creation—On or off
  - Assign Giaddr to Source IP—On or off
  - Layer 2 Unicast Replies—On or off
  - Giaddr Selects Interface—On or off
  - Broadcast Flag Replies—On or off
  - Relay Agent Information Option (82)—Status of the following options
    - Override Giaddr—On or off
    - Override Option—On or off
    - Trust All Clients—On or off
    - Preserve Option From Trusted Clients—On or off
    - Circuit-ID Sub-option (1)—On or off; when on includes a list of selected suboptions
    - Remote-ID Sub-option (2)—On or off
    - Vendor-Specific Sub-option (9)—On or off; when on includes a list of selected suboptions

- DHCP Server Addresses—IP addresses of configured DHCP servers

- Example

```
host1#show dhcp relay
```

```
DHCP Relay Configuration
```

```

Mode: Proxy
 Restore Client Timeout: 72
 Send First Offer: off
 Inhibit Access Route Creation: off
 Assign Giaddr to Source IP: off
 Layer 2 Unicast Replies: off
 Giaddr Selects Interface: off
 Broadcast Flag Replies: on
 Relay Agent Information Option (82):
 Override Giaddr: off
 Override Option: off
 Trust All Clients: off
 Preserve Option From Trusted Clients: off
 Circuit-ID Sub-option (1): on
 select - hostname
 select - exclude-subinterface-id
 Remote-ID Sub-option (2): on
 Vendor-Specific Sub-option (9): on
 select - layer2-circuit-id
 select - user-packet-class
```

```
DHCP Server Addresses
```

```

30.3.7.1
```

### **show dhcp relay statistics**

- Use to display DHCP packet error and relay agent option statistics that are reported for both DHCP relay and DHCP relay proxy, and also to display DHCP server statistics related only to DHCP relay.
- Use the optional **detail** keyword to display the following statistics on a per-server basis for DHCP relay only:
  - DHCP server statistics
  - Dropped unknown message type reply packets statistics
- Use the optional **delta** keyword to specify that baselined statistics are to be shown.



**NOTE:** The **show dhcp relay proxy statistics** command displays additional DHCP statistics that the router reports only for DHCP relay proxy.

---



- Field descriptions
  - Packet error statistics (standard & proxy modes)
    - ❑ dropped discover packets, no resources—Number of received DHCP relay discover messages that were discarded because of lack of resources
    - ❑ dropped dhcp packets, no resources—Number of received DHCP relay messages, other than discover messages, that were discarded because of lack of resources
    - ❑ dropped bad message operation packets—Number of received DHCP relay messages that were discarded because their message operation (for example, bootrequest, bootreply) was unknown, possibly due to corruption
    - ❑ dropped unknown message type request packets—Number of received DHCP relay request messages that were discarded because their message type (for example, discover, offer-request) was unknown, possibly due to corruption
    - ❑ dropped unknown message type reply packets—Number of received DHCP relay reply messages that were discarded because their message type (for example, offer, ack) was unknown, possibly due to corruption
  - Relay Agent Option statistics (standard & proxy modes)
    - ❑ add Relay Agent Option circuit ID suboption—Status of circuit ID suboption, on or off
    - ❑ add Relay Agent Option remote ID suboption—Status of remote ID suboption, on or off
    - ❑ packets with giaddr override—Number of received DHCP relay requests whose giaddr field is overridden with IP address 0.0.0.0
    - ❑ packets with Relay Agent Option override—Number of received DHCP relay requests whose relay agent information option is overridden with an option string created by this relay agent
    - ❑ packets forwarded with Relay Agent Option already present—Number of received DHCP relay requests already containing the relay agent information option that were forwarded to DHCP servers
    - ❑ dropped packets with Relay Agent Option already present—Number of received DHCP relay requests that were discarded because they already contained the relay agent information option when this relay agent was configured to insert the option
    - ❑ dropped giaddr spoof packets—Number of received DHCP relay requests that were discarded because the gateway IP address field already contained this relay agent's IP address
  - DHCP server statistics (standard mode only)
    - ❑ dropped duplicate request packets—Number of received DHCP relay requests that were discarded because they have a matching server address and XID of an outstanding DHCP server request
    - ❑ packets transmitted to servers—Number of DHCP relay requests successfully transmitted to DHCP servers

- ❑ packets received from servers—Number of DHCP relay replies successfully received from DHCP servers
- ❑ dropped unknown xid reply packets—Number of DHCP relay replies received from DHCP servers that were discarded because their server address and XID do not match an outstanding DHCP server request
- ❑ dropped stale request packets—Number of DHCP relay requests sent to DHCP servers that were discarded because their replies timed out

■ Example 1

host1#show dhcp relay statistics

| DHCP Relay Statistics                                     |        |
|-----------------------------------------------------------|--------|
| Statistic                                                 | Values |
| -----                                                     |        |
| Packet error statistics (standard & proxy modes):         |        |
| dropped discover packets, no resources                    | 0      |
| dropped dhcp packets, no resources                        | 0      |
| dropped bad message operation packets                     | 0      |
| dropped unknown message type request packets              | 0      |
| dropped unknown message type reply packets                | 0      |
| Relay Agent Option statistics (standard & proxy modes):   |        |
| add Relay Agent Option circuit ID suboption               | On     |
| add Relay Agent Option remote ID suboption                | On     |
| packets with giaddr override                              | 0      |
| packets with Relay Agent Option override                  | 2      |
| packets forwarded with Relay Agent Option already present | 4      |
| dropped packets with Relay Agent Option already present   | 3      |
| dropped giaddr spoof packets                              | 0      |
| DHCP server statistics (standard mode only):              |        |
| dropped duplicate request packets                         | 12     |
| packets transmitted to servers                            | 38     |
| packets received from servers                             | 26     |
| dropped unknown xid reply packets                         | 0      |
| dropped stale request packets                             | 12     |

■ Example 2

host1#show dhcp relay statistics detail

| DHCP Relay Detail Statistics         |           |               |              |
|--------------------------------------|-----------|---------------|--------------|
| Statistics                           | 10.10.1.1 | 192.168.32.12 | 192.168.32.1 |
| -----                                | -----     | -----         | -----        |
| Dropped unknown message type replies | 0         | 0             | 0            |
| Dropped duplicate requests           | 6         | 6             | 0            |
| Packets transmitted to server        | 6         | 6             | 26           |
| Packets received from server         | 0         | 0             | 26           |
| Dropped unknown xids replies         | 0         | 0             | 0            |
| Dropped stale requests               | 6         | 6             | 0            |

**show dhcp relay proxy statistics**

- Use to display statistics for the DHCP relay proxy.



**NOTE:** The **show dhcp relay statistics** command displays additional DHCP statistics that the router reports for both DHCP relay and DHCP relay proxy.

- Use the optional **delta** keyword to specify that baselined statistics are to be shown.
- Field descriptions
  - Address—IP address of the DHCP server
  - Disc.—Number of discover messages sent to server
  - Offer—Number of offers received from a server
  - Req.—Number of requests sent to a server
  - Ack—Number of ACK messages received from a server
  - Nak—Number of NAK messages received from a server
  - Decline—Number of decline messages sent to a server
  - Release—Number of releases sent to a server
  - Inform—Number of information messages sent to a server
  - Active Clients—Number of clients being maintained by the relay proxy
  - Clients to Restore—Number of host routes installed without an active client (waiting for renewal)
  - Client Packets—Total number of packets received from clients
  - Server Packets—Total number of packets received from servers
  - Timed Out—Number of clients removed because of lease expiration
  - No Offers—Number of clients removed because no server sent an offer
  - Modify Fail—Number of clients deleted because the relay proxy failed to modify the DHCP packet
- Example

host1#**show dhcp relay proxy statistics**

| DHCP Relay/Proxy Statistics |       |       |      |     |     |         |         |        |
|-----------------------------|-------|-------|------|-----|-----|---------|---------|--------|
| Address                     | Disc. | Offer | Req. | Ack | Nak | Decline | Release | Inform |
| 192.168.1.1                 | 9     | 0     | 0    | 0   | 0   | 0       | 0       | 0      |
| 192.168.1.2                 | 9     | 0     | 0    | 0   | 0   | 0       | 0       | 0      |
| 192.168.32.1                | 9     | 5     | 5    | 5   | 0   | 0       | 0       | 0      |

Active Clients: 5  
 Clients to Restore: 0  
 Client Packets: 14  
 Server Packets: 10  
 Timed Out: 0  
 No Offers: 4  
 Modify Fail: 0

**show dhcp server**

- Use to display DHCP proxy statistics.
- Field descriptions
  - O—Read-only value that displays the operational status of the server:
    - E—Enabled; indicates that the server is being actively used to supply IP addresses to clients
    - D—Draining; indicates that the server is not accepting any new requests for addresses, but is maintaining the addresses that it has already assigned
    - X—Disabled; means that the server is not accepting any new requests for addresses and has no outstanding addresses
  - A—Read/write value that displays the administrative status of the server:
    - E—Enabled; indicates that the server is being actively used to supply IP addresses to clients
    - D—Draining; indicates that the server is not accepting any new requests for addresses, but is maintaining the addresses that it has already assigned
    - X—Disabled; means that the server is not accepting any new requests for addresses and has no outstanding addresses
  - Address—IP address of a DHCP server
  - Leases—Number of IP address leases granted by the server
  - Offers—Number of offers sent by the server
  - Requests—Number of requests sent to the server
  - Acks—Number of acknowledgments received from the server
  - Naks—Number of negative acknowledgments received from the server
  - Declines—Number of IP addresses rejected because they were already in use
  - Releases—Number of IP addresses released back to the server
- Example

```
host1#show dhcp server
```

```

DHCP Proxy Client Status:

O A Address Leases Offers Requests Acks Naks Declines Releases
- - - - -
E E 10.6.128.10 0 0 0 0 0 0 0
E E 10.6.128.11 0 0 0 0 0 0 0

```

**show dhcp server statistics**

- Use to display DHCP proxy statistics
- Use the optional **delta** keyword to specify that baselined statistics are shown.
- Field descriptions
  - DHCP Server Address—IP address of the server
  - Discovers sent—Number of discover messages sent by the server
  - leases granted—Number of leases granted by the server
  - Offers received—Number of offers sent by the server
  - Requests sent—Number of requests sent to the server
  - Acks received—Number of acknowledgments received from the server
  - Naks received—Number of negative acknowledgments received from the server
  - addresses declined—Number of IP addresses rejected because they were already in use
  - addresses released—Number of IP addresses released back to the server
  - Informs sent—Number of inform messages sent to the server
  - unknown messages—Number of illegal DHCP messages or messages that cannot be handled by the router
  - bad messages—Number of messages not recognized as DHCP messages
- Example

```
host1#show dhcp server statistics
DHCP Proxy Global Statistics
Messages from Unknown Servers 0
```

| DHCP Proxy Server Statistics |             |            |                |
|------------------------------|-------------|------------|----------------|
| Statistic                    | Counts      | Counts     | Counts         |
| DHCP Server Address          | 10.6.128.10 | 10.10.0.42 | 192.168.200.10 |
| Discovers sent               | 0           | 0          | 0              |
| Leases granted               | 0           | 0          | 0              |
| Offers received              | 0           | 0          | 0              |
| Requests sent                | 0           | 0          | 0              |
| Acks received                | 0           | 0          | 0              |
| Naks received                | 0           | 0          | 0              |
| addresses declined           | 0           | 0          | 0              |
| addresses released           | 0           | 0          | 0              |
| Informs sent                 | 0           | 0          | 0              |
| unknown messages             | 0           | 0          | 0              |
| bad messages                 | 0           | 0          | 0              |

**show dhcp summary**

- Use to display which DHCP applications are configured whether they are active or inactive.
- Use this command to display the status of DHCP relay, DHCP relay proxy, DHCP local server, and DHCP external server.
- Field descriptions
  - configured—Applications that are currently configured
  - active or inactive—Current status of the application
- Example 1
 

```
host1#show dhcp summary
DHCP local-server configured and inactive
DHCP relay configured and active
```

**show dhcp vendor-option**

- Use to display configuration and action information for the DHCP vendor-option feature.
- Use the **default** keyword to display information for option 60 strings that do not match a configured vendor-option string.
- Use the **vendor-option-relay-server** keyword and server address to display information for option 60 strings that match a configured string that results in the packets being sent to the specified vendor-option server.
- Use the command without additional keywords to display information for all vendor option configurations.
- Field descriptions
  - Vendor-option—Option 60 string; an asterisk (\*) indicates that the string exactly matches a configured option 60 string, default indicates the action to take when the string does not match a configured option 60 string
  - Action—Action to take for the indicated string match; drop, forward to local-server, proxy client server, or all configured DHCP vendor option servers; or relay to the specified DHCP server
    - rx—Received packets that match a vendor-option string
    - no-match—Received packets that do not match a vendor-option string; no-match statistics appear only for default entries

■ Example 1

```
host1#show dhcp vendor-option
```

Codes:

- \* - the configured vendor-string is an exact-match
- default - all DHCP client packets not matching a configured vendor-string
- implied - the DHCP application is configured but has not been enabled with the vendor-option command
- drop - the DHCP application responsible for the action has not been configured yet therefore all packets for this application will be dropped

Total 4 entries.

| Vendor-option  | Action                                    |
|----------------|-------------------------------------------|
| Juniper        | relay to 10.10.1.1 (rx: 0)                |
| default(*)     | relay to 192.168.5.5 (rx: 0, no-match: 0) |
| someString(*)  | relay to 192.168.7.7 (rx: 0)              |
| someString2(*) | local-server (rx: 0)                      |

■ Example 2

```
host1#show dhcp vendor-option vendor-option-relay-server 10.10.1.1
```

Codes:

- \* - the configured vendor-string is an exact-match
- default - all DHCP client packets not matching a configured vendor-string
- implied - the DHCP application is configured but has not been enabled with the vendor-option command
- drop - the DHCP application responsible for the action has not been configured yet therefore all packets for this application will be dropped

Total 4 entries.

| Vendor-option | Action                     |
|---------------|----------------------------|
| Juniper       | relay to 10.10.1.1 (rx: 0) |

### **show ip dhcp-capture**

- Use to display the configuration for per-interface DHCP packet logging.
- Field descriptions
  - Router—Router name
  - Interface—Interface whose DHCP packets are logged
  - Type—Packet type to be logged, Rx (received), Tx (transmitted), or Rx/Tx (all)
  - Priority—Priority assigned to logged packets, low or high

■ Example

```
host1#show ip dhcp-capture
```

| Dhcp Capture Configuration |           |       |          |
|----------------------------|-----------|-------|----------|
| Router                     | Interface | Type  | Priority |
| default                    | ip3/1     | Rx/Tx | low/low  |
| default                    | ip5/1     | Rx    | high     |

**show ip dhcp-external binding**

- Use to display the mapping between the assigned IP address and the MAC address of the subscriber's computer.



**NOTE:** This command is deprecated and might be removed completely in a future release. The function provided by this command has been replaced by the **show dhcp binding** command.

- Field descriptions
  - Hardware—MAC address of subscriber's computer
  - IPAddress—Subscriber client's IP address
  - Server—DHCP server's address
  - Lease—Time for which the IP address is available, in seconds
  - Expire—Time remaining on the current lease, in seconds
  - Interface—Interface that is associated with the subscriber's computer
- Example

host1#show ip dhcp-external binding

| Dhcp External Binding |           |          |       |        |             |
|-----------------------|-----------|----------|-------|--------|-------------|
| Hardware              | IPAddress | Server   | Lease | Expire | Interface   |
| 3000.0001.9365        | 10.1.1.2  | 10.9.3.3 | 3600  | 3540   | ip201.1.1.2 |

**show ip dhcp-external binding-id**

- Use to display binding information for all DHCP clients.



**NOTE:** This command is deprecated and might be removed completely in a future release. The function provided by this command has been replaced by the **show dhcp binding** command.

- Field descriptions
  - Binding Id—DHCP client binding ID option value associated with the user
  - Hardware—MAC address of the subscriber's computer
  - IPAddress—IP address assigned to the client
- Example

host1(config)#show ip dhcp-external binding-id

| Dhcp External Binding Ids |                |           |
|---------------------------|----------------|-----------|
| Binding Id                | Hardware       | IPAddress |
| 3193657721                | 3000.0001.9365 | 10.1.1.2  |



**show ip dhcp-external configuration**

- Use to display information about the router's DHCP external server application.
- Field descriptions
  - Dhcp External—Enabled or disabled
  - Auto-Configure—Enabled or disabled
  - Server-Sync—Enabled or disabled
  - Disregard-Giaddr-Next-hop—Enabled or disabled
  - Servers—DHCP servers whose traffic is monitored by the E-series router.
- Example

```

host1(config)#show ip dhcp-external configuration
Dhcp External : Enabled
Auto-Configure : Enabled
Server-Sync : Enabled
Disregard-Giaddr-Next-Hop : Enabled

Servers:

10.1.1.1
10.2.1.1
10.3.1.1

```

**show ip dhcp-external statistics**

- Use to display statistics for all external DHCP servers, or for a specific server.
- Field descriptions
  - memUsage—Memory in bytes used by DHCP server
  - bindings—Number of IP addresses currently assigned
  - request—Number of DHCP request packets
  - ack (request)—Number of DHCP acknowledgment packets in response to DHCP requests
  - renew—Number of DHCP renew packets
  - ack (renew)—Number of DHCP acknowledgment packets in response to DHCP renewals
  - nak—Number of DHCP negative acknowledgment packets
  - release—Number of DHCP release packets
  - lease expirations—Number of lease expirations

- Example

```
host1(config)#show ip dhcp-external statistics server-address 100.20.32.1
DHCP External Statistics
Server Address 10.10.32.1

 Item Count

memUsage 136
bindings 1
request 69
ack (request) 1120
renew 38611
ack (renew) 38611
nak 42
release 68
lease expirations 0
```

### **show ip dhcp-local**

- Use to display the DHCP local server's configuration information.
- Field descriptions
  - Mode—DHCP local server mode, equal-access or standalone
  - SNMP Traps Enabled—Status of DHCP local traps support, yes or no
  - Unique Client IDs—Status of duplicate client ID and duplicate hardware address detection, enabled or disabled
- Example

```
host1#show ip dhcp-local

 DHCP Local Server Configuration
Mode: Standalone
SNMP Traps Enabled - no
Unique Client IDs - enabled
```

### **show ip dhcp-local auth**

- Use to display the DHCP local server's AAA authentication configuration information and statistics.
- Field descriptions
  - User-Prefix—Client's user prefix
  - Domain—Client's domain
  - Password—Password used to authenticate client
  - Virtual Router—Client's virtual router; excluded or included
  - Circuit Type—Client's circuit type; excluded or included
  - Circuit ID—Client's circuit ID; excluded or included
  - MAC Address—Client's MAC address; excluded or included
  - Option 82—Status of client's option 82 field; excluded or included
  - auth requests—Number of authorization requests received by this DHCP local server

- auth request failures—Number of authorization requests that have failed
- auth grants—Number of authorization requests that have been granted
- auth denies—Number of authorization requests that have been denied

■ Example 1

host1#**show ip dhcp-local auth config**

DHCP Local Server Authentication Configuration

```
User-Prefix : ERX4-Boston
Domain : ISP1.com
Password : to4Tool8
Virtual Router : included
Circuit Type : included
Circuit ID : included
MAC Address : excluded
Option 82 : excluded
```

■ Example 2

host1#**show ip dhcp-local auth statistics**

DHCP Local Server Authentication Statistics

| Item                  | Count |
|-----------------------|-------|
| auth requests         | 10    |
| auth request failures | 0     |
| auth grants           | 9     |
| auth denies           | 1     |

### **show ip dhcp-local binding**

- Use to display DHCP local server binding information for DHCP local server clients.



**NOTE:** This command is deprecated and might be removed completely in a future release. The function provided by this command has been replaced by the **show dhcp binding** command.

- Optionally, specify an IP address or an interface to display binding information for a particular address or interface.
- Field descriptions
  - Address—IP address
  - Hardware—MAC address of subscriber's computer
  - Lease—Infinite, or the number of seconds in which the IP address is available; grace period is shown in parentheses for clients in a grace period
  - Interface—Interface whose statistics are reported
  - State—Binding state; expired or released state for clients currently in the grace period

- Example 1

```
host1#show ip dhcp-local binding 192.168.1.3
```

| Dhcp Local Bindings |                   |       |                  |         |
|---------------------|-------------------|-------|------------------|---------|
| Address             | Hardware          | Lease | Interface        | State   |
| 192.168.1.3         | 11-11-22-22-33-33 | (600) | fastEthernet 5/0 | expired |

- Example 2

```
host1#show ip dhcp-local binding interface fastethernet 5/0.2
```

| Dhcp Local Bindings |                   |       |                    |         |
|---------------------|-------------------|-------|--------------------|---------|
| Address             | Hardware          | Lease | Interface          | State   |
| 192.168.0.6         | 40-00-00-0b-00-01 | 240   | fastEthernet 5/0.2 | bound   |
| 192.168.0.7         | 40-00-00-0c-00-01 | 240   | fastEthernet 5/0.2 | bound   |
| 192.168.1.3         | 11-11-22-22-33-33 | (600) | fastEthernet 5/0.2 | expired |

### **show ip dhcp-local duplicate-clients**

- Use to display duplicate MAC addresses that are being used by DHCP local server clients.
- Optionally, display information for a specific duplicate MAC address.
- Field descriptions
  - MAC—Duplicate MAC address
  - Interface—Interfaces used by the duplicate MAC address
  - Count—Number of times the duplicate MAC address has been detected
  - Time— Date and time the first duplication was detected

- Example

```
host1#show ip dhcp-local duplicate-clients 00-0D-61-7F-67-70
```

|     |                   |       |                                |
|-----|-------------------|-------|--------------------------------|
| MAC | 00-0D-61-7F-67-70 |       |                                |
|     | Interface         | Count | Time                           |
|     | ATM 3/0.1         | 100   | Sat Sept 17, 2005 06:00:51 UTC |
|     | ATM 3/0.2         | 90    | Sun Sept 18, 2005 09:00:00 UTC |

### **show ip dhcp-local excluded**

- Use to display addresses that have been excluded using the **ip dhcp-local excluded-address** command. The DHCP local server does not allocate excluded addresses, because they are already used by devices on the subnetwork.
- Field descriptions
  - Pool—Name of the pool that contains the excluded address
  - Low Address—Excluded address or first address in a range of addresses
  - High Address—Last address in a range of addresses

- Example

```
host1(config)#show ip dhcp-local excluded
Dhcp Excluded Addresses
```

| Pool     | Low Address | High Address |
|----------|-------------|--------------|
| default  | 10.10.1.1   |              |
| default  | 10.10.1.5   | 10.10.1.30   |
| cable2   | 10.10.2.1   |              |
| home.com | 10.10.3.1   |              |
| cable4   | 10.10.4.1   |              |
| cable5   | 10.10.5.1   |              |

### **show ip dhcp-local leases**

- Use to display lease information for a specific IP address or for all leases.
- Field descriptions
  - Address—IP address
  - Hardware—MAC address of the subscriber's computer
  - Lease—Infinite, or the number of seconds in which the IP address is available; grace period in parentheses for clients in the grace period
  - Initiated/Renewed—Day, date, and time the lease was most recently initiated or renewed; start time of grace period for clients in the grace period
  - Expiration—Day, date, and time the lease expires; expiration time of grace period for clients in the grace period
  - Remaining—Infinite, or the number of seconds remaining in the lease, if any; remaining time of grace period for clients in the grace period
  - Initial Lease Start—Day, date, and time the lease was initiated
- Example 1

```
host1#show ip dhcp-local leases 192.168.0.3
```

| Dhcp Local Leases |                              |       |                              |
|-------------------|------------------------------|-------|------------------------------|
| Address           | Hardware                     | Lease | Initiated/Renewed            |
| 192.168.0.3       | 10-06-10-00-10-33            | 120   | THU SEP 08 2005 08:02:11 UTC |
| Address           | Expiration                   |       | Remaining                    |
| 192.168.0.3       | THU SEP 08 2005 08:04:11 UTC |       | 79                           |
| Address           | Initial Lease Start          |       |                              |
| 192.168.0.3       | THU SEP 08 2005 08:01:12 UTC |       |                              |

■ Example 2

```
host1#show ip dhcp-local leases
```

| Dhcp Local Leases |                              |          |                              |
|-------------------|------------------------------|----------|------------------------------|
| Address           | Hardware                     | Lease    | Initiated/Renewed            |
| 192.168.0.2       | 10-06-10-00-10-32            | 120      | THU JUL 06 2006 08:02:11 UTC |
| 192.168.0.3       | 10-06-10-00-10-33            | 120      | THU JUL 06 2006 08:02:11 UTC |
| 192.168.55.4      | 10-06-10-00-10-34            | (600)    | THU JUL 06 2006 09:57:22 UTC |
| 192.168.55.5      | 10-06-10-00-10-35            | infinite | THU JUL 06 2006 08:03:10 UTC |
| Address           | Expiration                   |          | Remaining                    |
| 192.168.0.2       | THU JUL 06 2006 08:04:11 UTC |          | 80                           |
| 192.168.0.3       | THU JUL 06 2006 08:04:11 UTC |          | 80                           |
| 192.168.55.4      | THU JUL 06 2006 10:07:22 UTC |          | 575                          |
| 192.168.55.5      | THU JUL 06 2006 08:04:11 UTC |          | infinite                     |
| Address           | Initial Lease Start          |          |                              |
| 10.1.0.2          | THU JUL 06 2006 08:01:12 UTC |          |                              |
| 10.1.0.3          | THU JUL 06 2006 08:01:12 UTC |          |                              |
| 192.168.55.4      | THU JUL 06 2006 09:54:19 UTC |          |                              |
| 192.168.55.5      | THU JUL 06 2006 08:03:10 UTC |          |                              |

### *show ip dhcp-local limits*

- Use to display the maximum number of leases available for each VPI/VCI, VLAN, Ethernet subnetwork, or for a specific interface or subinterface.
- Field descriptions
  - ATM Limit—Number of leases available for each VPI/VCI
  - VLAN Limit—Number of leases available for each VLAN
  - Ethernet Limit—Number of leases available for each Ethernet subnet
  - Limit—Number of leases available to the specified interface or subinterface; indicates the configured value for the interface type unless a specific lease value is configured for the particular interface
  - Count—Number of active leases on the interface
  - Denied—Number of lease requests denied during the current denial period; this number is reset to zero (and the denial period restarted) when the number of active leases no longer exceeds the configured limit
  - Total Denied—Total number of lease requests denied on the interface since the interface became active

■ Example 1

```
host1(config)#show ip dhcp-local limits
```

```

DHCP Local Server Address Limits
ATM Limit - 5000
VLAN Limit - 2000
Ethernet Limit - 1000
```

■ Example 2

```
host1(config)#show ip dhcp-local limits interface atm 3/1
```

| Dhcp Local Interface Limits |       |       |        |                 |
|-----------------------------|-------|-------|--------|-----------------|
| -----                       |       |       |        |                 |
| Interface                   | Limit | Count | Denied | Total<br>Denied |
| -----                       | ----- | ----- | -----  | -----           |
| atm 3/1                     | 300   | 127   | 5      | 29              |

■ Example 3

```
host1(config)#show ip dhcp-local limits interface
```

| Dhcp Local Interface Limits |       |       |        |                 |
|-----------------------------|-------|-------|--------|-----------------|
| -----                       |       |       |        |                 |
| Interface                   | Limit | Count | Denied | Total<br>Denied |
| -----                       | ----- | ----- | -----  | -----           |
| fastEthernet0/0             | 200   | 0     | 0      | 0               |
| atm 3/1                     | 300   | 127   | 5      | 29              |
| atm 4/2                     | 5000  | 0     | 0      | 0               |
| atm 5/1                     | 5000  | 15    | 2      | 5               |

### **show ip dhcp-local pool**

- Use to display the IP DHCP local pool configurations.
- Field descriptions
  - Pool Name—Name of the DHCP local pool
  - Pool Id—ID of the pool
  - Domain Name—Domain name assigned to the pool
  - Network—Addresses that the DHCP local server can provide from the pool
  - Mask—Subnet mask that goes with the network address
  - NETBIOS Node Type—Type of NetBIOS server:
    - 1—Broadcast
    - 2—Peer-to-peer
    - 4—Mixed
    - 8—Hybrid
  - Lease—Time for which the supplied IP address is valid
  - Grace Period—Length of grace period
  - Grace period for released leases—Status of the grace period for released leases; enabled or disabled
  - DNS Servers—Address of each DNS server assigned to the pool
  - NETBIOS Name Servers—NetBIOS server assigned to subscribers
  - Default Routers—Address of default router used for subscribers
  - Server Address—DHCP server address that is sent to subscribers
  - Linked Pool—Names of any pools that are linked to this pool

- High utilization threshold—Threshold at which the utilization trap is triggered, if the trap is enabled
- Abated utilization threshold—Threshold at which the utilization trap is reenabled after the trap has been triggered
- Current utilization—Percentage of local address pool currently used
- Utilization trap—Status of the utilization trap, which is generated when the high utilization threshold is reached; enabled or disabled
- Shared pool allocations—Number of addresses allocated to shared pools
- Group Name—Group name; based on the name of the original pool
- Total Addresses Available—Number of addresses in the group
- Total Addresses In Use—Number of addresses currently being used
- Trap Enabled—Status of utilization trap, yes or no
- Pools—Names of pools in the group

■ Example 1

host1#show ip dhcp-local pool

```

Pool Name - ispBoston
Pool Id - 6
Domain Name - ispBoston
Network - 10.10.0.0
Mask - 255.255.255.0
NETBIOS Node Type - 1
Lease - Days:0 Hours:0 Minutes:24 Seconds:0
Grace Period - Days:0 Hours:0 Minutes:10 Seconds:0
Grace period for released leases enabled
DNS Servers
 10.10.1.1
NETBIOS Name Servers
 10.10.1.1
 10.10.1.2
Default Routers
 10.10.1.3
Server Address - 10.10.20.8
Linked Pool - cable5
High utilization threshold - 85%
Abated utilization threshold - 75%
Current utilization - 0%
Utilization trap disabled.
Shared pool allocations - 25
```



```
■ Example 2
host1#show ip dhcp-local pool groups

DHCP Local Server Pool Groups
There is 1 group configured

Group Name: pool8_7-1-Group
Total Addresses Available: 145
Total Addresses In Use: 0
High Utilization Thresh: 85%
Abated Utilization Thresh: 75%
Current Utilization: 0%
Trap Enabled: no
===== Pools =====
pool8_7-1
pool8_7-2
pool8_7-3
pool8_7-4
pool8_7-5
```

**show ip dhcp-local reserved**

- Use to display the static IP address/MAC address pairs that the DHCP local server supplies in standalone mode.
- Field descriptions
  - Pool—Name of pool in which the address is reserved
  - Address—IP address that is reserved
  - Hardware—Address for which the IP address is reserved
- Example

```
host1#show ip dhcp-local reserved
DHcp Reserved Addresses

Pool Address Hardware

cablemodem 10.44.44.100 12-34-12-34-12-34-00-00-00-00-00-00-00-00-00-00
cablemodem 10.44.44.101 22-33-22-33-22-33-00-00-00-00-00-00-00-00-00-00
```

**show ip dhcp-local statistics**

- Use to display statistics for the DHCP local server.
- Field descriptions
  - memUsage—Number of bytes of memory used by the DHCP local server
  - bindings—Number of leased IP addresses currently assigned
  - Receive Statistics—Statistics for packets that have been received
    - discover—Number of DHCP discover messages received
    - request(accept)—Number of DHCP requests accepted
    - request(renew)—Number of DHCP requests for renewal received
    - request(rebind)—Number of DHCP requests for rebinding received
    - request(other)—Number of DHCP unknown requests received

- ❑ decline—Number of DHCP decline messages received
- ❑ release—Number of DHCP release messages received
- ❑ inform—Number of DHCP inform messages received
- ❑ total in packet—Number of packets received
- ❑ in error—Number of packets received with errors that prevent further processing; count is independent of the message-type counters
- ❑ in discard—Number of packets received that are discarded due to system resource issues; count is independent of the message-type counters
- ❑ unknown client packet—Number of nonrequest packets that have no entry in the local server database received
- Transmit Statistics—Statistics for packets that have been transmitted
  - ❑ offer—Number of DHCP offer messages sent
  - ❑ ack(accept)—Number of DHCP acknowledgments sent in response to accepted requests
  - ❑ ack(renew)—Number of DHCP acknowledgments sent in response to renewal requests
  - ❑ ack(rebind)—Number of DHCP acknowledgments sent in response to rebinding requests
  - ❑ nak—Number of DHCP NAK messages sent in response to requests that cannot be bound or that are unknown to this local server
  - ❑ nak(renew)—Number of DHCP NAK messages sent in response to renewal requests
  - ❑ nak(rebind)—Number of DHCP NAK messages sent in response to rebinding requests
  - ❑ total out packet—Number of packets sent by the DHCP local server
  - ❑ out error—Number of packets that cannot be transmitted due to protocol errors or configuration errors; count is independent of the message-type counters
  - ❑ out discard—Number of packets that cannot be transmitted due to system resource issues; count is independent of the message-type counters
- Example 1

```
host1#show ip dhcp-local statistics
DHCP Local Server Statistics
```

| Item                   | Count |
|------------------------|-------|
| memUsage               | 184   |
| bindings               | 2     |
| --Receive Statistics-- |       |
| discover               | 8     |
| request(accept)        | 10    |
| request(renew)         | 6     |
| request(rebind)        | 2     |
| request(other)         | 6     |
| decline                | 0     |

```

release 6
inform 0
total in packet 38
in error 0
in discard 0
unknown client packet 6
--Transmit Statistics--
offer 8
ack(accept) 10
ack(renew) 6
ack(rebind) 2
nak 6
nak(renew) 0
nak(rebind) 0
total out packet 32
out error 0
out discard 0

```

## ■ Example 2

host1#show ip dhcp-local statistics interface atm 4/0.32

```

DHCP Local Server SubInterface Statistics
Interface Item Count

ATM4/0.32
Receive Statistics
discover 4
request(accept) 5
request(renew) 1
request(rebind) 1
request(other) 3
decline 0
release 3
inform 0
total in packet 17
in error 0
in discard 0
unknown client packet 3
Transmit Statistics
offer 4
ack(accept) 5
ack(renew) 1
ack(rebind) 1
nak 3
nak(renew) 0
nak(rebind) 0
total out packet 14
out error 0
out discard 0

```

**show ipv6 dhcpv6-local binding**

- Use to display the mapping between one or more IPv6 addresses and the DHCP unique ID of the subscriber's computer.
- Field descriptions
  - Prefix—IPv6 address
  - Client DUID—DHCP unique ID of subscriber's computer
  - Lease—Time for which the IPv6 address is available in seconds, or infinite
  - Intf—Router's interface that is associated with the subscriber's computer

## ■ Example

```
host1#show ipv6 dhcpv6-local binding 2001:db8:4::/48
```

| Prefix          | Client DUID         | Lease    | Intf               |
|-----------------|---------------------|----------|--------------------|
| 2001:db8:4::/48 | <LL 1/00A0DE113502> | infinite | FastEthernet 3/6.1 |

**show ipv6 dhcpv6-local dns-domain-searchlist**

- Use to display the DHCPv6 local servers DNS search list.
- Field descriptions
  - Domain—Domains in the search list.
- Example

```
host1#show ipv6 dhcpv6-local dns-domain-searchlist
Domain 1: xyzcorporation.net
Domain 2: xyzcorp.com
Domain 3: financeDomain.com
Domain 4: researchDomain.com
```

**show ipv6 dhcpv6-local dns-servers**

- Use to display a list of DNS servers configured on the DHCPv6 local server.
- Field descriptions
  - DNS server—IPv6 address of the DNS server
- Example

```
host1#show ipv6 dhcpv6-local dns-servers
DNS server 1: 2001:db8:18::
DNS server 2: 2001:db8:19::
DNS server 3: 2001:db8:20::
DNS server 4: 2001:db8:21::
```

**show ipv6 dhcpv6-local prefix-lifetime**

- Use to display the DHCPv6 default prefix lifetime.
- Field descriptions
  - default prefix lifetime—Number of days, hours, and minutes
- Example

```
host1#show ipv6 dhcpv6-local prefix-lifetime
default prefix lifetime is 1 day, 12 hours, 30 minutes
```

**show ipv6 dhcpv6-local statistics**

- Use to display statistics for the DHCPv6 local server.
- Field descriptions
  - memUsage—Number of bytes of memory used by DHCPv6 local server
  - bindings—Number of leased IPv6 prefixes currently assigned
  - solicit rx—Number of DHCPv6 solicit messages received
  - request(accept) rx—Number of DHCPv6 request messages received
  - request(renew) rx—Number of DHCPv6 requests for renewal received
  - decline rx—Number of DHCPv6 decline messages received
  - release rx—Number of DHCPv6 release messages received
  - inform rx—Number of DHCPv6 information-request messages received
  - confirm rx—Number of DHCPv6 confirm messages received
  - rebind rx—Number of DHCPv6 rebind messages received
  - reconfigure tx—Number of DHCPv6 reconfigure messages transmitted
  - advertise tx—Number of DHCPv6 advertise messages transmitted
  - successful reply tx—Number of reply messages transmitted with success reply code
  - failed reply tx—Number of reply messages transmitted with reply codes other than success
  - unknown msgs—Unused field; always 0
  - bad msgs—Number of messages with errors received by the DHCPv6 local server
- Example

```
host1#show ipv6 dhcpv6-local statistics
```

```
DHCPv6 Local Server Statist
```

| Item                | Count |
|---------------------|-------|
| memUsage            | 136   |
| bindings            | 1     |
| solicit rx          | 1     |
| request(accept) rx  | 1     |
| request(renew) rx   | 0     |
| decline rx          | 0     |
| release rx          | 0     |
| inform rx           | 0     |
| confirm rx          | 0     |
| rebind rx           | 0     |
| reconfigure tx      | 0     |
| advertise tx        | 1     |
| successful reply tx | 1     |
| failed reply tx     | 0     |
| unknown msgs        | 0     |
| bad msgs            | 0     |



## Chapter 9

# Configuring Subscriber Management

This chapter describes how to set up subscriber management on the E-series router. Subscriber management integrates a variety of router features and enables you to manage your constantly changing subscriber environment without affecting the performance you provide to your customers.

The following sections discuss subscriber management:

- [Overview](#) on page 399
- [Platform Considerations](#) on page 400
- [Subscriber Management Attributes](#) on page 400
- [Subscriber Management Procedure](#) on page 401
- [Subscriber Management Commands](#) on page 404
- [Configuration Examples](#) on page 411
- [Monitoring Subscriber Management](#) on page 413

## Overview

---

The E-series router enables customers to create a unified subscriber management, provisioning, and service delivery environment. The flexibility of the router provides a variety of methods and configurations that enable customers to dynamically provision new subscribers and quickly create new value-added services.

Two major aspects of subscriber management are subscriber provisioning and differentiated service delivery. The E-series router enables you to use both static and dynamic methods to add and delete subscribers. Important subscriber management concepts provided by JUNOS subscriber management include:

- Subscriber use of a shared medium
- Multiple subscribers using the same primary interface
- User authentication and accounting
- Differentiated services for individual subscribers

A subscriber management environment can include the following components:

- Local Dynamic Host Configuration Protocol (DHCP) server
- External DHCP server
- RADIUS server
- Service Deployment System (SDX) application

You employ the components you need in a variety of configurations, depending on your specific requirements.

## Platform Considerations

---

Subscriber management is supported on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E320 Module Guide* for modules supported on the E120 router and the E320 router.

## Subscriber Management Attributes

---

E-series routers take advantage of many of the JUNOS features to enable you to create the subscriber management environment that best meets your requirements. These features include:

- Authentication—Uses RADIUS to determine whether a user can access a specific service or resource.
- Accounting—Uses RADIUS and policy management to track service usage that can be used for volume-based billing.
- Dynamic address assignment—Uses RADIUS, DHCP, and profiles to dynamically allocate IP addresses to subscribers.
- Dynamic policy management—Uses policy and quality of service (QoS) management to assign and monitor subscriber bandwidth restrictions.
- Security—Uses policy management, source address validation, and media access control (MAC) address validation to grant subscriber access and to enable the use of classification when monitoring subscriber traffic flows.
- Dynamic interfaces—Automatically creates an interface column based on a catalyst packet or event.



- Marking—Uses policy management marking to enable differential treatment of specific packets.
- Policy routing—Uses policy management routing policies to assign subscriber routes that are based on classification.

### **Dynamic IP Subscriber Interfaces**

You can set up your subscriber management environment to create dynamic IP subscriber interfaces in two situations—when a DHCP event occurs or when a packet is detected.

In the first case, the interface is created when an external DHCP server or the DHCP local server responds to a subscriber request. In the second case, the subscriber interface is created when the router receives a packet (the packet detect feature) with a source IP address that is not in the demultiplexer table. In this second case the primary IP interface must be in autoconfiguration mode.

Subscriber management uses the following process when validating the IP source address of the packet:

- If the address is not valid, no subscriber interface is created. A discard entry is added to the demultiplexer table, and an error message is generated.
- If the address is valid with respect to the address ranges configured on the primary IP interface, subscriber management uses packet information to select the appropriate dynamic subscriber interface profile. The commands corresponding to the profile are then used to create the subscriber interface.

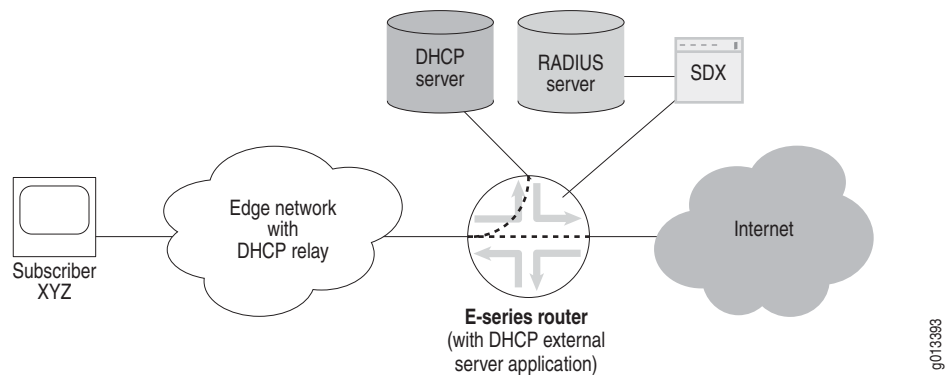
### **Subscriber Management Procedure**

---

Figure 15 shows a subscriber management environment that includes an external DHCP server, a RADIUS server, the SDX application, and the DHCP external server application running on the E-series router.

The E-series router DHCP external server application is used with other JUNOS features to provide subscriber management. Using the router's DHCP external server application for subscriber management enables you to take advantage of the following features:

- Profile assignment—A dynamic subscriber interface profile is associated with a specific source address by the router's packet detect feature.
- Dynamic subscriber interface packet detection and inactivity timer—Subscriber interfaces are dynamically created based on packet information that is identified by the packet detection feature. The inactivity timer determines when a dynamic subscriber interface expires and needs to be deleted.
- DHCP external server application—DHCP packets are examined to determine the state of subscribers.

**Figure 15: DHCP External Server**

In [Figure 15](#), the subscriber requests an address from the DHCP server. The E-series router DHCP external server application monitors all DHCP communications between the subscriber and the DHCP server. After the subscriber receives an IP address, the subscriber can access the Internet and use the value-added services provided by the SDX application. The following list describes the various procedures performed in the subscriber management environment:

- Subscriber PC—Requests an IP address from the DHCP server
- E-series router
  - Monitors DHCP traffic between the subscriber and the DHCP server:
    - Identifies the subscriber's IP address, MAC address, giaddr, and client identifier
    - Extracts the lease time, creates a shadow lease, and starts its own lease timer that is associated with the subscriber
  - Determines the subscriber is active when the subscriber sends a packet after receiving an IP address from DHCP. The router then:
    - Processes the subscriber's IP address by using a route map
    - Extracts the dynamic subscriber interface profile (optional)

The profile is used to authenticate the subscriber with authentication, authorization, accounting, and address assignment (AAAA) and RADIUS to obtain information for the subscriber's IP interface.

  - Creates the subscriber's dynamic subscriber interface (DSI)

- If the SDX application is configured, the router also alerts the SDX application that the subscriber's DSI and address exist.
- The DHCP external server application continues to monitor all traffic between the subscriber and the DHCP server, and periodically resets the shadow lease it originally created when the subscriber first requested an IP address. When the subscriber disconnects, the shadow lease eventually expires, at which time the E-series router performs the following:
  - Deletes the DSI
  - Alerts the SDX application that the DSI has been deleted
  - Alerts the SDX application that the subscriber's address has been deleted
- SDX application—Provides enhanced services to the subscriber.

### **Configuring Subscriber Management with an External DHCP Server**

To configure subscriber management for clients by using an external DHCP server, as in [Figure 15](#), use the following procedure on E-series routers:

1. Enable the DHCP external server application.

```
host1(config)#service dhcp-external
```

2. Specify each DHCP server for which to monitor traffic. You can specify a maximum of four DHCP servers.

```
host1(config)#ip dhcp-external server-address 10.10.10.1
```

3. Configure a default policy for subscribers, using a previously configured classifier group.

```
host1(config)#ip policy-list filterAll
host1(config-policy-list)#classifier-group filterGroupA
host1(config-policy-list-classifier-group)#filter
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
```

4. Configure a dynamic subscriber interface policy.

```
host1(config)#profile disableUser
host1(config-profile)#ip policy input filterAll
host1(config-profile)#ip policy output filterAll
host1(config-profile)#exit
```

5. Configure a route map.

```
host1(config)#route-map routeMapWest21
host1(config-route-map)#set ip interface-profile disableUser
host1(config-route-map)#exit
```

6. Enable autoconfiguration mode.

```
host1(config)#interface gigabitEthernet 12/0
host1(config-if)#ip address 192.168.1.1 255.255.255.0
host1(config-if)#ip auto-configure ip-subscriber include-primary
host1(config-if)#ip route-map ip-subscriber routeMapWest21
host1(config-if)#ip auto-detect ip-subscriber
host1(config-profile)#exit
```

## Subscriber Management Commands

---

This section describes the commands that you use to configure subscriber management. For commands related to a specific component, see the appropriate documentation.

- DHCP—[Chapter 8, Configuring DHCP](#)
- Policies—[JUNOS Policy Management Configuration Guide](#)
- QoS—[JUNOS Quality of Service Configuration Guide](#)
- Route maps—[JUNOS IP Services Configuration Guide, Chapter 1, Configuring Routing Policy](#)
- SDX software—SDX application documentation set

### **clear ip demux**

- Use to clear all dynamically created demultiplexer table entries associated with the route-map processing of the **set ip source-prefix** command.
  - **deny**—Drop addresses that appear in the source address range
  - **primary**—Associate the source prefix with the primary IP interface
- Example
 

```
host1(config-if)#clear ip demux
```
- There is no **no** version.

**domain**

- Use to specify a domain for an IP service profile.
- The domain is included in a username that is dynamically created by JUNOS subscriber management.
- The specify a domain name with up to 32 ASCII characters.
- Example  
`host1(config-service-profile)#domain eastcoast`
- Use the **no** version to remove the domain from the IP service profile.

**include circuit-identifier**

- Use to include the circuit identifier in the username that is dynamically created by JUNOS subscriber management.
- Specify one of the following circuit types: atm or vlan.
- Use the optional **prepend-circuit-type** keyword to specify that the circuit type is prepended to the circuit identifier in the username.
- Example  
`host1(config-service-profile)#include circuit-identifier atm prepend-circuit-type`
- Use the **no** version to disable inclusion of the circuit identifier in the username.

**include dhcp-option 82**

- Use to include a suboption of the DHCP relay agent information option (option 82) in the username that is dynamically created by JUNOS subscriber management.
- Specify one of the following suboptions: **agent-circuit-id** or **agent-remote-id**.
- Example  
`host1(config-service-profile)#include dhcp-option 82 agent-circuit-id`
- Use the **no** version to disable inclusion of the suboption in the username.

**include hostname**

- Use to include the router hostname in the username that is dynamically created by JUNOS subscriber management.
- Example  
`host1(config-service-profile)#include hostname`
- Use the **no** version to disable inclusion of the router hostname in the username.

***include ip-address***

- Use to include the IP address in the username that is dynamically created by JUNOS subscriber management.
- Example  
host1(config-service-profile)#**include ip-address**
- Use the **no** version to disable inclusion of the IP address in the username.

***include mac-address***

- Use to include the MAC address identifier in the username that is dynamically created by JUNOS subscriber management.
- Example  
host1(config-service-profile)#**include mac-address**
- Use the **no** version to disable inclusion of the MAC address in the username.

***include virtual-router-name***

- Use to include the virtual router name in the username that is dynamically created by JUNOS subscriber management.
- Example  
host1(config-service-profile)#**include virtual-router-name**
- Use the **no** version to disable inclusion of the virtual router name in the username.

***ip auto-configure ip-subscriber***

- Use to configure an IP interface to support creation of dynamic subscriber interfaces. The specified IP interface is considered the primary interface.
- The router creates the required dynamic subscriber interfaces when the IP address is assigned to the associated subscriber. The address might be assigned by an external DHCP server, the DHCP local server, or the packet detect feature.
- Use the **include-primary** keyword to specify that the primary interface can be assigned to a subscriber. Use the **exclude-primary** keyword to specify that the primary interface cannot be used for subscribers. The primary interface is not assigned to a subscriber by default.
- You can issue this command from Interface Configuration mode, Subinterface Configuration mode, or Profile Configuration mode.
- Example  
host1(config-if)#**ip auto-configure ip-subscriber include-primary**
- Use the **no** version to disable creation of dynamic subscriber interfaces associated with this primary IP interface. Use the **no** version with the **include-primary** keyword to specify that the primary interface is not assigned to a subscriber. Use the **no** version with the **exclude-primary** keyword to specify that the primary interface is assigned to a subscriber.

**ip auto-detect ip-subscriber**

- Use to set the router packet detect feature and specify that IP automatically detect packets that do not match any entries in the demultiplexer table. When an unmatched packet is detected, an event is generated that determines whether to create a dynamic subscriber interface or configure an existing interface.
- You can issue this command from Interface Configuration mode or Profile Configuration mode.
- Example  
host1(config-if)#**ip auto-detect ip-subscriber**
- Use the **no** version to restore the default, in which packet detection is disabled.

**ip destination-prefix**

- Use to specify a destination address for a subscriber interface or for a primary IP interface.
- Use the **deny** keyword to drop all packets that match the command.
- On the ERX-1440 router or the E320 router, you can configure up to 1024 subnets for static subscriber interfaces per primary IP interface when each subnet has a variable network mask that is less than /32. The number of subnets identifying a single route (/32) is still limited by the global maximum of 16,000 hosts per line module.
- Example  
host1(config-if)#**ip destination-prefix 10.0.0.0 255.0.0.0**
- Use the **no** version to remove the association between the interface and the specified IP destination address and mask.

**ip inactivity-timer**

- Use to configure the inactivity timer value.
- A dynamically created subscriber interface is deleted if it is inactive for a period longer than the inactivity timer value.
- On static interfaces, the subscriber's access route is removed when the inactivity timer is exceeded. When the subscriber logs back in, the timer is restarted.
- The timer value can in the range 1–65535 minutes.
- A timer value of 0 specifies that dynamically created subscriber interfaces are never deleted by the inactivity timer.
- Example  
host1(config-if)#**ip inactivity-timer 100**
- Use the **no** version to restore the default, in which inactivity timer feature is disabled.

**ip route-map ip-subscriber**

- Use to configure an interface to perform route-map processing, and to specify the route map that is applied to the IP interface subscriber. If no route map is specified, then all packets trigger the creation of a dynamic subscriber interface.
- You can issue this command from Interface Configuration mode or Profile Configuration mode.
- Example  

```
host1(config-if)#ip route-map ip-subscriber bostonRouteMap
```
- Use the **no** version to delete the route map.

**ip service-profile**

- Use to specify a service profile name and to enter IP Service Profile Configuration mode. Service profiles contain user and password information, and are used in route maps for subscriber management and to authenticate subscribers with RADIUS.
- You can specify a service profile name with up to 32 ASCII characters.
- You can create an IP service profile and reference it in a route map to configure IP subscribers on dynamic bridged Ethernet interfaces to support RADIUS authentication. If your router is running stateful SRP switchover (high availability), using an IP service profile for subscriber authentication is preferable to using either the **subscriber** command or the **atm atm1483 subscriber** command because these commands can suspend stateful SRP switchover on the router or prevent it from becoming active.  
  
 For more information, see [Authenticating Subscribers on Dynamic Bridged Ethernet over Static ATM Interfaces](#) in *JUNOS Link Layer Configuration Guide, Chapter 12, Configuring Dynamic Interfaces*, or [Authenticating Subscribers on Dynamic Bridged Ethernet over Dynamic ATM Interfaces](#) in *JUNOS Link Layer Configuration Guide, Chapter 13, Configuring Dynamic Interfaces Using Bulk Configuration*.
- Example  

```
host1(config)#ip service-profile class1Service
host1(config-service-profile)#
```
- Use the **no** version to delete the service profile.



**ip source-prefix**

- Use to specify a source address for a subscriber interface.
- Use the **deny** keyword to drop all packets that match the command.
- On the ERX-1440 router or the E320 router, you can configure up to 1024 subnets for static subscriber interfaces per primary IP interface when each subnet has a variable network mask that is less than /32. The number of subnets identifying a single route (/32) is still limited by the global maximum of 16,000 hosts per line module.
- Example  

```
host1(config-if)#ip source-prefix 10.0.0.0 255.0.0.0
```
- Use the **no** version to remove the association between the interface and the specified IP source address and mask.

**ip use-framed-routes ip-subscriber**

- Use to configure a static primary IP interface to use framed routes as source IP addresses when creating dynamic subscriber interfaces. The router uses the Framed-Route RADIUS attribute [22] sent in Access-Accept messages to apply framed routes to subscriber interfaces associated with the primary interface.
- Example  

```
host1(config-if)#ip use-framed-routes ip-subscriber
```
- Use the **no** version to disable the use of framed routes when creating dynamic subscriber interfaces associated with this primary IP interface.

**password**

- Use to specify the password for an IP service profile. The password is used as the dynamically created password by JUNOS subscriber management.
- You can specify a password with up to 32 ASCII characters.
- Example  

```
host1(config-service-profile)#password mypassword
```
- Use the **no** version to remove the password from the IP service profile.

**set ip interface-profile**

- Use to specify a dynamic subscriber interface profile that is used in the route map.
- Example  

```
host1(config)#route-map mapForEPort
host1(config-route-map)#set ip interface-profile disableUser
```
- Use the **no** version to delete the interface profile from the route map.

**set ip service-profile**

- Use to specify the name of a subscriber's service profile that is used in the route map.
- You can specify a service profile name with up to 32 ASCII characters.
- Example  
`host1(config-route-map)#set ip service-profile yourServiceProfile`
- Use the **no** version to remove the service profile from the route map.

**set ip source-prefix**

- Use to specify a source address range to be inserted into a specific interface, and the action to take with the range.
  - **deny**—Drop addresses that appear in the source address range
  - **primary**—Associate the source prefix with the primary IP interface
- Example  
`host1(config-route-map)#set ip source-prefix 10.10.30.0 255.255.255.0 primary`
- Use the **no** version to remove the source address range from the route map.

**user-name**

- Use to specify the username for an IP service profile. The username is used as the dynamically created username by JUNOS subscriber management.
- You can specify a username with up to 32 ASCII characters.
- Example  
`host1(config-service-profile)#user-name westford211`
- Use the **no** version to remove the user name from the IP service profile.

**user-prefix**

- Use to specify a user prefix for an IP service profile.
- This command appends the user prefix to the username that is dynamically created by JUNOS subscriber management.
- Example  
`host1(config-service-profile)#user-prefix xyz.atl`
- Use the **no** version to remove the user prefix from the IP service profile.

**vlan service-profile**

- Use to assign an IP service profile to a VLAN subinterface. Service profiles contain user and password information, and are used in route maps for subscriber management and to authenticate subscribers with RADIUS.
- You can specify a service profile name with up to 32 ASCII characters.
- Example

```
host1(config-profile)#vlan service-profile vlanClass1Service
host1(config-profile)#
```

- Use the **no** version to remove the service profile from the VLAN subinterface.

## Configuration Examples

---

This section contains examples of creating dynamic usernames and shows the usernames that are generated. The examples all use the following IP policy, interface profile, and route map:

- An IP policy that restricts access.

```
host1(config)#ip policy-list restrictAccess
host1(config-policy-list)#classifier-group *
host1(config-policy-list-classifier-group)#filter
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
host1(config)#
```

- An interface profile that references the restrictAccess policy.

```
host1(config)#profile atlInterfaceProfile
host1(config-profile)#ip policy input restrictAccess
host1(config-profile)#ip policy output restrictAccess
host1(config-profile)#exit
host1(config)#
```

- A route map that references the interface profile and the atlServiceProfile service profile.

```
host1(config)#route-map atlRouteMap
host1(config-route-map)#set interface-profile atlInterfaceProfile
host1(config-route-map)#set ip service-profile atlServiceProfile
host1(config-route-map)#exit
host1(config)#
```

Each example shows the configuration of a service profile that enables RADIUS authentication.

### Username with ATM Circuit Identifier and No Circuit Type

This example shows the steps to configure a service profile for a username that includes the ATM circuit identifier, but does not include the circuit type.

```
host1(config)#ip service-profile atlServiceProfile
host1(config-service-profile)#user-prefix xyzcorp.atl
host1(config-service-profile)#domain eastcoast
host1(config-service-profile)#include hostname
host1(config-service-profile)#include circuit-identifier atm
host1(config-service-profile)#exit
host1(config)#
```

The example generates the following username:

| user prefix | circuit identifier | domain     |
|-------------|--------------------|------------|
| xyzcorp.atl | 2.3.32.100         | @eastcoast |

The circuit identifier indicates a user at slot 2, port 3, with a virtual path identifier (VPI) of 32 and a virtual channel identifier (VCP) of 100.

### Username with VLAN Circuit Identifier and Circuit Type

This example shows the steps to configure a service profile for a username that includes a VLAN circuit identifier and the circuit type.

```
host1(config)#ip service-profile atlServiceProfile
host1(config-service-profile)#user-prefix xyzcorp.atl
host1(config-service-profile)#domain eastcoast
host1(config-service-profile)#include hostname
host1(config-service-profile)#include circuit-identifier vlan prepend-circuit-type
host1(config-service-profile)#exit
```

The example generates the following username:

| user prefix | circuit type | circuit identifier | domain     |
|-------------|--------------|--------------------|------------|
| xyzcorp.atl | vlan         | 1.0.0.45           | @eastcoast |

The circuit identifier indicates a user on slot 1, port 0, no stacked vlan, and a vlan ID of 45.

## Username with MAC Address

This example shows the steps to configure a service profile that generates a username that includes a MAC address.



**NOTE:** Including a MAC address in a username works only for DHCP users. It does not work for IP subscribers that have statically configured IP addresses.

```
host1(config)#ip service-profile atlServiceProfile
host1(config-service-profile)#user-prefix xyzcorp.atl
host1(config-service-profile)#domain eastcoast
host1(config-service-profile)#include hostname
host1(config-service-profile)#include circuit-identifier vlan
host1(config-service-profile)#include mac-address
host1(config-service-profile)#include dhcp-option 82 agent-circuit-id
host1(config-service-profile)#exit
host1(config)#
```

The example generates the following username, which includes the MAC address:

| user prefix | circuit identifier | mac-address    | domain     |
|-------------|--------------------|----------------|------------|
| xyzcorp.atl | 1.0.0.45           | 1234.5678.9012 | @eastcoast |

## Monitoring Subscriber Management

This section describes commands you can use to display status information and statistics for the subscriber management environment.

### **show ip service-profile**

- Use to display information for all IP service profiles or for a specific profile.
- Field descriptions
  - ip service-profile—Name of profile
  - user-name—Username used to retrieve information from RADIUS for subscriber interfaces
  - user-prefix—User prefix used to retrieve information from RADIUS for subscriber interfaces
  - domain—Domain used to retrieve information from RADIUS for subscriber interfaces
  - include ip-address—IP address is included in the service profile
  - include virtual-router-name—Virtual router is included in the service profile
  - include mac-address—MAC address is included in the service profile
  - include circuit-identifier—Circuit identifier that is included in the service profile; atm or vlan, and whether the circuit type is prepended

- include hostname—Router hostname is included in the service profile
- include dhcp-option 82—Suboptions of DHCP option 82 are included in the service profile: agent-circuit-id or agent-remote-id
- password—Password used to retrieve information from RADIUS for subscriber interfaces

■ Example

```
host1#show ip service-profile
ip service-profile west500
 user-name: finance22
 user-prefix: xyz.bos
 domain: xyzcorp.net
 include virtual-router-name
 include mac-address
 include circuit-identifier atm prepend-circuit-type
 password: 4398aa

ip service-profile at1SerPro9
 user-name: salesCorp
 domain: xyzcorp.net
 include virtual-router-name
 include circuit-identifier vlan
 password: u473qv
```

### **show ip-subscriber**

- Use to display information about active IP subscribers that were created by the JUNOS software's subscriber management feature.
- Field descriptions
  - Id—ID of the subscriber
  - User Name—Username used to retrieve information from RADIUS for the subscriber interface
  - Ip Address—IP address of the subscriber interface
  - Virtual Router—Name of the virtual router on which the subscriber interface is configured
  - Interface—Name of subscriber interface; **ip** indicates that subscriber manager created this interface
  - Login Time—Day, date, and time that the subscriber logged in
  - Mac Address—MAC address of the subscriber
  - Profile Handle—AAA profile handle
  - Interface Profile—Interface profile name used to configure the subscriber interface
  - Service Profile—IP service profile name used by subscriber management to authorize and configure the subscriber interface with AAA
  - Option 82—DHCP relay agent information (option 82) circuit identifier that describes the physical interface location associated with the subscriber

## ■ Example 1

```
host1#show ip-subscriber 2835349506
```

| Id         | User Name      | Ip Address  | Virtual Router | Interface     |
|------------|----------------|-------------|----------------|---------------|
| 2835349506 | user1@isp1.com | 192.168.0.1 | default        | ip192.168.0.1 |

| Id         | Login time               |
|------------|--------------------------|
| 2835349506 | WED AUG 23 20:46:24 2006 |

## ■ Example 2

```
host1#show ip-subscriber detail
```

| Subscriber List |                |             |                |               |
|-----------------|----------------|-------------|----------------|---------------|
| Id              | User Name      | Ip Address  | Virtual Router | Interface     |
| 2835349506      | user1@isp1.com | 192.168.0.1 | default        | ip192.168.0.1 |

| Id         | Login Time               | Mac Address    | Profile Handle |
|------------|--------------------------|----------------|----------------|
| 2835349506 | WED AUG 23 20:46:24 2006 | 3000.0001.9365 | 13631489       |

| Id         | Interface Profile | Service Profile | Option 82        |
|------------|-------------------|-----------------|------------------|
| 2835349506 | myProfile         | profile22       | FastEthernet 3/1 |





## Chapter 10

# Configuring Subscriber Interfaces

This chapter describes how to configure static and dynamic subscriber interfaces for remote access to the E-series router. This chapter contains the following sections:

- [Overview](#) on page 417
- [Platform Considerations](#) on page 422
- [References](#) on page 423
- [Dynamic Creation of Subscriber Interfaces](#) on page 424
- [Configuring Static Subscriber Interfaces](#) on page 427
- [Configuring Dynamic Subscriber Interfaces](#) on page 433
- [Monitoring Subscriber Interfaces](#) on page 445

## Overview

---

You can configure E-series routers to create subscriber interfaces statically or dynamically.

The following list shows the underlying (layer 2) interfaces on which you can currently configure each type of subscriber interface.

- Static subscriber interfaces
  - Bridged Ethernet over ATM (with and without VLANs)
  - Fast Ethernet (with and without VLANs)
  - Gigabit Ethernet (with and without VLANs)
  - 10-Gigabit Ethernet (with and without VLANs)
  - IP over ATM
  - POS
  - Generic Routing Encapsulation (GRE) tunnels

- Dynamic subscriber interfaces
  - Bridged Ethernet over ATM (with and without VLANs)
  - Fast Ethernet (with and without VLANs)
  - Gigabit Ethernet (with and without VLANs)
  - 10-Gigabit Ethernet (with and without VLANs)
  - GRE tunnels

For information about platform support for subscriber interfaces, see [Platform Considerations](#) on page 422.

### **Relationship to Shared IP Interfaces**

A subscriber interface is an extension of a *shared IP interface*. A shared IP interface is one of a group of IP interfaces that use the same layer 2 interface.

Shared IP interfaces are unidirectional—they can transmit but not receive traffic. In contrast, subscriber interfaces are bidirectional—they can both receive and transmit traffic.

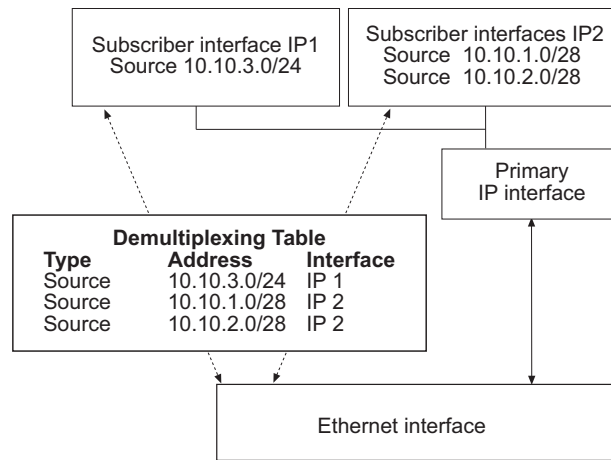
For details about shared IP interfaces, see [Shared IP Interfaces](#) in *JUNOS IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP*.

### **Relationship to Primary IP Interfaces**

A subscriber interface operates only with a *primary IP interface*—a normal IP interface on a supported layer 2 interface, such as Ethernet. You create a primary interface by assigning an IP address to the Ethernet interface. Although you can configure a subscriber interface directly on an Ethernet interface, the subscriber interface does not operate until you assign an IP address to the Ethernet interface.

To configure a subscriber interface you must associate either a source address or a destination address with the interface. The router receives packets on a subscriber interface after demultiplexing the packet according to the specified source address or destination address. You can associate multiple source addresses or multiple destination addresses with a subscriber interface. However, a single primary interface and its associated subscriber interfaces can only demultiplex source addresses or destination addresses at any given time.

For example, [Figure 16](#) illustrates the relationship between subscriber interfaces, an associated primary IP interface, and an associated Ethernet interface.

**Figure 16: Subscriber Interfaces over Ethernet**

g013303

When the router receives traffic on a primary interface, the primary interface performs a lookup in its demultiplexing table. If the result of the lookup is a subscriber interface, the traffic is received on the associated subscriber interface.



**NOTE:** You can use the **set dhcp relay giaddr-selects-interface** command to specify that the primary interface is identified by information in the giaddr field of DHCP ACK messages. By default, the router identifies the primary interface based on the interface used by the DHCP-destined packets. See [Using the Giaddr to Identify the Primary Interface for Dynamic Subscriber Interfaces](#) on page 319.

## Ethernet Interfaces and VLANs

In the absence of VLANs, Ethernet does not have a demultiplexing layer. A subscriber interface adds a demultiplexing layer for an Ethernet interface that is configured without VLANs. Using subscriber interfaces, the router can demultiplex or separate the traffic associated with different subscribers.

You can configure subscriber interfaces with VLANs. If you do so, the E-series router demultiplexes packets by using first the VLAN and then the subscriber interface.

## Moving Interfaces

A shared IP interface that has associated subscriber demultiplexing attributes retains these attributes when it moves.

For details about moving shared IP interfaces, see [Moving IP Interfaces](#) in *JUNOS IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP*.

## Preventing IP Spoofing

You can prevent IP spoofing on subscriber interfaces by using media access control (MAC) address validation.

For information about configuring MAC address validation, see [MAC Address Validation](#) in *JUNOS IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP*.

## Routing Protocols

You configure unicast routing protocols on subscriber interfaces in the same way that you configure routing protocols on primary IP interfaces, provided that you configure them to use unicast addressing when communicating with a peer. You can also enable multicast routing protocols such as IGMP on subscriber interfaces; however, we do not recommend this type of configuration.

## Policies and QoS

You can configure policies, such as rate limiting and filtering, and quality of service (QoS) for subscriber interfaces in the same way that you do for primary IP interfaces. For more information, see the [JUNOS Policy Management Configuration Guide](#) and the [JUNOS Quality of Service Configuration Guide](#).

## Applications

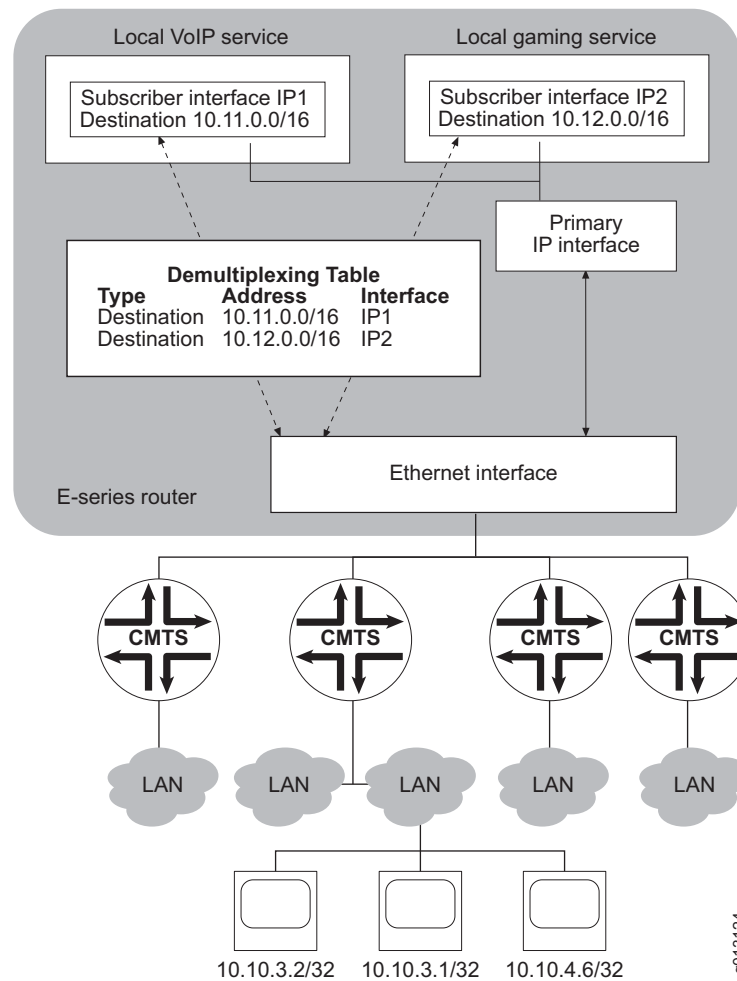
In a cable modem network, service providers can use subscriber interfaces to:

- Direct traffic toward special local content in the network
- Differentiate traffic for virtual private networks (VPNs)

### Directing Traffic Toward Special Local Content

[Figure 17](#) shows an example of a cable modem network. Multiple cable modem termination systems (CMTSs) connect to multiple shared media access LANs. Many subscribers connect to each LAN.

In this example, the service provider uses subscriber interfaces to direct traffic toward special local content on the network: a voice over Internet Protocol (VoIP) service on network 10.11.0.0/16, or a local gaming service on network 10.12.0.0/16. Rate limits and policies on the subscriber interface customize the service level for the associated service. In this application, the E-series router is the first-hop router for the subscribers, and the subscriber interfaces demultiplex traffic based on the destination address.

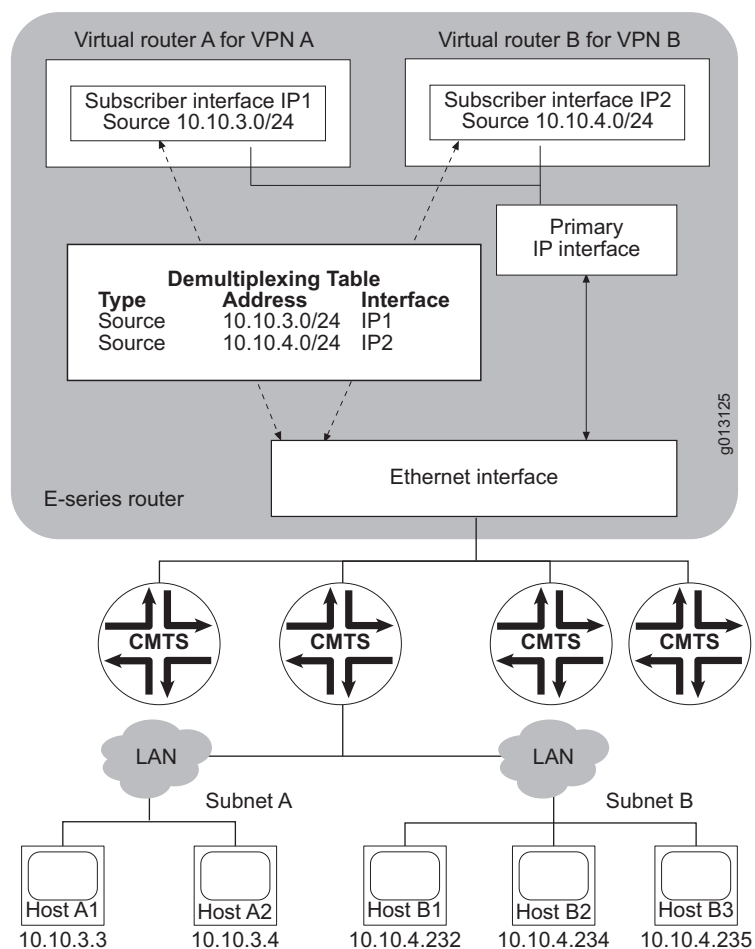
**Figure 17: Subscriber Interfaces in a Cable Modem Network**

For instructions on configuring the application shown in [Figure 17](#), see [Using a Destination Address to Demultiplex Traffic](#) on page 427.

### Differentiating Traffic for VPNs

Similarly, service providers can use subscriber interfaces to differentiate traffic for VPNs. [Figure 18 on page 422](#) shows an example of this application.

Customers on subnet A need to connect to VPN A, and customers on subnet B need to connect to VPN B. The E-series router connects to VPN A through virtual router A and to VPN B through virtual router B. Using two subscriber interfaces on the same primary interface (one on virtual router B and one on virtual router A), the E-series router can separate the traffic from subnets A and B. Because the E-series router is forwarding traffic in this application, the shared IP interface should demultiplex the traffic by using a source address.

**Figure 18: Associating Subnets with a VPN Using Subscriber Interfaces**

For instructions on configuring the application shown in [Figure 18](#), see [Using a Source Address to Demultiplex Traffic](#) on page 429.

## Platform Considerations

For information about modules that support subscriber interfaces on the ERX-7xx models, ERX-14xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, ERX Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support subscriber interfaces.

For information about modules that support subscriber interfaces on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support subscriber interfaces.

## Interface Specifiers

The configuration task examples in this chapter use the *slot/port* format to specify an interface. However, the interface specifier format that you use depends on the router that you are using.

For ERX-7xx models, ERX-14xx models, and ERX-310 routers, use the *slot/port* format. For example, the following command specifies a Gigabit Ethernet interface on slot 0, port 1 of an ERX-7xx model, ERX-14xx model, or ERX-310 router.

```
host1(config)#interface gigabitEthernet 0/1
```

For E120 and E320 routers, use the *slot/adapter/port* format, which includes an identifier for the bay in which the I/O adapter (IOA) resides. In the software, adapter 0 identifies the right IOA bay (E120 router) and the upper IOA bay (E320 router); adapter 1 identifies the left IOA bay (E120 router) and the lower IOA bay (E320 router). For example, the following command specifies a Gigabit Ethernet interface on slot 5, adapter 0, port 0 of an E320 router.

```
host1(config)#interface gigabitEthernet 5/0/0
```

For more information about supported interface types and specifiers on E-series routers, see [Interface Types and Specifiers](#) in *JUNOS Command Reference Guide, About This Guide*.

## References

---

For more information about the DHCP local server and DHCP external server, which are used in dynamic creation of subscriber interfaces, consult the following resources:

- [Chapter 8, Configuring DHCP](#)
- [RFC 2131—Dynamic Host Configuration Protocol \(March 1997\)](#)

## Dynamic Creation of Subscriber Interfaces

---

As an alternative to creating static subscriber interfaces, you can configure E-series routers to create subscriber interfaces dynamically.

When you create a static subscriber interface, as described in [Configuring Static Subscriber Interfaces](#) on page 427, each layer in the interface stack is created through an existing configuration mechanism such as command-line interface (CLI) or Simple Network Management Protocol (SNMP).

By contrast, the router creates dynamic subscriber interfaces on demand, in response to an external event. Two types of external events can cause dynamic creation of subscriber interfaces: when a Dynamic Host Configuration Protocol (DHCP) event occurs or when the router detects a packet.

### DHCP Servers

The DHCP event that triggers dynamic creation of subscriber interfaces occurs when either a local DHCP server or external DHCP server assigns an IP address to a subscriber that has issued a DHCP request. After the DHCP server assigns the IP address and the router creates the associated dynamic subscriber interface, the subscriber can access required network services.

#### DHCP Local Server and Address Allocation

You can configure the DHCP local server to operate in either equal-access mode or standalone mode.

In standalone mode, the DHCP local server provides a basic DHCP service. The server receives a client request for an IP address and immediately allocates the subscriber an IP address from one of the local address pools.

In equal-access mode, the DHCP local server works with Juniper Networks Service Deployment System (SDX) and authorization, accounting, and address assignment utility (AAAA) to provide an advanced subscriber configuration and management service. After the subscriber is authenticated through RADIUS, the DHCP server assigns the subscriber an IP address with a long lease time. This assignment of an IP address triggers the creation of dynamic subscriber interfaces.

For more information about the DHCP servers and the SDX application, see the following chapters:

- [Chapter 8, Configuring DHCP](#)
- [SDX Getting Started Guide, Chapter 1, Product Overview](#)

#### DHCP External Server and Address Allocation

With DHCP external server, all communication between the subscriber and the DHCP server is monitored by the E-series router. The subscriber requests an address from the DHCP server through the E-series router. After the subscriber receives an IP address, the subscriber can access the Internet and use the value-added services provided by the E-series router and by the SDX software. The edge network must be using a DHCP relay function.



The services provided by integrating the E-series router's DHCP external server application with SDX software are similar to those provided when the DHCP local server is integrated with SDX software. For more information, see *SDX Getting Started Guide, Chapter 1, Product Overview*.

### DHCP Relay Configuration

When you are configuring dynamic subscriber interface support, and you configure DHCP relay in the same virtual router as the dynamic subscriber interfaces, you must use the **set dhcp relay inhibit-access-route-creation** command to ensure that DHCP relay does not install access internal routes. Otherwise, DHCP relay will overwrite the access internal routes that are originally created for the subscriber interface.

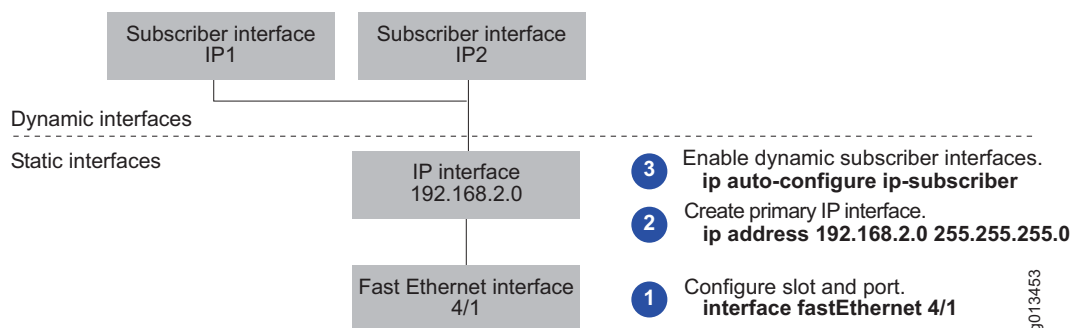
### Supported Configurations

E-series routers currently support dynamic creation of subscriber interfaces with DHCP servers in the following configurations:

- IP over Ethernet
- IP over VLAN over Ethernet
- IP over bridged Ethernet over ATM

For example, [Figure 19](#) shows the interface stacking in an IP over Ethernet dynamic subscriber interface configuration. The illustration indicates which layers in the stack are static and dynamic, and identifies the CLI commands typically used to create the configuration.

**Figure 19: IP over Ethernet Dynamic Subscriber Interface Configuration**



As shown in [Figure 19](#), issuing the **ip auto-configure ip-subscriber** command configures the primary IP interface to enable dynamic creation of subscriber interfaces. However, the router does not actually create the dynamic subscriber interface until the DHCP server assigns an IP address to the associated subscriber.

To configure each supported configuration, see [Configuring Dynamic Subscriber Interfaces](#) on page 433.

## Packet Detection

For GRE tunnel interfaces, the event that triggers dynamic creation of subscriber interfaces occurs when the router receives a packet with a source IP address that is not in the demultiplexer table. In this case, the primary IP interface must be in autoconfiguration mode.

Packet detection is the only method of dynamically creating subscriber interfaces on GRE tunnel interfaces; you cannot use DHCP local server or DHCP external server.

Issuing the **ip auto-configure ip-subscriber** command configures the primary IP address to enable dynamic configuration of subscriber interfaces. Unlike DHCP configurations, the router creates the dynamic subscriber interface when it receives the first packet that contains the subscriber's IP address as the source address.

In addition, a dynamic subscriber interface becomes inactive after a period of time in which the router receives no packets that contain the subscriber's IP address as the source address. You can configure the period of time by issuing the **ip inactivity-timer** command.

To configure dynamic creation of subscriber interfaces on GRE tunnel interfaces, see [Configuring Dynamic Subscriber Interfaces](#) on page 433.

## Designating Traffic for the Primary IP Interface

When dynamic creation of subscriber interfaces is enabled on the primary IP interface (by means of the **ip auto-configure ip-subscriber** command), you can use the **ip source-prefix** command to specify the source address of traffic that is destined for the primary IP interface instead of the subscriber interface. If the DHCP server (for DHCP server configurations) or the router (for packet detection configurations) then assigns a subscriber an IP address matching this source prefix, the router does not create a dynamic subscriber interface for that address.

## Using Framed Routes

You can use the **ip use-framed-routes ip-subscriber** command to enable a primary IP interface to use framed routes as source IP addresses when creating dynamic subscriber interfaces. The framed routes are applied to the dynamic subscriber interface during configuration so traffic from the subsets can traverse the interface. By applying framed routes in this fashion, you can extend the per-subscriber interface management to any subnetworks behind the dynamic subscriber interface. RADIUS includes the Framed-Route attribute [22] in Access-Accept messages to specify the route in the following format:

Framed-Route = *ipAddress/mask nextHop*

## Configuring Static Subscriber Interfaces

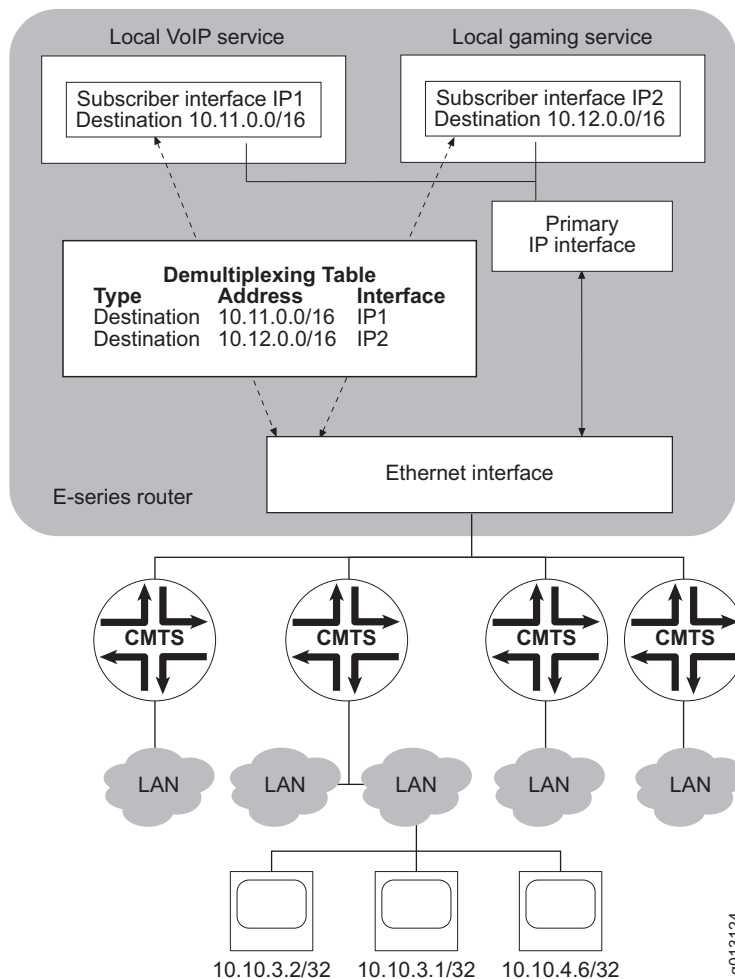
You can configure static subscriber interfaces on ATM, Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, or POS layer 2 interfaces.

The examples in this section show how to configure static subscriber interfaces on a Fast Ethernet interface, but the steps for configuring static subscriber interfaces over other supported layer 2 interface types are similar.

### Using a Destination Address to Demultiplex Traffic

The example in [Figure 20](#) shows how you can use static subscriber interfaces to direct traffic toward special local content on the network, based on the traffic's destination address. In this application, a local VoIP service is on network 10.11.0.0/16, and a local gaming service is on network 10.12.0.0/16.

**Figure 20: Subscriber Interfaces Using a Destination Address to Demultiplex Traffic**



To configure the static subscriber interfaces shown in [Figure 20](#), perform the following steps:

1. Configure a primary IP interface on a supported layer 2 interface.

- a. Create a layer 2 interface.

```
host1(config)#interface fastEthernet 3/1
```

- b. Create a primary IP interface.

```
host1(config-if)#ip address 10.1.1.1 255.0.0.0
```

- c. Configure the primary interface to use a destination address to demultiplex traffic. (By default, a source address is used to demultiplex traffic.)

```
host1(config-if)#ip demux-type da-prefix
```

- d. Exit Interface Configuration mode.

```
host1(config-if)#exit
```

2. Configure subscriber interface IP1.

- a. Create the shared IP interface.

```
host1(config)#interface ip ip1
```

- b. Associate the shared IP interface with the layer 2 interface by using one of the following methods:

- Static

```
host1(config-if)#ip share-interface fastEthernet 3/1
```

- Dynamic

```
host1:vr-a:vrf-1(config-if)#ip share-nexthop 10.1.1.2
```

- c. To fully configure the shared interface, assign an address or make it unnumbered.

```
host1(config-if)#ip unnumbered loopback 0
```

- d. Specify the destination addresses for the subscriber interface to use to demultiplex traffic.

```
host1(config-if)#ip destination-prefix 10.11.0.0 255.255.0.0
```

- e. Exit Interface Configuration mode.

```
host1(config-if)#exit
```

- Repeat Step 2 to configure subscriber interface IP2.

```

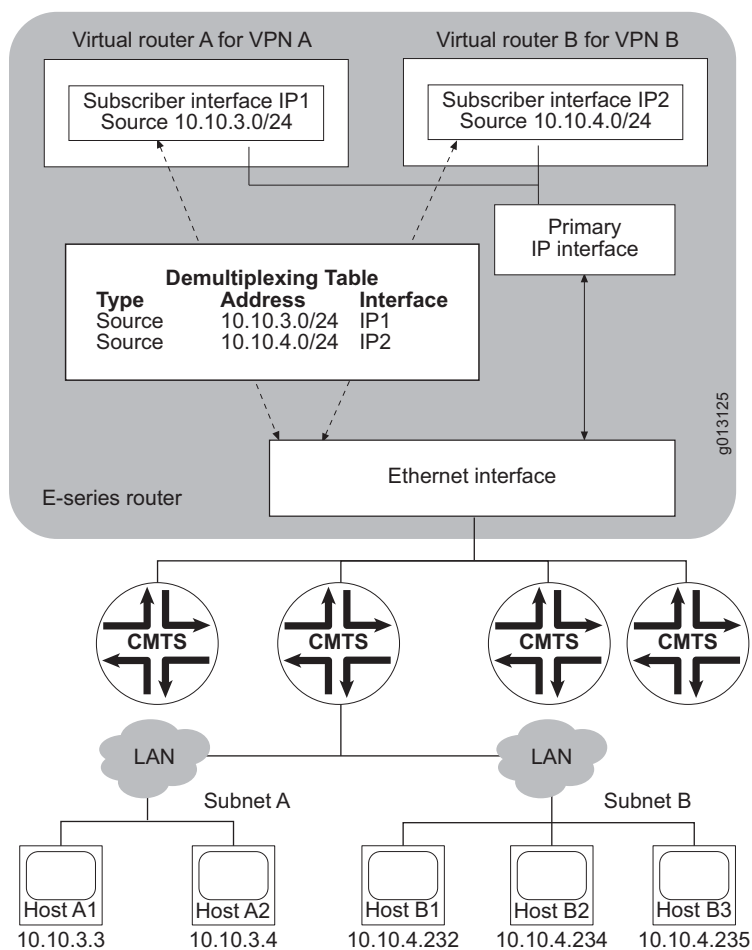
host1(config)#interface ip ip2
host1(config-if)#ip share-interface fastEthernet 3/1
host1(config-if)#ip unnumbered loopback 0
host1(config-if)#ip destination-prefix 10.12.0.0 255.255.0.0

```

### Using a Source Address to Demultiplex Traffic

Figure 21 shows how you can use static subscriber interfaces to differentiate traffic for VPN access, based on the traffic's source address.

**Figure 21: Subscriber Interfaces Using a Source Address to Demultiplex Traffic**



To configure the static subscriber interfaces shown in [Figure 21](#), perform the following steps:

1. Configure a primary IP interface on a supported layer 2 interface.

- a. Create a layer 2 interface.

```
host1(config)#interface fastEthernet 4/1
```

- b. Create a primary IP interface.

```
host1(config-if)#ip address 10.1.1.1 255.255.255.0
```

- c. Exit Interface Configuration mode.

```
host1(config-if)#exit
```

2. Configure subscriber interface IP1.

- a. Create the shared IP interface.

```
host1(config)#virtual-router vra
Proceed with new virtual-router creation? [confirm] yes
host1:vra(config)#interface ip ip1
```

- b. Associate the shared IP interface with the layer 2 interface by using one of the following methods:

- Static

```
host1:vra(config-if)#ip share-interface fastEthernet 4/1
```

- Dynamic

```
host1:vra(config-if)#ip share-nexthop 10.1.1.2
```

- c. To fully configure the shared interface, assign an address or make it unnumbered.

```
host1:vra(config-if)#ip unnumbered loopback 0
```

- d. Specify the source addresses for the subscriber interface to use to demultiplex traffic, then exit Interface Configuration mode.

```
host1:vra(config-if)#ip source-prefix 10.10.3.0 255.255.255.0
host1:vra(config-if)#exit
```

3. Create a static route that sends traffic for destination address 10.10.3.0 to subscriber interface IP1.

```
host1:vra(config)#ip route 10.10.3.0 255.255.255.0 ip ip1
```

4. Repeat Step 2 to configure subscriber interface IP2.

```
host1(config)#virtual-router vrb
Proceed with new virtual-router creation? [confirm] yes
host1:vrp(config)#interface ip ip2
host1:vrp(config-if)#ip share-interface fastEthernet 4/1
host1:vrp(config-if)#ip unnumbered loopback 0
host1:vrp(config-if)#ip source-prefix 10.10.4.0 255.255.255.0
host1:vrp(config-if)#exit
```

5. Create a static route that sends traffic for destination address 10.10.4.0 to subscriber interface IP2.

```
host1:vrp(config)#ip route 10.10.4.0 255.255.255.0 ip ip2
```

6. Specify that DHCP relay does not install host routes—this avoids a conflict that can causes undesirable ARP behavior.

```
host1(config)#set dhcp relay inhibit-access-route-creation
```

For details about the cause of this conflict and the use of the **set dhcp relay inhibit-access-route-creation** command to avoid the conflict, see [DHCP Relay Configuration and ARP Spoof Checking](#) on page 319.

### **interface ip**

- Use to create an IP interface to share a layer 2 interface.
- Use the specified name to refer to the shared IP interface; you cannot use the layer 2 interface to refer to the shared IP interface, because the shared interface can be moved.
- Example  

```
host1(config)#interface ip si0
```
- Use the **no** version to delete the IP interface.

### **ip demux-type da-prefix**

- Use to specify that the router use a destination address to demultiplex traffic for the subscriber interface.
- Example  

```
host1(config-if)#ip demux-type da-prefix
```
- Use the **no** version to restore the default situation in which the router uses a source address to demultiplex traffic.

***ip destination-prefix***

- Use to specify a destination address for a subscriber interface or for a primary IP interface.
- On the ERX-1440 router or the E320 router, you can configure up to 1024 subnets for static subscriber interfaces per primary IP interface when each subnet has a variable network mask that is less than /32. The number of subnets identifying a single route (/32) is still limited by the global maximum of 16,000 hosts per line module.
- Example  

```
host1(config-if)#ip destination-prefix 196.168.2.2 255.0.0.0
```
- Use the **no** version to remove the association between the interface and the specified IP destination address and mask.

***ip share-interface***

- Use to specify the layer 2 interface for this IP interface to share. The command fails if the layer 2 interface does not yet exist.
- If you issue this command on a shared IP interface, you cannot issue the **ip share-nexthop** command for the interface.
- After creating the shared IP interface, you can configure it as you do any other IP interface.
- The shared interface is operationally up when the layer 2 interface is operationally up and IP is properly configured.
- You can create operational shared IP interfaces in the absence of a primary IP interface.
- Example  

```
host1(config-if)#ip share-interface atm 5/3.101
```
- Use the **no** version to remove the association between the layer 2 interface and the shared IP interface. You can delete shared and primary IP interfaces independently.

***ip share-nexthop***

- Use to specify that the shared IP interface dynamically tracks a next hop. If the next hop changes, the shared IP interface moves to the new layer 2 interface associated with the IP interface toward the new next hop.
- If you issue this command on a shared IP interface, you cannot issue the **ip share-interface** command for the interface.
- If you specify a virtual router, the command fails if the VR does not already exist. If you do not specify a VR, the current VR is assumed.
- After creating the shared IP interface, you can configure it as you do any other IP interface.
- The shared interface is operationally up when the layer 2 interface associated with the specified next hop is operationally up and IP is properly configured.



- Example  
host1(config-if)#**ip share-nexthop 192.168.10.16**
- Use the **no** version to halt tracking of the next hop.

#### **ip source-prefix**

- Use to specify a source address for a subscriber interface.
- On the ERX-1440 router or the E320 router, you can configure up to 1024 subnets for static subscriber interfaces per primary IP interface when each subnet has a variable network mask that is less than /32. The number of subnets identifying a single route (/32) is still limited by the global maximum of 16,000 hosts per line module.
- Example  
host1(config-if)#**ip source-prefix 192.168.0.0 255.0.0.0**
- Use the **no** version to remove the association between the interface and the specified IP source address and mask.

## **Configuring Dynamic Subscriber Interfaces**

---

You can configure dynamic subscriber interfaces in the following configurations:

- IP over Ethernet
- IP over VLAN over Ethernet
- IP over bridged Ethernet over ATM
- GRE tunnels

The following sections describe how to create each of these basic configurations. In addition, [Dynamic Subscriber Interface Configuration Example](#) on page 438, provides a detailed sample configuration.

### **Configuring Dynamic Subscriber Interfaces over Ethernet**

To configure a dynamic subscriber interface in an IP over Ethernet configuration by using DHCP events, perform the following steps:

1. Configure the DHCP server.

For instructions, see [Configuring the DHCP Local Server](#) in [Chapter 8, Configuring DHCP](#).

2. Specify a Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet port.

```
host1(config)#interface fastEthernet 4/1
```

3. Create the primary IP interface by assigning an IP address and mask to the Ethernet interface (or make it unnumbered).

```
host1(config-if)#ip address 192.168.2.0 255.255.255.0
```

4. Configure the primary IP interface to enable dynamic creation of subscriber interfaces.

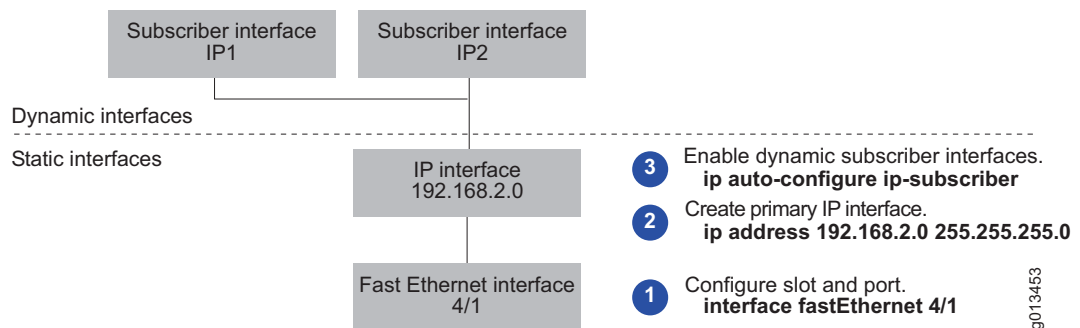
```
host1(config-if)#ip auto-configure ip-subscriber
```

5. (Optional) Specify the source address of traffic that is destined for the primary IP interface.

```
host1(config-if)#ip source-prefix 192.168.2.0 255.255.255.0
```

Figure 22 shows the interface stack built for this configuration.

**Figure 22: IP over Ethernet Dynamic Subscriber Interface Configuration**



## Configuring Dynamic Subscriber Interfaces over VLANs

To configure a dynamic subscriber interface in an IP over VLAN over Ethernet configuration by using DHCP events, perform the following steps:

1. Configure the DHCP server.

For instructions, see [Configuring the DHCP Local Server](#) in [Chapter 8, Configuring DHCP](#).

2. Specify a Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet port.

```
host1(config)#interface gigabitEthernet 1/0
```

3. Specify VLAN as the encapsulation method on the interface. This command creates the VLAN major interface.

```
host1(config-if)#encapsulation vlan
```

4. Create a VLAN subinterface by adding a subinterface number to the interface identification command.

```
host1(config-if)#interface gigabitEthernet 1/0.1
```

5. Assign a unique VLAN ID to the VLAN subinterface.

```
host1(config-if)#vlan id 101
```

6. Create the primary IP interface by assigning an IP address and mask to the VLAN subinterface (or make it unnumbered).

```
host1(config-if)#ip address 192.168.2.10 255.255.255.0
```

7. Configure the primary IP interface to enable dynamic creation of subscriber interfaces.

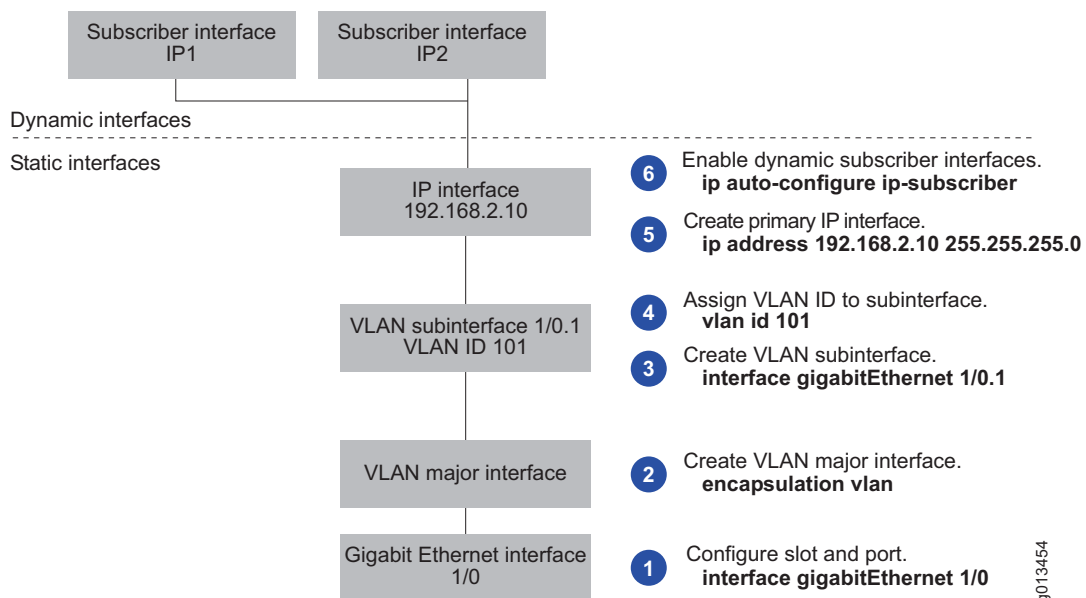
```
host1(config-if)#ip auto-configure ip-subscriber
```

8. (Optional) Specify the source address of traffic that is destined for the primary IP interface.

```
host1(config-if)#ip source-prefix 192.168.2.10 255.255.255.0
```

Figure 23 on page 435 shows the interface stack built for this configuration.

**Figure 23: IP over VLAN over Ethernet Dynamic Subscriber Interface Configuration**



## Configuring Dynamic Subscriber Interfaces over Bridged Ethernet

To configure a dynamic subscriber interface in an IP over bridged Ethernet over ATM configuration by using DHCP events, perform the following steps:

1. Configure DHCP server.

For instructions, see [Configuring the DHCP Local Server](#) in *Chapter 8, Configuring DHCP*.

2. Create an ATM major interface.

```
host1(config)#interface atm 3/3
```

3. Create an ATM 1483 subinterface.

```
host1(config-if)#interface atm 3/3.1
```

4. Configure an associated PVC for the ATM 1483 subinterface by specifying the VCD, the VPI, the VCI, and the encapsulation type.

```
host1(config-subif)#atm pvc 10 100 22 aal5snap
```

5. Specify bridged Ethernet as the encapsulation method on the ATM 1483 subinterface.

```
host1(config-subif)#encapsulation bridge1483
```

6. Create the primary IP interface by assigning an IP address and mask to the bridged Ethernet interface (or make it unnumbered).

```
host1(config-subif)#ip address 192.168.2.20 255.255.255.0
```

7. Configure the primary IP interface to enable dynamic creation of subscriber interfaces.

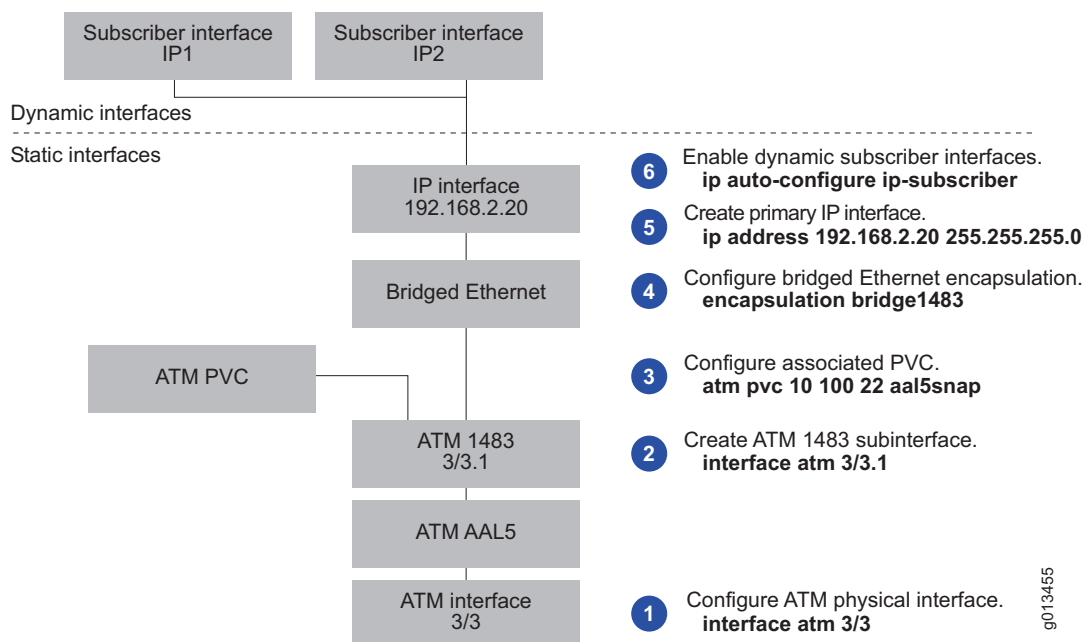
```
host1(config-subif)#ip auto-configure ip-subscriber
```

8. (Optional) Specify the source address of traffic that is destined for the primary IP interface.

```
host1(config-subif)#ip source-prefix 192.168.2.20 255.255.255.0
```

Figure 24 shows the interface stack built for this configuration.

**Figure 24: IP over Bridged Ethernet over ATM Dynamic Subscriber Interface Configuration**



### Configuring Dynamic Subscriber Interfaces over GRE Tunnels

To configure a dynamic subscriber interface in an GRE tunnel configuration by using packet detection, perform the following steps:

1. Create a GRE tunnel interface.

For instructions, see [Configuration Tasks](#) in *JUNOS IP Services Configuration Guide, Chapter 10, Configuring IP Tunnels*.

2. Create the primary IP interface by assigning an IP address and mask to the bridged Ethernet interface (or make it unnumbered).

```
host1(config-subif)#ip address 192.168.2.20 255.255.255.0
```

3. Configure the packet detect feature and specify that IP automatically detect packets that do not match any entries in the demultiplexer table.

```
host1(config-if)#ip auto-detect ip-subscriber
```

4. Configure the primary IP interface to enable dynamic creation of subscriber interfaces.

```
host1(config-subif)#ip auto-configure ip-subscriber
```

5. (Optional) Specify the IP inactivity timer.

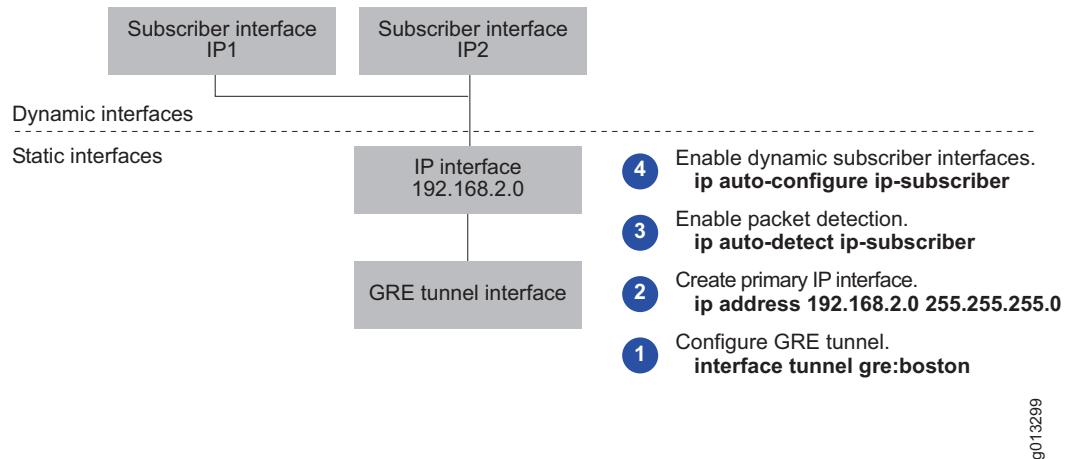
```
host1(config-subif)#ip inactivity-timer 100
```

6. (Optional) Specify the source address of traffic that is destined for the primary IP interface.

```
host1(config-subif)#ip source-prefix 192.168.2.0 255.255.255.0
```

Figure 25 shows the interface stack built for this configuration.

**Figure 25: GRE Tunnel Dynamic Subscriber Interface Configuration**



### Dynamic Subscriber Interface Configuration Example

The procedure in this section shows how to configure dynamic subscriber interfaces by using the same loopback interface referenced by multiple unnumbered IP interfaces. Instead of assigning a different IP address to each physical interface, this example assigns an IP address to a loopback interface (loopback 0). Each physical interface is then configured as an unnumbered IP interface, referencing the same loopback interface. This example uses a DHCP local server.

This approach has the following benefits:

- A loopback interface provides a stable IP address that can minimize the impact if a physical interface in the network goes down.
- Unnumbered IP interfaces preserve valuable IP address space.

To configure dynamic subscriber interfaces, perform the following steps:

1. Enable the DHCP local server for standalone mode.

```
host1(config)#service dhcp-local standalone
```

2. Access DHCP Local Pool Configuration mode for the local address pool.

```
host1(config)#ip dhcp-local pool ispWestford
```

3. Specify the enduring IP addresses that the DHCP local server can assign from the local address pool.

```
host1(config-dhcp-local)#network 10.20.0.0 255.255.192.0
```

4. Specify the router to forward traffic from the IP addresses to destinations on other subnets.

```
host1(config-dhcp-local)#default-router 10.20.32.1
```

5. Exit DHCP Local Pool Configuration mode.

```
host1(config-dhcp-local)#exit
```

6. Configure a loopback interface.

```
host1(config)#interface loopback 0
```

7. Assign an IP address and mask to the loopback interface.

```
host1(config-if)#ip address 10.20.32.1 255.255.255.0
```

8. Exit Interface Configuration mode.

```
host1(config-if)#exit
```

9. Specify a Fast Ethernet port.

```
host1(config)#interface fastEthernet 3/0
```

10. Create an unnumbered primary IP interface associated with the loopback interface configured in Steps 6 and 7.

```
host1(config-if)#ip unnumbered loopback 0
```

11. Configure the primary IP interface to enable dynamic creation of subscriber interfaces.

```
host1(config-if)#ip auto-configure ip-subscriber
```

12. Exit Interface Configuration mode.

```
host1(config-if)#exit
```

13. Repeat Steps 9 through 12 for each Fast Ethernet interface on which you want to configure dynamic subscriber interfaces. For example:

```
host1(config)#interface fastEthernet 3/1
host1(config-if)#ip unnumbered loopback 0
host1(config-if)#ip auto-configure ip-subscriber
host1(config-if)#exit
host1(config)#interface fastEthernet 3/2
host1(config-if)#ip unnumbered loopback 0
host1(config-if)#ip auto-configure ip-subscriber
host1(config-if)#exit
```

**atm pvc**

- Use to configure a PVC on an ATM interface.
- Specify the VCD, the VPI, the VCI, and the encapsulation type. (For more information about these parameters, see [Creating a Basic Configuration](#) in *JUNOS Link Layer Configuration Guide, Chapter 1, Configuring ATM*.)
- Example  
host1(config-subif)#**atm pvc 10 100 22 aal5snap**
- Use the **no** version to remove the specified PVC.

**default-router**

- Use to specify the IP address of the router for the subscriber's computer to use for traffic destined for locations beyond the local subnet.
- Specify the IP address of a primary server, and optionally, specify the IP address of a secondary server.
- Example  
host1(config-dhcp-local)#**default-router 10.10.1.1**
- Use the **no** version to remove the association between the address pool and the router.

**encapsulation bridge1483**

- Use to configure bridged Ethernet as the encapsulation method on an interface.
- Example  
host1(config-subif)#**encapsulation bridge1483**
- Use the **no** version to remove bridged Ethernet as the encapsulation method on the interface.

**encapsulation vlan**

- Use to configure VLAN as the encapsulation method on an interface.
- Issuing this command creates the VLAN major interface.
- Example  
host1(config-if)#**encapsulation vlan**
- Use the **no** version to disable VLAN encapsulation on the interface.



**interface atm**

- Use to configure an ATM interface or subinterface type in the *slot/port.subinterface* format:
  - *slot*—Specifies router chassis slot
  - *port*—Specifies I/O module port
  - *subinterface*—Specifies subinterface number
- Example  
`host1(config-if)#interface atm 9/1.1`
- Use the **no** version to remove the ATM interface or subinterface.

**interface fastEthernet**

- Use to select a Fast Ethernet (FE) interface on a line module or an SRP module.
- Example  
`host1(config)#interface fastEthernet 1/0`
- Use the **no** version to remove IP from an interface or subinterface. You must issue the **no** version from the highest level down; you cannot remove an interface or a subinterface if the one above it still exists.

**interface gigabitEthernet**

- Use to select a Gigabit Ethernet interface.



**NOTE:** You can configure only the primary port, 0, on the Gigabit Ethernet module. The router automatically uses the redundant port if the primary port fails.

---

- Example  
`host1(config)#interface gigabitEthernet 1/0`
- Use the **no** version to remove IP from an interface. You must issue the **no** version from the highest level down; you cannot remove an interface or a subinterface if the one above it still exists.

**interface tenGigabitEthernet**

- Use to select a 10-Gigabit Ethernet interface on the E120 router or the E320 router.
- Use the *slot/adapter/port* format.
- Example  
`host1(config)#interface tenGigabitEthernet 4/0/1`
- Use the **no** version to remove IP from an interface. You must issue the **no** version from the highest level down; you cannot remove an interface or subinterface if the one above it still exists.

**interface loopback**

- Use to access and configure a loopback interface.
- You can use a loopback interface to provide a stable IP address that can minimize the impact if a physical interface goes down.
- Example
 

```
host1(config)#interface loopback 10
host1(config-if)#ip address 10.20.32.1 255.255.255.0
```
- Use the **no** version to delete the loopback interface.

**ip address**

- Use to set an IP address for an interface or a subinterface.
- Specify the layer 2 encapsulation before you set the IP address.
- Issuing this command creates the primary IP interface. You must create a primary IP interface on which to enable dynamic creation of subscriber interfaces.
- Example
 

```
host1(config-subif)#ip address 192.168.2.50 255.255.255.0
```
- Use the **no** version to remove the IP address or to disable IP processing.

**ip auto-configure ip-subscriber**

- Use to configure an IP interface to support creation of dynamic subscriber interfaces. The specified IP interface is considered the primary interface.
- The router creates the required dynamic subscriber interfaces when the IP address is assigned to the associated subscriber. The address might be assigned by an external DHCP server, the DHCP local server, or the packet detect feature.
- Use the **include-primary** keyword to specify that the primary interface can be assigned to a subscriber. Use the **exclude-primary** keyword to specify that the primary interface is not used for subscribers. The primary interface is not assigned to a subscriber by default.
- You can issue this command from Interface Configuration mode, Subinterface Configuration mode, or Profile Configuration mode.
- Example
 

```
host1(config-if)#ip auto-configure ip-subscriber include-primary
```
- Use the **no** version to disable creation of dynamic subscriber interfaces associated with this primary IP interface. Use the **no** version with the **include-primary** keyword to specify that the primary interface is not assigned to a subscriber.

***ip auto-detect ip-subscriber***

- Use to set the router's packet detect feature and specify that IP automatically detect packets that do not match any entries in the demultiplexer table. When an unmatched packet is detected, an event is generated that determines whether to create a dynamic subscriber interface.
- Example  

```
host1(config-if)#ip auto-detect ip-subscriber
```
- Use the **no** version to restore the default, in which packet detection is disabled.

***ip dhcp-local pool***

- Use to access DHCP Local Pool Configuration mode.
- The DHCP local server uses pool names other than default to maintain configuration information for subscribers to a particular domain.
- Example  

```
host1(config)#ip dhcp-local pool ispBoston
```
- Use the **no** version to prevent the DHCP local server from supplying IP addresses from the specified pool.

***ip inactivity-timer***

- Use to configure the inactivity timer value. A dynamically created subscriber interface is deleted if it is inactive for a period longer than the inactivity timer value.
- The timer value can be in the range 1–65335 minutes.
- A timer value of 0 specifies that dynamically created subscriber interfaces are never deleted by the inactivity timer.
- Example  

```
host1(config-if)#ip inactivity-timer 100
```
- Use the **no** version to restore the default, in which inactivity timer feature is disabled.

***ip source-prefix***

- Use to configure a subscriber interface or a primary IP interface enabled for dynamic creation of subscriber interfaces to demultiplex traffic with the specified source address.
- You can issue this command from either Interface Configuration mode or Subinterface Configuration mode.
- Example  

```
host1(config-if)#ip source-prefix 10.10.2.0 255.255.255.0
```
- Use the **no** version to remove the association between the interface and the specified IP source address and mask.

***ip unnumbered***

- Use to configure an unnumbered IP interface.
- This command enables IP processing on an interface without assigning an explicit IP address to the interface.
- You must specify an interface location, which is the identifier of another interface on which the router has an assigned IP address. This interface cannot be another unnumbered interface.
- Examples
 

```
host1(config-if)#ip unnumbered fastEthernet 3/0
host1(config-if)#ip unnumbered loopback 10
```
- Use the **no** version to disable IP processing on the interface.

***ip use-framed-routes ip-subscriber***

- Use to configure a static primary IP interface to use framed routes as source IP addresses when creating dynamic subscriber interfaces. The router uses the Framed-Route RADIUS attribute [22] sent in Access-Accept messages to apply framed routes to subscriber interfaces associated with the primary interface.
- Example
 

```
host1(config-if)#ip use-framed-routes ip-subscriber
```
- Use the **no** version to disable the use of framed routes when creating dynamic subscriber interfaces associated with this primary IP interface.

***network***

- Use to specify the IP addresses that the DHCP local server can provide from an address pool.
- Example
 

```
host1(config-dhcp-local)#network 10.10.1.0 255.255.255.0
```
- Use the **no** version to remove the network address and mask.

***service dhcp-local***

- Use to enable the DHCP local server to operate in either equal-access mode or standalone mode.
- Example
 

```
host1(config)#service dhcp-local standalone
```
- Use the **no** version to disable the DHCP local server.

**set dhcp relay giaddr-selects-interface**

- Use to configure DHCP relay to use information in the giaddr in DHCP server-destined packets to identify the primary interface on which dynamic subscriber interfaces are built. See [Using the Giaddr to Identify the Primary Interface for Dynamic Subscriber Interfaces](#) on page 319 for additional information about this feature.
- Example  

```
host1(config)#set dhcp relay giaddr-selects-interface
```
- Use the **no** version to restore the default in which DHCP relay builds dynamic subscriber interfaces on the IP interface that is used for DHCP server-destined messages.

**vlan id**

- Use to configure a VLAN ID for a VLAN subinterface.
- Specify a VLAN ID number that is in the range 0–4095 and is unique within the Ethernet interface.
- Issue the **vlan id** command before you configure any upper-layer interfaces, such as IP.
- Example  

```
host1(config-if)#vlan id 400
```
- There is no **no** version.

## Monitoring Subscriber Interfaces

---

The state of the subscriber interface is determined by state of the Ethernet interface and the existence of the primary IP interface, which you can monitor with the **show ip interface** command. For information about using the **show ip interface** command, see [Monitoring IP](#) in *JUNOS IP Services Configuration Guide, Chapter 1, Configuring IP*.

You can use the **show ip demux interface** command to monitor the configuration of subscriber interfaces.

**show ip demux interface**

- Use to display information about subscriber interfaces.
- Field descriptions
  - Prefix/Length—Source or destination addresses that the subscriber interface demultiplexes
  - SA/DA—Demultiplexing method for subscriber interface
    - SA—Source address
    - DA—Destination address
  - Subscriber-Intf—Name of shared interface on which subscriber interface is configured

- VR/VRF—Name of virtual router (VR) or VPN routing and forwarding (VRF) instance on which the subscriber interface is configured
- Description—Text description for the IP interface on which subscriber interface is configured (added with the **ip description** command)
- Example

```
host1#show ip demux interface fastEthernet 2/0
Prefix/Length SA/DA Subscriber-Intf VR/VRF Description
10.12.2.2/32 SA ip subsc1 3 subsc1@test
10.12.2.3/32 SA ip subsc2 3 subsc2@test
10.12.2.4/32 SA ip subsc3 3 subsc3@test
10.12.2.5/32 SA ip subsc4 3 subsc4@test
```

### **show ip-subscriber**

- Use to display information about active IP subscribers that were created by the JUNOS software's subscriber management feature.
- Field descriptions
  - Id—ID of the subscriber
  - User Name—Username used to retrieve information from RADIUS for the subscriber interface
  - Ip Address—IP address of the subscriber interface
  - Virtual Router—Name of the virtual router on which the subscriber interface is configured
  - Interface—Name of subscriber interface; **ip** indicates that subscriber manager created this interface
  - Login Time—Day, date, and time that the subscriber logged in
  - Mac Address—MAC address of the subscriber
  - Profile Handle—AAA profile handle
  - Interface Profile—Interface profile name used to configure the subscriber interface
  - Service Profile—IP service profile name used by subscriber management to authorize and configure the subscriber interface with AAA
  - Option 82—DHCP relay agent information (option 82) circuit identifier that describes the physical interface location associated with the subscriber
- Example 1

```
host1#show ip-subscriber 2835349506
```

| Id         | User Name      | Ip Address  | Virtual Router | Interface     |
|------------|----------------|-------------|----------------|---------------|
| 2835349506 | user1@isp1.com | 192.168.0.1 | default        | ip192.168.0.1 |

| Id         | Login time               |
|------------|--------------------------|
| 2835349506 | WED AUG 23 20:46:24 2006 |

■ Example 2

host1#show ip-subscriber detail

```

 Subscriber List

 Id User Name Ip Address Virtual
 ----- ----- ----- Router Interface
2835349506 user1@isp1.com 192.168.0.1 default ip192.168.0.1

 Id Login Time Mac Address Profile
 ----- ----- ----- Handle
2835349506 WED AUG 23 20:46:24 2006 3000.0001.9365 13631489

 Id Interface Profile Service Profile Option 82
 ----- ----- ----- -----
2835349506 myProfile profile22 FastEthernet 3/1

```





## Chapter 11

# Configuring Service Manager

This chapter describes how to use the Service Manager application to define, activate, and monitor networking services for your subscribers. This chapter discusses the following topics:

- [Overview](#) on page 450
- [Platform Considerations](#) on page 451
- [References](#) on page 451
- [Configuration Tasks](#) on page 452
- [Service Definitions](#) on page 453
- [Referencing Policies in Service Definitions](#) on page 457
- [Referencing QoS Configurations in Service Definitions](#) on page 458
- [Configuring the Service Manager License](#) on page 466
- [Managing and Activating Service Sessions](#) on page 466
- [Using RADIUS to Manage Subscriber Service Sessions](#) on page 467
- [Using Mutex Groups to Activate and Deactivate Subscriber Services](#) on page 473
- [Configuring RADIUS Accounting for Service Manager](#) on page 475
- [Using the CLI to Manage Subscriber Service Sessions](#) on page 477
- [Configuring Service Manager Statistics](#) on page 485
- [Service Manager Performance Considerations](#) on page 488
- [Service Definition Examples](#) on page 489
- [Monitoring Service Manager](#) on page 500

## Overview

The JUNOS Service Manager application provides authentication, service selection, and service activation and deactivation to subscribers. The application also collects accounting information and statistics, and monitors subscriber and service sessions.

Service Manager supports two client types—RADIUS and CLI. Service Manager starts when it receives a request from a RADIUS or CLI client. For RADIUS clients, RADIUS Access-Accept messages and Change-of-Authorization-Request (CoA-Request) messages can create and delete Service Manager subscriber sessions and activate and deactivate service sessions. For CLI clients, CLI commands create and delete the subscriber sessions and activate and deactivate service sessions.

A subscriber's service is based on a service definition — service definitions can include profiles, policies, and quality of service (QoS) settings that define the scope of a service granted to the subscriber. Service definitions can also specify statistics configurations.

Service Manager provides convenience and flexibility to both service providers and subscribers.

- Providers are able to separate services and access technology and also to 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—subscribers can dynamically connect to and disconnect from the services, when they want and for how long they want. They are billed based on the service type and usage, rather than being charged a set rate regardless of usage.

## Service Manager Terms and Acronyms

[Table 37](#) defines terms and acronyms that are used in this discussion of the Service Manager application.

**Table 37: Service Manager Terms and Acronyms**

| Term                | Definition                                                                                                                                                                                                                                                                             |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Guided entrance     | A service that creates a controlled Internet browsing environment by transparently directing the subscriber to a specific Web site. At the Web site, the subscriber is presented with a selection of available services. Also called <i>walled gardens</i> or <i>captive portals</i> . |
| Macro language      | The JUNOS macro language that you use for service definitions                                                                                                                                                                                                                          |
| Mutex service       | A service session that is part of a mutex group—the service definition for the service includes the mutex-group attribute.                                                                                                                                                             |
| RADIUS login method | The method that uses RADIUS VSAs in the Access-Accept packet to create a subscriber session and activate a service session when the subscriber logs in                                                                                                                                 |

**Table 37: Service Manager Terms and Acronyms (continued)**

| Term                    | Definition                                                                                                                                                                                                                                                                        |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RADIUS CoA method       | The method that uses RADIUS CoA-Request messages and VSAs to create a subscriber session and activate a service session for a subscriber that is already logged in                                                                                                                |
| Service definition      | A macro file that defines a named parameterized description of a service; used to create a service instance and the resulting subscriber service session; can include a combination of parameters such as policy lists, rate-limit profiles, QoS profiles, and interface profiles |
| Service instance        | An instance that is created when you specify parameter values for a service definition to create a service session                                                                                                                                                                |
| Service session         | A session that is created when a service instance is activated for a subscriber; a subscriber can have multiple active service sessions                                                                                                                                           |
| Service session profile | A provider-configured profile that applies optional attributes to a service session; CLI only                                                                                                                                                                                     |

## Platform Considerations

Service Manager is supported on all E-series routers. For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

## References

For more information about the topics covered in this chapter, see the following documents:

- Data-Over-Cable Service Interface Specifications (DOCSIS) 2.0 Radio Frequency Interface Specification CM-SP-RF1v2.0-110-051209.
- For information about using the JUNOS software's macro language, see [JUNOS System Basics Configuration Guide, Chapter 9, Writing CLI Macros](#).
- For information about setting up policy-based routing features for Service Manager, such as rate-limit profiles, classifier control lists, policy lists, and hierarchical and merged policies, see the [JUNOS Policy Management Configuration Guide](#).
- For information about creating QoS profiles and QoS parameters, see the [JUNOS Quality of Service Configuration Guide](#).
- For information about creating IPv4 interface profiles, see [JUNOS IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP](#).

## Configuration Tasks

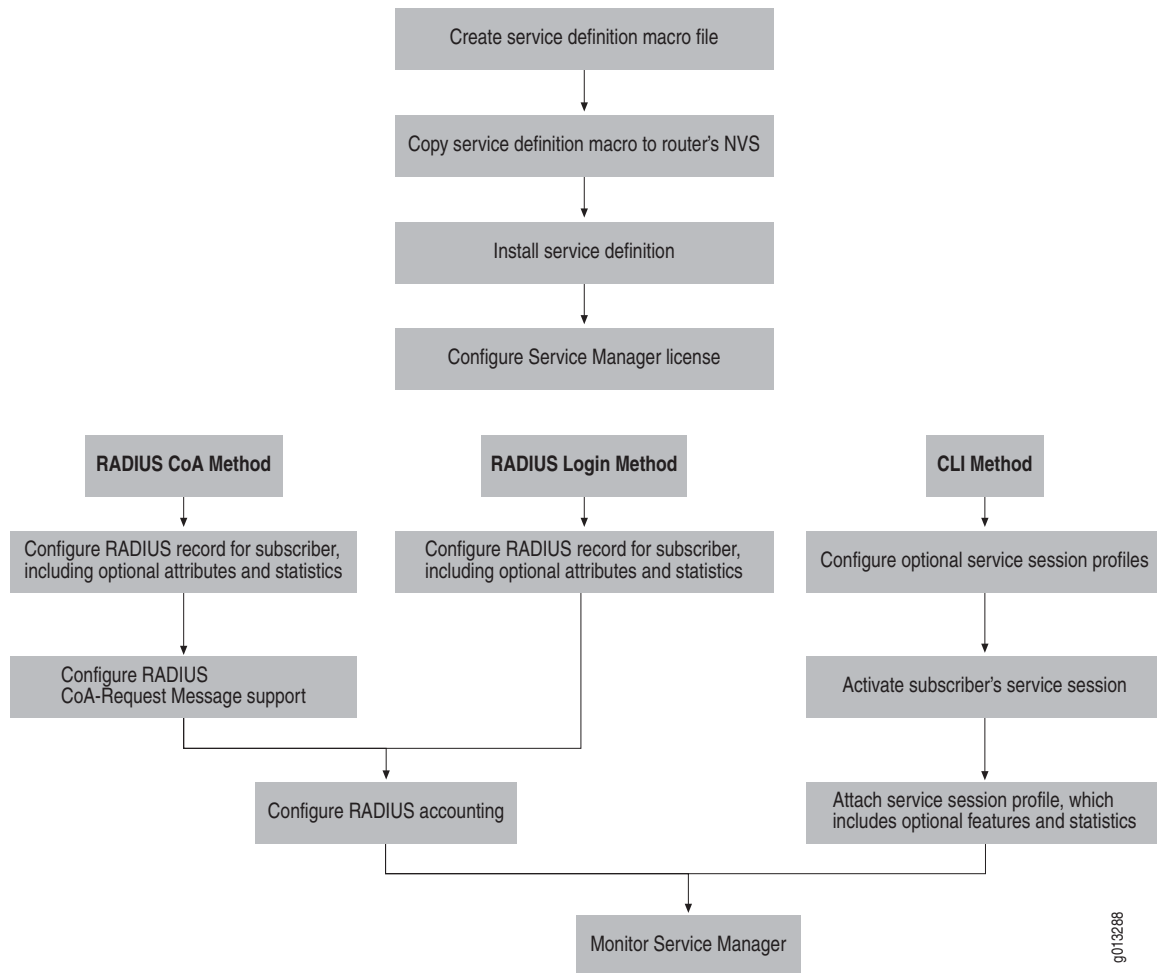
---

To use the Service Manager application to create subscriber service sessions, you perform the following tasks:

- Create and manage service definitions
  - Use the macro language to define service definitions
  - Download service definition macro files to the router's nonvolatile storage (NVS)
  - Install service definitions on the router
  - Uninstall service definitions
- Configure the Service Manager license
- Configure RADIUS accounting
- Use RADIUS login and RADIUS CoA to manage subscriber service sessions
  - Specify the subscriber
  - Specify optional attributes
  - Enable statistics collection
  - Activate the service session
  - Deactivate service sessions
  - (Optional for RADIUS CoA method) Configure the CoA feature for the RADIUS dynamic-request server
- Use the CLI to manage subscriber service sessions
  - Specify the subscriber
  - Create and apply optional service session profiles
  - Enable statistics collection
  - Activate the service session
  - Deactivate service sessions

Figure 26 shows the sequence of operations you use to create and monitor subscriber service sessions.

**Figure 26: Service Manager Configuration Flowchart**



## Service Definitions

A service definition is a high-level, platform-independent template that defines a service that you want to let your subscribers use. You use the JUNOS software's embedded macro language on your computer to create the macro file that defines the service. You copy and install the macro file on the E-Series router, and then you can associate the service definition with subscribers to create their service sessions.

Service definitions gives you flexibility by enabling you to use:

- A single service definition to create a service for multiple subscribers.
- Parameterized service definitions to create variations of a service definition.
- Different service definitions to create multiple services for a single subscriber.

A service definition might use the following types of JUNOS objects to define the characteristics and capabilities of the service you want to provide:

- Interface profiles—Specify a set of characteristics that can be dynamically assigned to IP interfaces. A service definition must use at least one interface profile.
- Policy lists—Specify policy actions for traffic traversing an interface.
- Classifier lists—Specify the criteria by which the router defines a packet flow.
- Rate-limit profiles—Specify a set of bandwidth attributes and associated actions that limit a classified packet flow or a source interface to a rate that is less than the physical rate of the port.
- QoS parameters—Specify attributes such as shaping rate, shared-shaping rate, assured rate, and scheduler weight for scheduler nodes and queues.
- QoS profiles—Specify queue, drop statistics gathering, and scheduler configuration for an interface hierarchy.

## Creating Service Definitions

To create a service definition, you use the JUNOS software's macro language to specify the parameters that define the desired service. A macro file can define only one service—however, the file can have multiple templates to define characteristics of the desired service. You create service definitions independent of the Service Manager commands and operations, which are performed on the E-series router.

For detailed information about the JUNOS software's macro language, see [JUNOS System Basics Configuration Guide, Chapter 2, Command-Line Interface](#).

[Figure 27](#) is an example of a service definition macro file that creates a tiered service. A tiered service typically provides set bandwidths for both inbound and outbound traffic for a subscriber. In this example, the input (inputBW) and output (outputBW) bandwidth values are parameterized. This example assumes that QoS profile triplePlayIP and QoS parameter maxSubscBW are configured. See [Service Definition Examples](#) on page 489 for additional service definition examples.

Service Manager only tracks JUNOS objects that are passed back in the `env.setResult` method when a service definition is executed. [Table 38](#) describes the supported objects:

**Table 38: JUNOS Objects Tracked by Service Manager**

| Name                       | Requirement | Description                                                                                                                          |
|----------------------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------|
| input-stat-clacl           | Optional    | <ul style="list-style-type: none"> <li>■ Collects input statistics from policy manager</li> <li>■ Can be a list of clacs</li> </ul>  |
| secondary-input-stat-clacl | Optional    | <ul style="list-style-type: none"> <li>■ Collects input statistics from policy manager</li> <li>■ Can be a list of clacs</li> </ul>  |
| output-stat-clacl          | Optional    | <ul style="list-style-type: none"> <li>■ Collects output statistics from policy manager</li> <li>■ Can be a list of clacs</li> </ul> |

**Table 38: JUNOS Objects Tracked by Service Manager (continued)**

| Name                 | Requirement | Description                                                                                                                                                                                                                                                       |
|----------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| activate-profile     | Required    | <ul style="list-style-type: none"> <li>■ Specifies the interface profile used on activation of the service</li> <li>■ Deletion of the profile is Service Manager's responsibility</li> </ul>                                                                      |
| deactivate-profile   | Optional    | <ul style="list-style-type: none"> <li>■ Specifies the interface profile used on deactivation of the service</li> <li>■ If not specified, is the same as the activation-profile</li> <li>■ Deletion of the profile is Service Manager's responsibility</li> </ul> |
| command-in-error     | Optional    | <ul style="list-style-type: none"> <li>■ Passes the value <code>env.getErrorCommand</code></li> <li>■ Service Manager displays the line in the service definition that has the error</li> </ul>                                                                   |
| command-error-status | Optional    | <ul style="list-style-type: none"> <li>■ Passes the value <code>env.getErrorStatus</code></li> <li>■ Service Manager displays the error status for the error</li> </ul>                                                                                           |

**Figure 27: Sample Service Definition Macro File**

```

!parameterizes input and output bandwidth
<# tiered(inputBW, outputBW) #>

<# uid := app.servicemanager.getUniqueId #>
<# name := "SM-tiered-" $ uid #>
<# oname := "SM-O-tiered-" $ uid #>

classifier-list matchAll ip any any
rate-limit-profile <# name #> one-rate
 committed-rate <# inputBW; '\n' #>

policy-list <# name; '\n' #>
 classifier-group matchAll precedence 10000
 rate-limit-profile <# name; '\n' #>
 traffic-class best-effort

policy-list <# oname; '\n' #>
 classifier-group matchAll precedence 10000
 traffic-class best-effort

profile <# name; '\n' #>
 ip policy secondary-input <# name #> statistics enabled merge
 ip policy output <# oname #> statistics enabled merge
 qos-profile triplePlayIP
 qos-parameter maxSubscBW <# outputBW; '\n' #>

<# env.setResult("activate-profile", name) #>
<# env.setResult("secondary-input-stat-clac1", "matchAll") #>
<# env.setResult("output-stat-clac1", "matchAll") #>

<# endtmp1 #>

```

## Managing Your Service Definitions

After you have created the macro file for your service definition, you can perform the following operations with the service definition macro file:

1. **Copy**—You must copy the service definition from the local computer that you used to create the macro file to the router's NVS card.
2. **Install**—You must install the service definition before you can use it to create a service session. During installation, Service Manager precompiles the definition and extracts the definition file's timestamp. Precompiling the service definition improves Service Manager performance. The timestamp enables the Service Manager application to track any modifications you might make while the definition is being used.
3. **Uninstall**—You can uninstall a service definition file, for example, if you no longer want to use that definition. When you uninstall a service definition file, any existing service sessions that were activated using the original service definition continue to use the original definition until you deactivate the service session.
4. **Modify**—You can update an existing service definition file at any time. To update a service definition file:
  - a. Use your text editor on your computer to make changes to the original service definition file.
  - b. Copy the updated service definition file back to your router's NVS—this overwrites the original file on the router.
  - c. Install the new service definition file.

All new service sessions will be activated using the new service definition. Any existing service sessions that were activated using the original service definition continue to use the original definition until you deactivate the service session.

### copy

- Use to copy a service definition macro file from your computer to the router's NVS.
- Specify the directory containing the macro file you want to copy and the name you want to use for the file in NVS.
- Example  

```
host1#copy boston:/serviceDefs/triplePlay/tiered.mac tiered.mac
```
- There is no **no** version.



**service-management install**

- Use to install or uninstall a service definition.
- You must include the .mac extension.
- During installation, Service Manager precompiles the service definition and extracts the definition file's timestamp.
- After you install the service definition, you can use the definition to create service sessions for subscribers.
- To update an existing service definition, you make changes to the original macro file on your computer, copy the updated file to NVS, and install the updated file. All subsequent service sessions use the new service definition file. However, currently active service sessions continue to use the original definition file until the sessions are deactivated, then reactivated.
- Example 1—Installing  
`host1(config)#service-management install tiered.mac`
- Example 2—Uninstalling  
`host1(config)#no service-management install tiered.mac`
- Example 3—Updating  
 ! update the original macro file on the remote system  
  
 ! copy the updated macro file to the router  
`host1#copy boston:/serviceDefs/triplePlay/tiered.mac tiered.mac`  
`host1#configure terminal`  
 ! install the updated service definition on the router  
`host1(config)#service-management install tiered.mac`
- Use the **no** version to uninstall a service definition.

**Referencing Policies in Service Definitions**

In Profile Configuration mode, policy interface commands for IP and L2TP allow attachments to be merged into any existing merge-capable attachment at an attachment point. Merged policies are dynamically created. Service Manager can request that multiple interface profiles be applied or removed at an interface as part of service activation or deactivation. Service Manager also specifies whether or not the attachments created from these interface profiles persist on subsequent reloads.

Service Manager can specify whether a component policy attachment is non-volatile. If the interface where the component policy is attached is volatile, then policy management makes the attachment volatile even when the Service Manager specifies otherwise. A non-volatile interface can have both volatile and non-volatile component policy attachments. The merged policy that is created is the merge of all component policies attached at a given attachment point regardless of their volatility. The merged policy and its attachments are always volatile and reconstructed on each reload operation.

For further details on merging policies, see [JUNOS Policy Management Configuration Guide, Chapter 2, Creating Policies](#).

## Referencing QoS Configurations in Service Definitions

---

You can use QoS profiles and QoS parameters to define a service for a subscriber. For example, you can configure the shaping rate for traffic in a video service by using a QoS parameter instance.

To transmit the QoS configuration to the subscriber interface (that is, the forwarding interface at the top of the interface column), you must configure the QoS profiles and QoS parameter instances in static profiles.

### Specifying QoS Profiles in a Service Definition

You can configure one QoS profile per subscriber interface. We recommend that you specify the QoS profile in the first set of services applied to the subscriber's interface.

You can modify the QoS profile by modifying configurations referenced by the QoS profile, including QoS parameter instances. You can also attach a new QoS profile when activating a service, but make sure that the QoS profile is attached to the subscriber's interface.

For more information about configuring QoS profiles, see [JUNOS Quality of Service Configuration Guide, Chapter 7, Configuring QoS Profiles](#).

### Configuring a QoS Profile for Service Manager

To configure a QoS profile for Service Manager:

1. Configure the profile.

```
host1(config)#profile videoService
```

2. Configure the QoS profile.

```
host1(config-profile)#qos-profile videoBandwidth1
```

3. (Optional) Complete the QoS profile configuration described in [JUNOS Quality of Service Configuration Guide, Chapter 7, Configuring QoS Profiles](#).

#### **profile**

- Use to create a profile and enter Profile Configuration mode.
- You specify a profile name with up to 80 alphanumeric characters.
- Example
 

```
host1(config)#profile iptv
host1(config-profile)#
```
- Use the **no** version to remove a profile.

**qos-profile**

- Use to add a QoS profile command for use with Service Manager. When the service is activated, the QoS profile is created and attached to the subscriber interface.
- Example
 

```
host1(config)#profile iptv
host1(config-profile)#qos-profile video
```
- Use the **no** version to remove the QoS profile from the profile.

**Specifying QoS Profiles in a Service Definition**

After you configure a QoS profile for Service Manager, you can reference it in a service definition. For example:

```
profile <# eastcoast ; '\n' #>
qos-profile <# video; '\n' #>
```

In this example, activating the service definition attaches the video QoS profile to the subscriber interface. Service Manager overwrites the existing QoS profile attachment at the subscriber interface.

Deactivating the service detaches the video QoS profile from the subscriber interface.

**Specifying QoS Parameter Instances in a Service Definition**

You can specify that Service Manager create QoS parameter instances when the subscriber logs in (during service activation) or through RADIUS QoS parameter VSAs.

You can specify up to eight parameter instance commands within a profile. When you activate a service, Service Manager creates or modifies parameter instances for the subscriber interface that matches one of the subscriber-interface types configured in the QoS parameter definition.

Deactivating a service can modify or remove QoS parameter instances.

Using a service definition, you can also configure QoS parameters instances to add value to an existing parameter instance using the **add** keyword or dynamically create new parameter instances with an initial value using the **initial-value** keyword.

For more information about configuring QoS parameters, see [JUNOS Quality of Service Configuration Guide, Chapter 11, Configuring QoS Parameters](#).

## Creating a Parameter Instance in a Profile

To create a QoS parameter instance for Service Manager:

1. Configure the QoS parameter definition described in *JUNOS Quality of Service Configuration Guide, Chapter 11, Configuring QoS Parameters*.

You must configure at least one controlled-interface type and one subscriber-interface type. The range specified in the parameter definition controls the available value of the parameter instance.

2. Configure the QoS profile.

```
host1(config)#profile video
```

3. Configure the QoS parameter instance command in the profile.

```
host1(config-profile)#qos-parameter videoBandwidth1 add 40000
```

### qos-parameter

- Use to create a parameter instance command in a profile. When the service is activated, the parameter instances are created for the subscriber interface.
- Use the **add** keyword in Profile Configuration mode to add a value to an existing parameter instance.
- Use the **initial-value** keyword to create a new instance with the specified value.
- Examples

```
host1(config)#profile video
host1(config-profile)#qos-parameter max-subscriber-bandwidth initial-value
15000
```

- In Profile Configuration mode, the **no** version removes the QoS parameter instance command in the profile.

## Specifying QoS Parameter Instances in a Service Definition

After you configure a QoS parameter instance for Service Manager, you can reference it in a service definition. For example:

```
<# qoserviceone(bandwidth1, bandwidth2) #>
 profile <# profileName ; '\n' #>
 qos-parameter <# qosParameterName1 ; ' ' ; bandwidth1 ; '\n' #>
 qos-parameter <# qosParameterName2 ; ' ' ; bandwidth2 ; '\n' #>
 <# endtpl #>
```

When you activate a service, Service Manager creates the parameter instance and overwrites previous parameter instances. For example, activating the qoserviceone service definition creates a profile containing two QoS parameter instances. Service Manager creates the qosParameterName1 parameter instance with the value of bandwidth1, and creates qosParameterName2 with a value of bandwidth2.

If you activate the service definition using qoserviceone(2000000,3000000), Service Manager creates qosParameterName1 with a value of 2000000 and qosParameterName2 instance with a value of 3000000.

### Specifying the Add and Initial-Value Keywords

You can use the **add** keyword to add value to an existing parameter instance. For example:

```
<# qoserviceone(bandwidth1, bandwidth2) #>
 profile <# profileName ; '\n' #>
 qos-parameter <# qosParameterName3 ; ' add ' ; bandwidth2 ; '\n' #>

<# endtmpl #>
```

When you specify parameter instances using the **add** keyword, you can also use the **initial-value** keyword to specify an initial value. For example:

```
<# qoserviceone(bandwidth1, bandwidth2) #>
 profile <# profileName ; '\n' #>
 qos-parameter <# qosParameterName4 ; ' add ' ; bandwidth2 ;
 ' initial-value 1000000' ; '\n' #>

<# endtmpl #>
```

When you activate the service, Service Manager locates the existing QoS parameter instance in the interface column. If Service Manager does not find a parameter instance, it creates one with a value specified in the **initial-value** keyword (in this case, 100000). The value in the command is then added to the initial value. If an existing parameter instance is found, Service Manager adds the value to the existing interface.

For example, when you activate qosServiceOne as qosServiceOne(2000000,3000000), Service Manager attempts to locate the parameter instance qosParameterName4 for the subscriber's interface. If it finds a parameter instance, it adds bandwidth2 (3,000,000) to the current value. If Service Manager does not find a parameter instance, it creates one with an initial value of 1,000,000 and adds 3,000,000. The final parameter instance value is 4,000,000.

When deactivating the service, Service Manager locates the QoS parameter instance and subtracts the value in the command from the existing instance value. If the parameter is no longer referenced, the parameter instance is removed.

## Modifying QoS Configurations with Service Manager

This section describes how to modify QoS configurations with Service Manager.

### Modifying Parameter Instances

Service Manager activates services without considering current parameter instance values. For example, when you deactivate a video service, Service Manager can add 5 Mbps to a parameter associated with the shaping rate of a video queue.

Similarly, Service Manager can deactivate services and restore parameter instances to their previous value. For example, when you deactivate a video service, Service Manager can subtract 5 Mbps from a parameter associated with the shaping rate of a video queue.

Table 39 lists the results of a series of activations and deactivations of parameters using the **add** and **initial-value** keywords.

**Table 39: Sample Modifications Using the Add and Initial-Value Keywords**

| Action     | QoS Parameter Instance                                | Result                                                                      |
|------------|-------------------------------------------------------|-----------------------------------------------------------------------------|
| Activate   | qos-parameter video-bw add 5000000<br>initial-value 0 | Parameter instance video-bw is created with a value of 5000000              |
| Activate   | qos-parameter video-bw add 1000000<br>initial-value 0 | Parameter instance video-bw is increased by 1000000, for a total of 6000000 |
| Deactivate | qos-parameter video-bw add 1000000<br>initial-value 0 | Parameter instance video-bw is decreased by 1000000, for a total of 500000  |
| Deactivate | qos-parameter video-bw add 5000000<br>initial-value 0 | Parameter instance video-bw is removed                                      |

Removing a parameter instance using profiles is based on the number of times a parameter instance is modified, not the value added.

Modifying parameter instances in profiles and modifying explicit parameter instances can cause invalid parameter instance values. Table 40 lists a series of activations and deactivations using parameter instances in profiles and explicit parameter instances. By the second deactivation, the parameter has a negative value (-4000000).



**NOTE:** We recommend that you do not configure negative values for Service Manager.

**Table 40: Sample Modifications Using Parameter Instances**

| Action     | QoS Parameter Instance                                | Result                                                                         |
|------------|-------------------------------------------------------|--------------------------------------------------------------------------------|
| Activate   | qos-parameter video-bw add 5000000<br>initial-value 0 | Parameter instance video-bw is created with a value of 5000000                 |
| Activate   | qos-parameter video-bw add 1000000<br>initial-value 0 | 1000000 is added to parameter instance video-bw, for a total of 6000000        |
| Activate   | qos-parameter video-bw 2000000                        | Parameter instance video-bw is set to 2000000                                  |
| Deactivate | qos-parameter video-bw add 1000000<br>initial-value 0 | 1000000 is subtracted from parameter instance video-bw for a total of 1000000  |
| Deactivate | qos-parameter video-bw add 5000000<br>initial-value 0 | 5000000 is subtracted from parameter instance video-bw for a total of -4000000 |
| Deactivate | qos-parameter video-bw 2000000                        | Parameter instance video-bw is removed                                         |

### Modifying QoS Configurations in a Single Service Manager Event

QoS accepts QoS profile attachments and parameter instances created using multiple sources (profiles, RADIUS, or Service Manager) within a single Service Manager event. Events include:

- Subscriber login
- Subscriber logout
- RADIUS Change of Authority (CoA)

QoS prioritizes the creation of QoS profiles and parameter instances within events. [Table 41](#) lists the sources that overwrite QoS profiles and parameter instances created by other sources. Each row represents new QoS profiles and parameter instances; columns represent existing QoS profiles and parameter instances.

**Table 41: Configuration Within a Single Service Manager Event**

|                        | Profile | RADIUS | Service Manager |
|------------------------|---------|--------|-----------------|
| <b>Profile</b>         | ✓       | –      | –               |
| <b>RADIUS</b>          | ✓       | ✓      | –               |
| <b>Service Manager</b> | ✓       | ✓      | ✓               |

### Modifying QoS Configurations Using Other Sources

You can modify QoS configurations with Service Manager by using other QoS sources. For example, you can modify a parameter instance that was created with Service Manager by using the CLI. Similarly, you can use SNMP to detach a QoS profile attached by Service Manager.

[Table 42](#) lists the sources that you can use to modify QoS profile attachments and parameter instances.

**Table 42: Modifying QoS Configurations with Other Sources**

|                 | QoS Profile Attachment | QoS Parameter Instances |
|-----------------|------------------------|-------------------------|
| Service Manager | ✓                      | ✓                       |
| RADIUS          | ✓                      | ✓                       |
| SNMP            | ✓                      | –                       |
| SDX software    | ✓                      | –                       |
| CLI             | ✓                      | ✓                       |

The following sections describe the precedence of each source when modifying configurations.

#### Service Manager

QoS profile attachments and parameter instances created through Service Manager have precedence over all other sources. For example, Service Manager can overwrite a QoS profile attachment modified through RADIUS, SNMP, the SDX software, or the CLI.

Conversely, Service Manager configurations can be overwritten through SNMP, the SDX software, and the CLI, but not by RADIUS.

Service Manager counts references of parameter instances. You can modify parameter instances created by Service Manager using other sources without affecting the reference counts. For more information, see [QoS Statistics](#) on page 465.

### **RADIUS**

QoS profile attachments and parameter instances configured through RADIUS can overwrite QoS profile attachments and parameter instances configured through the SNMP, the SDX software, and the CLI, but not those created by Service Manager.

Conversely, QoS profiles and parameter instances configured through RADIUS can be overwritten by any source (SNMP, the SDX software, CLI, and Service Manager).

### **SNMP, the SDX Software, and the CLI**

QoS profile attachments and parameter instances configured through the CLI can overwrite QoS profile attachments and parameter instances configured through any source.

QoS profiles attached through SNMP and the SDX software can also overwrite QoS profile attachments configured through any source.

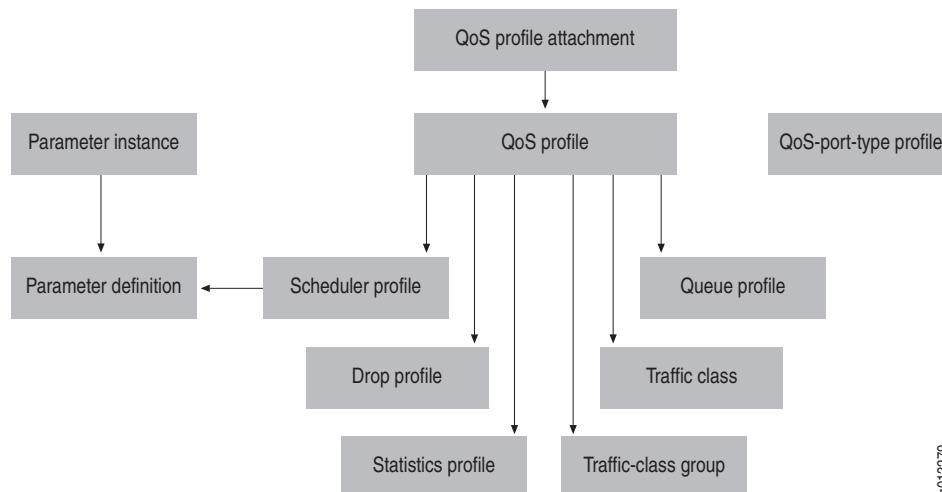
Conversely, QoS profiles and parameter instances configured through the CLI, SNMP, or the SDX software can be overwritten by any source.

## **Removing QoS Configurations Referenced by Service Manager**

When Service Manager no longer references a QoS configuration, it must be removed from the service definition.

[Figure 28](#) shows the references for QoS configurations.

**Figure 28: QoS Configuration Dependency Chain**



9013279



Service Manager automatically removes QoS profiles and parameter instances. After removing the QoS profile and parameter instances, Service Manager automatically removes the following QoS configurations in the following order:

1. QoS profiles
2. Scheduler profiles
3. Queue profiles
4. Drop profiles
5. Statistics profiles

Service Manager does not automatically remove the following QoS configurations:

- Parameter definitions
- Traffic classes
- Traffic-class groups
- QoS-port-type profiles

### **QoS for Service Manager Considerations**

When you specify QoS configurations in Service Manager, the following considerations apply.

#### **RADIUS or Service Manager**

We recommend that you choose either RADIUS or Service Manager to create a single parameter instance. If you use both RADIUS and Service Manager, parameter instances activated using Service Manager take precedence.

#### **Interoperability with Other Service Components**

Service Manager removes QoS profiles and parameter instances if other components in the service definition (for example, policies) cause an error.

#### **QoS Statistics**

Service Manager counts references of parameter instances in profiles. The reference count is incremented each time the parameter is configured through the CLI, RADIUS, or Service Manager. The reference count is decremented each time the parameter is unconfigured, such as through service deactivation. Modifications to parameter instances are also reference counted, using a separate reference count. Parameter instances are removed when both reference counts reach zero.

Service Manager also counts references of modified parameters in profiles using the **add** keyword. The reference count is incremented each time the parameter is modified through service activation with the **add** keyword. The reference count is decremented each time the parameter is modified through service deactivation. References of regular parameter instances are also counted, using a separate reference count. Parameter instances are removed when both reference counts reach zero.

## Ranges

You can verify ranges for parameter instances by specifying a range in the parameter definition using the **range** command.

When activating the service or modifying parameters, Service Manager verifies the value of the parameter instance to be within the specified range and generates an informational log message indicating the value is outside the range. Service Manager does not verify ranges when you specify the parameter instances within profiles at the time of configuration.

## Configuring the Service Manager License

---

Use the Service Manager license to enable full Service Manager application support. Service manager supports a maximum number of subscriber sessions equal to the number of IP interfaces supported on your router. For information about the maximum number of IP interfaces supported, see *JUNOS Release Notes, Appendix A, System Maximums*.

You can create a maximum of 10 subscriber sessions when the Service Manager license is not enabled. If you disable the Service Manager license and more than 10 subscriber sessions exist, you cannot enable any new sessions—however, all existing active subscriber sessions continue to function.

### *license service-management*

- Use to specify the Service Manager license and enable full Service Manager application support—if the license is not enabled, you are limited to 10 subscriber sessions.
- The license is a unique string of up to 15 alphanumeric characters.



**NOTE:** Obtain the license from Juniper Networks Customer Service or your Juniper Networks sales representative.

---

- Example  

```
host1(config)#license service-management 123456789
```
- Use the **no** version to disable the license.

## Managing and Activating Service Sessions

---

You can use either RADIUS or the CLI to manage, activate, and deactivate service sessions. The following list describes some of the differences between using RADIUS and the CLI to manage the Service Manager application.

- RADIUS-based login and RADIUS CoA support:
  - Provides dynamic activation and deactivation based on subscriber service selection
  - Provides greater flexibility and efficient management for a large number of subscribers and services

- Enables you to use mutual exclusion (mutex) groups to create mutex services (RADIUS CoA only)
- CLI-based support:
  - Provides static activation and deactivation for subscribers who are always logged in
  - Is useful for testing new service definitions
  - Enables you to preprovision services that you can activate later

## Using RADIUS to Manage Subscriber Service Sessions

---

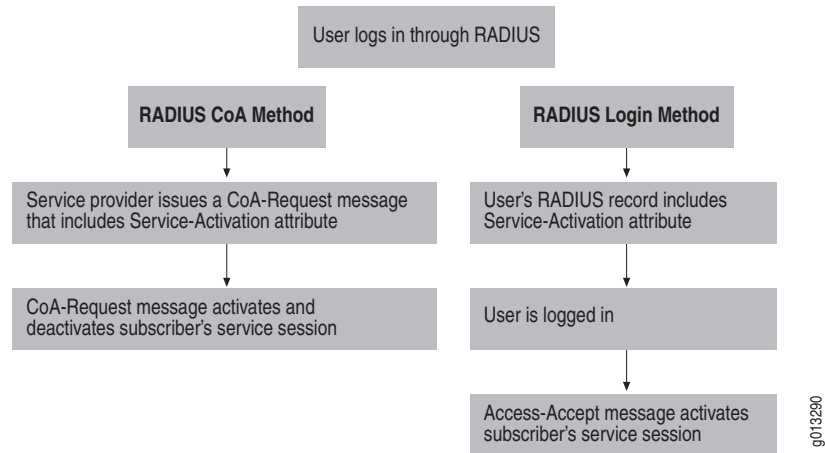
Service Manager supports two RADIUS-based methods for dynamically activating subscriber service sessions. Dynamic service sessions that RADIUS activates are not stored in NVS. Both methods can also apply optional statistics and session threshold (volume and time) configurations. The two methods differ in how Service Manager activates a subscriber service session:

- RADIUS login method—The service session is activated when the subscriber logs in. At login, RADIUS verifies that the Activate-Service attribute is configured in the subscriber's RADIUS record. RADIUS then uses vendor-specific attributes (VSAs) in the Access-Accept packet to activate the service session for the subscriber. This method is useful when your subscribers are not currently logged in.
- RADIUS CoA method—Supports dynamic service selection for subscribers. For example, the subscriber might have logged in without a service, or might have used the RADIUS login method to activate a service at login. If no service was activated at login (because of no Activate-Service attribute in the user's RADIUS record), you can later use the CoA method and a separate RADIUS record to create a subscriber session and activate a service session for the subscriber. Or, if the RADIUS login method was used and the subscriber already has an active service session, you can use the CoA method and a new RADIUS record to activate a new service session for the subscriber (and optionally deactivate the existing service session). The RADIUS CoA method is useful when you have a large number of users already logged in through RADIUS and you want to activate new services for them. This method is also used for the guided entrance service described in [Guided Entrance Service Definition Example](#) on page 493.

The RADIUS CoA method also supports the use of mutex groups to create mutex services. See [Using Mutex Groups to Activate and Deactivate Subscriber Services](#) on page 473.

Figure 29 compares the two RADIUS-based methods.

**Figure 29: Comparing RADIUS Login and RADIUS CoA Methods**



### Using RADIUS to Activate Subscriber Service Sessions

To use RADIUS to activate subscriber service sessions, you create a RADIUS record that includes the Activate-Service VSA. For the RADIUS login method, this RADIUS record is used by the Access-Accept message to start Service Manager and activate the service when the subscriber logs in.

For the RADIUS CoA method, the service provider uses a CoA-Request message to activate and deactivate the service for the subscriber who is already logged in.

To configure a service session that will be activated by RADIUS:

1. Create the RADIUS record for the subscriber and service:
  - For RADIUS login—Create the RADIUS record for the subscriber and include the Activate-Service VSA in the record. Specify values for the parameters defined in the service template name of the definition macro file.
  - For RADIUS CoA—Format the CoA message to create the RADIUS record for the subscriber. Include the Activate-Service VSA in the record. Optionally, include the Deactivate-Service VSA if the subscriber has an active service session that you want to deactivate. Specify values for the parameters defined in the service template name of the definition macro file.



**NOTE:** You specify the parameter values in the order in which the parameters appear in the template name of the service definition file. For example, in the tiered service that is defined in [Figure 27 on page 455](#), the template name is:

```
<# tiered(inputBW, outputBW) #>
```

For the RADIUS Activate-Service VSA, you specify values for the input and output bandwidth:

```
tiered(1280000, 5120000)
```

2. Specify optional VSAs for the service session as needed:

- Service-Volume
- Service-Timeout
- Service-Stats

## Service Manager RADIUS Attributes

For the RADIUS login method, the RADIUS VSAs for service activation, threshold configuration, and statistics configuration in Access-Accept messages at subscriber login are used by Service Manager to activate the appropriate service session. For the RADIUS CoA method, Service Manager uses the VSAs for service activation and deactivation, threshold configuration, and statistics configuration in CoA-Request messages to activate the service session. The accounting-related VSAs are included in RADIUS accounting messages.

[Table 43](#) lists the Service Manager-related attributes and indicates which are tagged VSAs. See [Using Tags with RADIUS Attributes](#) on page 471 for a discussion about using tagged VSAs to group attributes for a service.

**Table 43: Service Manager RADIUS Attributes**

| Attribute Number | Attribute Name     | RADIUS Message Type           | VSA Description                                                                                                                         |
|------------------|--------------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| [26-65]          | Activate-Service   | Access-Accept and CoA-Request | Name of the service to be activated; includes parameter values; a tagged VSA                                                            |
| [26-66]          | Deactivate-Service | Access-Accept and CoA-Request | Name of the service to be deactivated<br><br><b>Note:</b> This VSA is only used by CoA.                                                 |
| [26-67]          | Service-Volume     | Access-Accept and CoA-Request | Number of MB of traffic that the service can consume; the service is terminated when output byte count exceeds this value; a tagged VSA |
| [26-68]          | Service-Timeout    | Access-Accept and CoA-Request | Number of seconds that the service is to remain active; the service is terminated when the time expires; a tagged VSA                   |

**Table 43: Service Manager RADIUS Attributes (continued)**

| Attribute Number | Attribute Name  | RADIUS Message Type                                                   | VSA Description                                                                                                                                                                                   |
|------------------|-----------------|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [26-69]          | Service-Stats   | Access-Accept and CoA-Request                                         | Statistics configuration; a tagged VSA:<br>0 = disable<br>1 = timestamp only<br>2 = timestamp and volume                                                                                          |
| [26-83]          | Service-Session | For service sessions only:<br>Acct-Start<br>Acct-Stop<br>Interim-Acct | Name of the service (including parameter values) with which the statistics are associated                                                                                                         |
| [44]             | Acct-Session-ID | Acct-Start<br>Acct-Stop<br>Interim-Acct                               | Accounting identifier that makes it easy to match start and stop records in a log file; the format is extended to include a colon-separated value that uniquely identifies the subscriber session |



**NOTE:** Service Manager statistics collection is a two-part procedure. You must configure statistics information in the service definition macro file and also enable statistics collection in the RADIUS record.

The Service-Volume and Service-Timeout VSAs rely on the values captured by the Service Manager statistics feature to determine when a threshold is exceeded. Therefore, you must configure and enable statistics collection to use these attributes. Service-Volume For detailed information about Service Manager statistics see [Configuring Service Manager Statistics](#) on page 485.

[Table 44](#) describes a partial RADIUS Access-Accept packet that activates a service session for subscriber client1@isp1.com. ([Figure 27 on page 455](#) shows the service definition macro file that creates the tiered service.) The session enables the subscriber to use the tiered service with an input bandwidth of 1280000 and output bandwidth of 5120000. The subscriber can use the service for 5 hours (18000 seconds), and Service Manager captures both timestamp and volume statistics during the session (service-statistics value of 2).

**Table 44: Sample RADIUS Access-Accept Packet**

| RADIUS Attribute   | Tag  | Value                    |
|--------------------|------|--------------------------|
| username           | none | client1@isp1.com         |
| class              | none | (binary data)            |
| service-activation | 6    | tiered(1280000, 5120000) |
| service-timeout    | 6    | 18000                    |
| service-statistics | 6    | 2                        |

### Using Tags with RADIUS Attributes

Service Manager uses tagged RADIUS VSAs to enable a single RADIUS record to activate multiple service sessions for a subscriber, with each session having unique attributes. A particular tag identifies a specific Activate-Service attribute and all other RADIUS attributes that are associated with that Activate-Service attribute.

You can specify a maximum of 8 tags (1–8), which enables you to activate up to eight unique service sessions for a subscriber in a single RADIUS record. The following are tagged VSAs—they must always have a tag in their RADIUS entry:

- Activate-Service
- Service-Stats
- Service-Timeout
- Service-Volume

Table 45 describes an Access-Accept packet that activates the two services, tiered and voice, for subscriber client1@isp1.com. Each service has its own unique tag, enabling you to assign attributes for one service, but not the other. For example, the two services have different timeout settings, and statistics are enabled only for the tiered service.

**Table 45: Using Tags**

| RADIUS Attribute   | Tag  | Value                    |
|--------------------|------|--------------------------|
| username           | none | client1@isp1.com         |
| class              | none | (binary data)            |
| service-activation | 2    | tiered(1280000, 5120000) |
| service-timeout    | 2    | 18000                    |
| service-statistics | 2    | 1                        |
| service-activation | 6    | voice(100000)            |
| service-timeout    | 6    | 1440                     |

### Using RADIUS to Deactivate Service Sessions

A service session can be deactivated by a CoA-Request message or when a subscriber logs out of a RADIUS-activated service session. If the subscriber logs off the router, Service Manager deactivates that subscriber session and all associated service sessions.

RADIUS also supports attributes that you can use to manage deactivation of service sessions. You can:

- Set time or volume thresholds for the service
- Use the Deactivate-Service RADIUS attribute

## Setting Thresholds

You can set a threshold for the session by including one or both of the following attributes in the RADIUS record:



**NOTE:** The Service-Timeout and Service-Volume attributes use values captured by the Service Manager statistics feature to determine when a threshold is exceeded. Therefore, you must configure and enable statistics collection to use these attributes. See [Configuring Service Manager Statistics](#) on page 485.

- **Service-Timeout**—The number of seconds that the service session is active. You can specify a number in the range 0–16777251. A value of 0 indicates that the session never times out. A particular Service-Timeout VSA can be used by a maximum of 2000 services.

The service-timeout threshold accuracy is within 30 seconds of the specified value.

- **Service-Volume**—The total number of MB of traffic that can use the service session. You can specify a number in the range 0–16777251 MB. A value of 0 indicates that there is no limit to the amount of traffic for the session. A particular Service-Volume VSA can be used by a maximum of 1000 services.



Service Manager terminates a session when the *output* byte count exceeds the configured service-volume threshold. The output byte count is captured by the **output-stat-clacl** string in the classifier list variable that you configure to collect statistics. See [Configuring Service Manager Statistics](#) on page 485.

The service-volume threshold accuracy is based on a 30-second period. Service Manager does not immediately deactivate a service session when the output byte count reaches the service-volume threshold. Instead, Service Manager checks the volume in 30-second intervals and deactivates a service session at the end of the 30-second period in which the output byte count reaches the volume threshold. For example, if a threshold is reached 5 seconds into the 30-second interval, the session continues for the remaining 25 seconds in the measuring period and is then terminated. Therefore, the total volume equals the threshold plus the volume during the additional 25 seconds.

When the output byte count reaches the threshold, RADIUS deactivates the service session. You must use tags to associate threshold attributes with the Activate-Service attribute for the service session.

## Using the Deactivate-Service Attribute

You can also include the Deactivate-Service attribute in the subscriber's RADIUS record. The format for this attribute is the same as the format of the Activate-Service attribute—the name of the service, including parameters. The Deactivate-Service attribute is used by RADIUS CoA messages, such as in a guided entrance service. See [Guided Entrance Service Example](#) on page 492 for more information.



## Using Mutex Groups to Activate and Deactivate Subscriber Services

---

Service Manager supports two methods that use RADIUS CoA-Request messages to activate and deactivate subscriber services and that can also dynamically change a service that is currently provided to a subscriber.

In the first method, you use a CoA message with the Activate-Service VSA to activate the new service; you can optionally include the Deactivate-Service VSA to deactivate the subscriber's existing service. This method is described in [Using RADIUS to Activate Subscriber Service Sessions](#) on page 468.

The second method uses mutual exclusion (mutex) groups to create mutex services. With this method, you group services together in a mutex group. When you use a CoA message to activate a service that is in a mutex group, Service Manager activates the new service and implicitly deactivates any existing service that is a member of the same mutex group as the newly activated service. Service Manager does not deactivate an existing service that is a member of a different mutex group or is not a member of a mutex group.

Using mutex services results in an more reliable activation and deactivation process than the original CoA-Request method. With mutex services, Service Manager always activates the new service before deactivating the existing service. This ensures that the subscriber is never without an active service. In the original CoA-Request method, the order of activation and deactivation is random—in some cases the existing service might be deactivated before the new service is activated, or the new activation might fail. In these cases, the subscriber might be without an active service.

If statistics are enabled when you activate a mutex service, Service Manager sends a RADIUS Acct-Stop message for the deactivated service.

### Activating and Deactivating Multiple Services

The Service Manager mutex service feature enables you to activate and deactivate multiple services with a single CoA-Request message. A CoA-Request message can have more than one service activation request—the multiple service requests might be from the same mutex group or from different groups. The following examples describe how you might use mutex groups to activate and deactivate multiple services.

- **Example 1—Multiple mutex services of the same mutex group**

Service Manager activates the multiple mutex services, which are in the same group, then deactivates all previously existing services that are also members of that mutex group. Active services that are members of different mutex groups are unaffected.

- **Example 2—Multiple mutex services of different mutex groups**

Service Manager activates the mutex services, which are members of different mutex groups. Service Manager then deactivates all previously existing services that are members of the same mutex groups as any of the newly activated services. Active services that are members of different mutex groups are unaffected.

## Configuring a Mutex Service

To configure and enable a mutex service, you complete the following steps:

1. Create the new service definition and configure the service as a member of a mutex group.

When you create the service definition, include the following service attribute in the service definition, where *groupIndex* identifies the mutex group for this service.

```
<# env.setResult("mutex-group", "groupIndex") #>
```

For example (the mutex group attribute is highlighted in bold text):

```
!parameterizes input and output bandwidth
<# tiered(inputBW, outputBW) #>

<# uid := app.servicemanager.getUniqueId #>
<# name := "SM-tiered-" $ uid #>
<# oname := "SM-O-tiered-" $ uid #>

classifier-list matchAll ip any any
rate-limit-profile <# name #> one-rate
 committed-rate <# inputBW; '\n' #>

policy-list <# name; '\n' #>
 classifier-group matchAll precedence 10000
 rate-limit-profile <# name; '\n' #>
 traffic-class best-effort

policy-list <# oname; '\n' #>
 classifier-group matchAll precedence 10000
 traffic-class best-effort

profile <# name; '\n' #>
 ip policy secondary-input <# name #> statistics enabled merge
 ip policy output <# oname #> statistics enabled merge
 qos-profile triplePlayIP
 qos-parameter maxSubscBW <# outputBW; '\n' #>

<# env.setResult("mutex-group", "12") #>
<# env.setResult("activate-profile", name) #>
<# env.setResult("secondary-input-stat-clac1", "matchAll") #>
<# env.setResult("output-stat-clac1", "matchAll") #>

<# endtmpl #>
```

2. Activate the mutex service

Use a RADIUS CoA-Request message and the new service definition to create the mutex service. The new service is considered a mutex service because it belongs to a mutex group.

Service Manager activates the new service and deactivates any existing active service that is a member of the same mutex group as the new service.

3. (Optional) Verify the status of the new service.

```
host1#show service-management subscriber-session client1@isp.com interface ip
192.168.0.1
```

```
User Name: CLIENT1@ISP.COM, Interface: ip 192.168.0.1
```

```
Id: 1
```

```
Owner: AAA 4194326
```

```
Non-volatile: False
```

```
State: Active
```

```
ServiceSessions:
```

| Name                    | mutex        | Owner/Id    | State              | Operation |
|-------------------------|--------------|-------------|--------------------|-----------|
| tiered(2000000,3000000) | 12           | AAA 4194326 | ConfigApplySuccess | Activate  |
| Name                    | Non-volatile |             |                    |           |
| tiered(2000000,3000000) | False        |             |                    |           |

## Configuring RADIUS Accounting for Service Manager

The Service Manager application supports RADIUS accounting for subscriber service sessions that are activated by the RADIUS login and RADIUS CoA methods. When RADIUS accounting is enabled, RADIUS generates:

- An Acct-Start message when a service session is activated
- An Acct-Stop message when a service session is deactivated
- Interim-Acct messages

RADIUS accounting messages always include Service Manager time statistics. You must enable Service Manager volume statistics for a service session.



**NOTE:** Service Manager statistics collection is a two-part procedure. You must configure statistics information in the service definition macro file and also enable statistics collection. For detailed information about Service Manager statistics, see [Configuring Service Manager Statistics](#) on page 485.

To support RADIUS accounting for Service Manager, the RADIUS Acct-Session-ID attribute [44] has been extended to include a colon-separated identifier, which uniquely identifies a service for a subscriber. For example:

```
erx FastEthernet 12/0:0001048580:002478
```

The Service-Session attribute (VSA 26-83) identifies the name of the service. This attribute is the value of the Activate-Service or Deactivate-Service attribute (including parameter values) that was used in the RADIUS Access-Accept message to activate or deactivate the service session. For example:

```
tiered(1280000, 5120000)
```

Table 46 lists the RADIUS accounting attributes used by the Service Manager application.

**Table 46: Service Manager RADIUS Accounting Attributes**

| Attribute Number | Attribute Name  | RADIUS Message Type                                                   | VSA Description                                                                                                                                                                                   |
|------------------|-----------------|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [26-83]          | Service-Session | For service sessions only:<br>Acct-Start<br>Acct-Stop<br>Interim-Acct | Name of the service (including parameter values) with which the statistics are associated                                                                                                         |
| [44]             | Acct-Session-ID | Acct-Start<br>Acct-Stop<br>Interim-Acct                               | Accounting identifier that makes it easy to match start and stop records in a log file; the format is extended to include a colon-separated value that uniquely identifies the subscriber session |

Table 47 describes a sample Acct-Start message for a service session. In the table, the two fields used by Service Manager are highlighted. An Acct-Start message for a subscriber session without any active services does not include the Service-Session attribute.

**Table 47: Sample Acct-Start Message for a Service Session**

| RADIUS Attribute             | Sample Value                                   |
|------------------------------|------------------------------------------------|
| acct-status-type             | 1                                              |
| username                     | client1@isp1.com                               |
| event-timestamp              | 1112191723                                     |
| acct-delay-time              | 0                                              |
| nas-identifier               | ERX-01-00-06                                   |
| <b>acct-session-id</b>       | <b>erx FastEthernet 12/0:0001048580:002478</b> |
| nas-ip-address               | 10.6.128.45                                    |
| class                        | (binary data)                                  |
| framed-protocol              | 0                                              |
| framed-compression           | 0                                              |
| framed-ip-address            | 100.20.0.1                                     |
| framed-ip-netmask            | 0.0.0.0                                        |
| ingress-policy-name (vsa)    | forwardAll                                     |
| egress-policy-name (vsa)     | forwardAll                                     |
| calling-station-id           | #ERX-01-00-06#E12#0                            |
| acct-input-gigawords         | 0                                              |
| acct-input-octets            | 4032                                           |
| acct-output-gigawords        | 0                                              |
| acct-output-octets           | 2163                                           |
| acct-input-gigapackets (vsa) | 0                                              |

**Table 47: Sample Acct-Start Message for a Service Session (continued)**

|                               |                          |
|-------------------------------|--------------------------|
| acct-input-packets            | 7                        |
| acct-output-gigapackets (vsa) | 0                        |
| acct-output-packets           | 7                        |
| nas-port-type                 | 15                       |
| nas-port                      | 3221225472               |
| nas-port-id                   | FastEthernet 12/0        |
| acct-authentic                | 1                        |
| acct-session-time             | 0                        |
| acct-service-session          | tiered(1280000, 5120000) |

## Using the CLI to Manage Subscriber Service Sessions

The CLI-based Service Manager creates static subscriber sessions and service sessions. You can also use CLI commands to immediately deactivate subscriber service sessions. The CLI-based support is particularly useful for:

- Testing your service definitions—for example, you might use the CLI commands to verify that a newly created service definition is correct. When you are satisfied with the service definition, you can then use RADIUS to activate the service for your subscribers.
- Preprovisioning Service Manager services—preprovisioning improves performance and efficiency by freeing Service Manager from having to repeatedly create and remove a service that you activate and deactivate for multiple subscribers. See [Preprovisioning Services](#) on page 480 for more information about service preprovisioning.

## Using the CLI to Activate Subscriber Service Sessions

A subscriber session represents a specific subscriber—the session consists of the subscriber's name, the interface used for the session, and any active services for the subscriber. A subscriber can have one subscriber session active at any given time.

You create a subscriber's service session when you assign a service definition to a subscriber session. Like an AAA-created service, a single subscriber session can have multiple simultaneous service sessions. You can use one method to create the subscriber session, and then a different method to activate the subscriber's service session. For example, you might use RADIUS to create the AAA subscriber session, then use the CLI to activate the service session for the subscriber. You can optionally specify a service session profile that you want to attach to the service session.

You can use the CLI to activate a service session based on subscriber information or owner information:

- Subscriber name and interface method—Activates the service session based on the subscriber name and the interface that the subscriber is using for this subscriber session.

```
host1(config)#service-management subscriber-session client1@isp1.com
interface atm 4/0.1 service-session "tiered(1280000, 5120000)"
```

- Owner name and ID method—Activates the service session based on the owner that created the subscriber session and the ID that was generated by the owner. For example, if RADIUS is used to create the subscriber session, the owner name is AAA and the owner ID is the Acct-Session-ID that was generated by RADIUS during subscriber creation.

```
host1(config)#service-management owner-session AAA 537446 service-session
"tiered(1280000, 5120000)"
```



**NOTE:** You must specify the parameter values in the order in which the parameters appear in the template name of the service definition file. Enclose the service definition name in double quotation marks, with the service's parameter values in parentheses. For example, for the tiered service that is defined in [Figure 27 on page 455](#), the template name is:

```
<# tiered(inputBW, outputBW) #>
```

Use the following format with the **service-session** keyword:

```
"tiered(1280000, 5120000)"
```

#### **service-management owner-session**

- Use to activate a service for an existing subscriber by identifying the owner used to create the subscriber session and specifying the service session to use.
- The subscriber session must exist before you use this command.
- Use this command in Privileged Exec mode to create a dynamic subscriber session—dynamic sessions are deleted after a router reboot.
- Use this command in Global Configuration mode to create persistent subscriber sessions that are retained across reboots.
- Specify the name of the owner (the method originally used to create the subscriber session), and the ID generated by the of the owner. For example, if RADIUS was used to create the subscriber session, the owner name is AAA and the owner ID is the Acct-Session-ID generated by RADIUS when the subscriber session was created.
- Include the optional **service-session-profile** keyword to assign a profile to the service session. The service session profile includes additional attributes, such as the type of statistics to be captured for the service session.

- You can activate one subscriber session for a subscriber—and multiple service sessions for a particular subscriber session. If you create a second subscriber session for the same subscriber, only the newest subscriber session, with its services, is used.
- Example 1—Activate a service session for an existing subscriber  

```
host1(config)#service-management owner-session aaa 573498 service-session "video(4500000, 192.168.10.3)"
```
- Example 2—Activate multiple service sessions for an existing subscriber  

```
host1(config)#service-management owner-session aaa 573498 service-session "video(4500000, 192.168.10.3)"
host1(config)#service-management owner-session aaa 573498 service-session "tiered(1000000, 2000000)"
host1(config)#service-management owner-session aaa 573498 service-session "voice(1000000, 10.10.10.1)"
```
- Example 3—Include a service session profile when you activate a subscriber's service session  

```
host1(config)#service-management owner-session aaa 426777 service-session "video(4500000, 192.168.10.3)" service-session-profile vodISP1
```
- Use the **no** version to deactivate service sessions based on owner information. See [Using the CLI to Deactivate Subscriber Service Sessions](#) on page 483 for more information about deactivating subscriber service sessions.

### **service-management subscriber-session service-session**

- Use to activate a service for a subscriber by creating a subscriber session and a service session.



**NOTE:** Always activate at least one service session for a subscriber session. The ability to create a subscriber session without a service session (by omitting the **service-session** keyword) is not currently supported.

---

- Use this command in Privileged Exec mode to create a dynamic subscriber session—dynamic sessions are deleted after a router reboot.
- Use this command in Global Configuration mode to create persistent subscriber sessions that are retained across reboots.
- Include the optional **service-session-profile** keyword to assign a profile to the service session. The service session profile includes additional attributes, such as the type of statistics to be captured for the service session.
- You can create one subscriber session for a subscriber—and multiple service sessions for a particular subscriber session. If you create a second subscriber session for the same subscriber, only the newest subscriber session, with its services, is used.
- Example 1—Activate a subscriber session with a single service session  

```
host1(config)#service-management subscriber-session client1@isp1.com interface atm 4/0.1 service-session "video(4500000, 192.168.10.3)"
```

- Example 2—Activate a single subscriber session with multiple service sessions

```
host1(config)#service-management subscriber-session client1@isp1.com
interface atm 4/0.1 service-session "video(4500000, 192.168.10.3)"
host1(config)#service-management subscriber-session client1@isp1.com
interface atm 4/0.1 service-session "tiered(1000000, 2000000)"
host1(config)#service-management subscriber-session client1@isp1.com
interface atm 4/0.1 service-session "voice(1000000, 10.10.10.1)"
```

- Example 3—Include a service session profile when you activate a subscriber's service session

```
host1(config)#service-management subscriber-session client1@isp1.com
interface atm 4/0.1 service-session "video(4500000, 192.168.10.3)"
service-session-profile vodISP1
```

- Use the **no** version to deactivate service sessions. See [Using the CLI to Deactivate Subscriber Service Sessions](#) on page 483 for more information about deactivating subscriber service sessions.

## Preprovisioning Services

Preprovisioning service sessions is a technique you can use to improve Service Manager's performance. Typically, when you use a service definition to activate a subscriber's service session, Service Manager uses resources to build that service. However, if you later use the same service definition to activate a service session for a second subscriber, Service Manager does not have to rebuild the service—it bases the new service on the service that it built for the first service session. After you deactivate the first session, Service Manager must build a new service for any subsequent subscribers.

Preprovisioning entails activating a service for a dummy user on the null interface. You can then use the preprovisioned service session to activate service sessions for actual subscribers. This technique improves performance because you only require Service Manager to build the service one time, then reuse the original service when you activate future subscriber service sessions.

To preprovision a service you use a command similar to the following example:

```
host1(config)#service-management subscriber-session dummy interface null
service-session "tiered(1000000, 2000000)"
```

## Using Service Session Profiles

Service session profiles provide additional flexibility to the Service Manager application by enabling you to assign one or more supported attributes to a particular activation of a service.

For example, you might assign the same video service to two subscribers, but use different service session profiles to set different time limits for each subscriber's service. One subscriber uses the video service for 5 hours (18000 seconds) while the other subscriber's video service is for 10 hours (36000 seconds). Or, you might enable statistics on a subscriber's voice service and disable statistics on the same subscriber's video service.



You can create multiple service session profiles independent of the service activation process. Then, when you activate a service session, you specify the profile that you want to use with that particular service session—you can apply one profile to a service session.

You can configure the following attributes in service session profiles:

- **statistics**—Enables statistics and specifies the type of statistics you want to capture for the service. See [Configuring Service Manager Statistics](#) on page 485 for additional information about capturing Service Manager statistics. You can specify the following types of statistics:
  - **time**—The service’s duration
  - **volume-time**—The service’s duration and traffic volume
- **volume**—Specifies that the service is automatically deactivated when the indicated traffic volume is exceeded.
- **time**—Specifies that the service is automatically deactivated when the indicated time period is exceeded.



**NOTE:** The **volume** and **time** attributes use values captured by the Service Manager statistics feature to determine when the threshold is exceeded. Service Manager collects time statistics by default—you must configure and enable volume statistics collection. See [Configuring Service Manager Statistics](#) on page 485.

To create or modify a service session profile:

1. Specify the name of the service session profile; doing this enters Service Session Profile Configuration mode.

```
host1(config)#service-management service-session-profile vodISP1
host1(config-service-session-profile)#
```

2. Specify the attributes you want to include in the profile.

```
host1(config-service-session-profile)#statistics volume-time
host1(config-service-session-profile)#time 6000
```

3. (Optional) To modify an existing profile, you can add new attributes or use the **no** version of a command to remove an attribute.

```
host1(config-service-session-profile)#no time
```

**service-management service-session-profile**

- Use to create a new service session profile or to specify the name of an existing profile you want to modify, and to enter Service Session Profile Configuration mode.
- In Service Session Profile Configuration mode, you specify the attributes used in the service session profile, such as the maximum volume limit for the session and the maximum time the session can be used. You can also specify that Service Manager collect statistics for time, or volume, or both.
- Example  

```
host1(config)#service-management service-session-profile vodISP1
host1(config-service-session-profile)#
```
- Use the **no** version to delete the service session profile.

**statistics**

- Use to enable statistics collection and to specify the type of statistics to collect.
  - Use the **time** keyword to collect statistics about the duration of the service session.
  - Use the **volume-time** keyword to collect statistics about both the volume of traffic and the duration of the service session.
- Example  

```
host1(config)#service-management service-session-profile vodISP1
host1(config-service-session-profile)#statistics volume-time
```
- Use the **no** version to disable statistics collection.



**NOTE:** Service Manager statistics collection is a two-part procedure. You must configure statistics information in the service definition macro file and also enable statistics collection. See [Configuring Service Manager Statistics](#) on page 485.

---

**time**

- Use to specify the maximum amount of time that the service session can be active for the subscriber.
- The router immediately terminates the subscriber's service session when the specified time is exceeded.
- The range is 0–16777251 seconds.
- Example  

```
host1(config)#service-management service-session-profile vodISP1
host1(config-service-session-profile)#time 6000
```
- Use the **no** version to delete the time attribute from the service session profile.

**volume**

- Use to specify the maximum amount of bandwidth that can use the service.
- The router immediately terminates the subscriber's service session when the specified traffic volume is exceeded.



**NOTE:** The **volume** attribute uses values captured by the Service Manager statistics feature to determine when the threshold is exceeded. Therefore, you must configure and enable statistics collection to use this attribute. See [Configuring Service Manager Statistics](#) on page 485.

- The range is 0–16777251 MB.
- Example  

```
host1(config)#service-management service-session-profile vodISP1
host1(config-service-session-profile)#volume 1000000
```
- Use the **no** version to delete the volume attribute from the service session profile.

## Using the CLI to Deactivate Subscriber Service Sessions

The CLI supports several methods that enable you to manually deactivate service sessions. You can:

- Gracefully terminate all services or a specific service for a particular subscriber
- Gracefully terminate all service or a specific service associated with a particular owner
- Force the immediate termination of all of a subscriber's sessions
- Use service session profiles to create time or volume thresholds for the service and deactivate the service when the threshold is reached. See [Using Service Session Profiles](#) on page 480.



**NOTE:** You can use the CLI commands described in this section to delete subscriber and service sessions that are created by either RADIUS or the CLI.

The Service Manager CLI commands enable you to use variations of the **no service-management subscriber-session** command to terminate service sessions.

### Gracefully Deactivating Subscriber Service Sessions

Use the following commands to gracefully deactivate subscriber's services—you can deactivate a specific service for a subscriber, or you can delete a subscriber session, which deactivates all of the subscriber's service sessions. We recommend you use this command to deactivate subscriber service sessions.

***no service-management owner-session***

- Use to gracefully deactivate service sessions for a subscriber based on owner information.
- Specify the owner name and owner ID of the service session you want to deactivate.
- Use the **no** version with the **service-session** keyword to deactivate the specified service session.
- Use the **no** version *without* the **service-session** keyword to delete the subscriber's session and deactivate all of the subscriber's service sessions.
- Example  

```
host1(config)#no service-management owner-session aaa 426777
service-session "video(4500000, 192.168.10.3)"
```
- This is the **no** version of the **service-management owner-session** command.

***no service-management subscriber-session service-session***

- Use to gracefully deactivate service sessions for a subscriber.
- Use the subscriber's username and interface, not the subscriber session ID, for graceful deactivation.
- Use the **no** version without the **service-session** keyword to delete the subscriber's session and deactivate all of the subscriber's service sessions.
- Use the **no** version with the **service-session** keyword to deactivate the specified service session.
- Example  

```
host1(config)#no service-management subscriber-session client1@isp1.com
interface atm 4/0.1 service-session "tiered(1000000, 2000000)"
```
- This is the **no** version of the **service-management subscriber-session** command.

**Forcing Immediate Deactivation of Subscriber Service Sessions**

Use the following command to force the immediate deactivation of the specified subscriber session—doing this deletes all active service sessions for the subscriber. We recommend this method if you encounter difficulty when you used the graceful deactivation method. Always use the graceful method first.

***no service-management subscriber-session force***

- Use to force the immediate termination of a subscriber session and to deactivate all services for the specified subscriber session.
- You must specify the subscriber session ID to use the **force** keyword to terminate the subscriber session.



**NOTE:** To determine the subscriber session ID of a session you want to deactivate, use the **show service-management subscriber-session brief** command. The display lists the IDs of all active subscriber sessions and the owner that created the session, such as AAA (RADIUS) or CLI.

- Example

```
host1(config)#no service-management subscriber-session 8 force
```

- There is no affirmative version of this command; there is only a **no** version.

### Using Service Session Profiles to Deactivate Service Sessions

To terminate a subscriber service session when a threshold is reached, you create a service session profile that includes a time threshold, or a volume threshold, or both. Then, you attach the service session profile when you activate the service session. When the specified threshold is reached, the service session is terminated.



**NOTE:** This feature is not supported by the **service-management owner-session** command. The **service-management owner-session** command only supports service session profiles when activating service sessions.

The following example shows the commands you might use to create a time threshold for deactivating a service session. See [Using Service Session Profiles](#) on page 480 for information about using the **time** and **volume** keywords in service session profiles.

To create or modify a service session profile:

1. Specify the name of the service session profile and configure the threshold:

```
host1(config)#service-management service-session-profile vodISP1
host1(config-service-session-profile)#time 6000
host1(config-service-session-profile)#exit
```

2. Include the service session profile when you activate the subscriber service session:

```
host1(config)#service-management subscriber-session client1@isp1.com
interface atm 4/0.1 service-session "video(4500000, 192.168.10.3)"
service-session-profile vodISP1
```

## Configuring Service Manager Statistics

The Service Manager application provides a flexible and efficient process for identifying and capturing statistics related to subscriber service sessions. Configuring Service Manager to collect statistics is a two-part process. First, you design the service definition macro file to identify the statistics that you want to collect. Second, you configure Service Manager to enable statistics collection when a service session is activated by either RADIUS or the CLI.

The following section describes how to configure the service definition macro file. For information about configuring Service Manager to enable statistics, see [Enabling Statistics Collection with RADIUS](#) on page 487 if you are using RADIUS to activate services, or see [Enabling Statistics Collection with the CLI](#) on page 487 if you are using the CLI.

## Setting Up the Service Definition File for Statistics Collection

Service Manager statistics are based on classifier lists—the classifier lists are referenced by policy lists that you define in your service definition macro file.

When you configure your service definition for statistics, you include the macro environment command **env.setResult** to indicate the type of statistics to track and to identify the classifier lists to use when generating statistics. The format of the environment command is:

```
<# env.setResult("string", "classifier-list-name") #>
```

The *string* variable specifies the type of statistics to track—Service Manager supports the following strings:

- **input-stat-clacl**—track input statistics
- **output-stat-clacl**—track output statistics
- **secondary-input-stat-clacl**—track input statistics for a policy attached at the secondary input stage

The *classifier-list-name* variable is the name of the classifier list that is associated with the policy list that is defined in the service definition. You can specify multiple classifier lists in the command.

**Example 1** This example is a portion of the service definition macro file in [Figure 27 on page 455](#). The two highlighted commands specify the statistics used by the Service Manager application.

```
profile <# name; '\n' #>
 ip policy secondary-input <# name #> statistics enabled merge
 ip policy output <# oname #> statistics enabled merge
 qos-profile triplePlayIP
 qos-parameter maxSubscBW <# outputBW; '\n' #>

<# env.setResult("activate-profile", name) #>
<# env.setResult("secondary-input-stat-clacl", "matchAll") #>
<# env.setResult("output-stat-clacl", "matchAll") #>

<# endtmpl #>
```

The **<# env.setResult("secondary-input-stat-clacl", "matchAll") #>** command specifies that Service Manager track statistics associated with the classifier list named *matchAll*, and that this classifier list is associated with the policy that is attached at the secondary input stage.

The **<# env.setResult("output-stat-clacl", "matchAll") #>** command specifies that Service Manager track the output statistics associated with the *matchAll* classifier list, which is associated with the policy attached at the output stage.

**Example 2** This example shows how you can also configure your service definition to collect total statistics from multiple classifier lists. The following command specifies that three classifier lists are used to generate output statistics for a service created by the service definition. Each time statistics are reported for this service, Service Manager uses the total of the statistics for clacl1, clacl2, and clacl3.

```
<# env.setResult("output-stat-clacl", "clacl1" "clacl2" clacl3") #>
```

### Enabling Statistics Collection with RADIUS

You use the Service-Stats RADIUS VSA [26-69] with either the RADIUS login or CoA-Request method to enable statistics for RADIUS-activated service sessions. To enable statistics, configure the Service-Stats VSA with a value of either 1 (timestamp only) or 2 (volume and timestamp).

Table 48 describes a partial RADIUS message in which the Service-Stats attribute has a value of 2—this enables volume and timestamp statistics for the tiered service assigned to subscriber client1@isp1.com.

**Table 48: RADIUS-Enabled Statistics**

| RADIUS Attribute | Tag  | Value                    |
|------------------|------|--------------------------|
| username         | none | client1@isp1.com         |
| activate-service | 6    | tiered(1280000, 5120000) |
| service-stats    | 6    | 2                        |

When you enable statistics for a RADIUS-activated service, RADIUS accounting reports can use the statistics.

### Enabling Statistics Collection with the CLI

You use service session profiles to enable statistics when you activate a service session with the CLI. See [Using Service Session Profiles](#) on page 480 for detailed information about creating and using service session profiles.

For example, you can use the following procedure to capture statistics that are defined in the service definition macro file for the tiered service:

1. Configure the service session profile to enable statistics. Specify the type of statistics you want to capture (either time or both volume and time).

```
host1(config)#service-management service-session-profile isp1_tiered3
host1(config-service-session-profile)#statistics volume-time
host1(config-service-session-profile)#
```

2. Apply the service session when you activate the subscriber service session.

```
host1(config)#service-management subscriber-session client1@isp1.com
interface atm 4/0.1 service-session "tiered(1000000, 2000000)"
service-session-profile isp1_tiered3
```

The captured statistics are now used when you use the Service Manager **show service-management** commands. For example:

```
host1#show service-management subscriber-session client1@isp1.com interface atm
4/0.1 service-session
User Name: client1@isp1.com, Interface: atm 4/0.1
Service : tiered(1000000,2000000)
Non-volatile : False
Owner : CLI
State : Config ApplySuccess
Activate : True
Statistics Type : time-based and volume-based
Statistics Complete : False
Poll Interval : 0
Poll Expire : 0
Activate Time : THU MAR 01 21:09:12 2006
Time : 0
Time Expire : 0
Volume MBytes: 2
Volume Expire MBytes: 1
Input Bytes : 594
Output Bytes : 1196
Input Packets : 1
Output Packets : 2
```

## Service Manager Performance Considerations

---

Like any application, Service Manager requires a certain amount of system resources. Consider the following guidelines to maximize the performance of Service Manager when delivering subscriber services:

- Minimize service definitions—Use the minimum number of JUNOS commands in a service definition to specify a service.
- Reference objects in service definitions—Referencing commonly used objects is more resource-efficient than using unique objects for each subscriber (for example, using a subscriber's IP address as a match criteria in a classifier list).
- Preprovision frequently used services— Preprovisioning saves resources by requiring Service Manager to build a popular service only once. You then reuse the original service when you activate future subscriber service sessions. See [Preprovisioning Services](#) on page 480 for details.
- Capture volume statistics when needed—Repeatedly capturing volume statistics can waste resources.



## Service Definition Examples

This section provides examples of service definition macro files. Commented text explains the parameterized values in the examples. Each example is followed by examples of RADIUS information and the CLI command that you might use to activate a subscriber service session.

### Tiered Service Example

This example creates a tiered service. A tiered service typically provides set bandwidths for both inbound and outbound traffic for a subscriber. In this example, the bandwidth values are parameterized. Also, this example assumes that QoS profile triplePlayIP and QoS parameter maxSubscBW are configured.

```
!parameterizes input and output bandwidth
<# tiered(inputBW, outputBW) #>

<# uid := app.servicemanager.getUniqueId #>
<# name := "SM-tiered-" $ uid #>
<# oname := "SM-O-tiered-" $ uid #>

classifier-list matchAll ip any any
rate-limit-profile <# name #> one-rate
 committed-rate <# inputBW; '\n' #>

policy-list <# name; '\n' #>
 classifier-group matchAll precedence 10000
 rate-limit-profile <# name; '\n' #>
 traffic-class best-effort

policy-list <# oname; '\n' #>
 classifier-group matchAll precedence 10000
 traffic-class best-effort

profile <# name; '\n' #>
 ip policy secondary-input <# name #> statistics enabled merge
 ip policy output <# oname #> statistics enabled merge
 qos-profile triplePlayIP
 qos-parameter maxSubscBW <# outputBW; '\n' #>

<# env.setResult("activate-profile", name) #>
<# env.setResult("secondary-input-stat-clacl", "matchAll") #>
<# env.setResult("output-stat-clacl", "matchAll") #>

<# endtmpl #>
```

#### Sample RADIUS Attributes

| RADIUS Attribute | Tag  | Value                    |
|------------------|------|--------------------------|
| username         | none | client1@isp1.com         |
| activate-service | 1    | tiered(1280000, 5120000) |

#### Sample CLI Command

```
host1(config)#service-management subscriber-session client1@isp1.com
interface atm 4/0.1 service-session "tiered(1280000, 5120000)"
```

## Video-on-Demand Service Definition Example

The following example shows a sample service definition macro file that creates a video-on-demand service—the service provides bandwidth that meets the needs of video streams. The definition creates the bandwidth towards the subscriber and parameterizes the source of the video feed.

The sample CLI command shows an example of the **service-management owner-session** command that you can use to activate the service session.

```
!parameterizes download bandwidth and server address
<# videoMin(downloadBW, serverAddress) #>

<# uid := app.servicemanager.getUniqueId #>
<# name := "SM-video-" $ uid #>

classifier-list <# name #> ip any <# serverAddress #> 0.0.0.0

policy-list <# name; '\n' #>
 classifier-group <# name #> precedence 5000
 traffic-class video

profile <# name; '\n' #>
 ip policy output <# name #> statistics enabled merge
 qos-parameter maxVideoBW add <# downloadBW; '\n' #>
 exit

<# env.setResult("activate-profile", name) #>
<# env.setResult("output-stat-clacl", name) #>

<# endtmpl #>
```

### Sample Owner ID

| Owner        | Owner ID                              | Value  |
|--------------|---------------------------------------|--------|
| AAA (RADIUS) | Acct-Session-ID (RADIUS attribute 44) | 573498 |

### Sample CLI Command

```
host1(config)#service-management owner-session aaa 573498 service-session
"videoMin(4500000, 192.168.23.58)"
```

## Voice-over-IP Service Definition Example

This example provides a voice-over-IP service. The service is a session border controller (SBC) media gateway (MG)-based service that has upstream and downstream components.

The IP address and port for both the subscriber and the opposite end of the phone call were originally negotiated with the SBC. The VoIP service learns the IP addresses and ports for both ends of the call, and then specifies that any traffic to either end is put in the voice traffic class.

```
!parameterizes source address and port, destination address and port, and protocol type
<# mgFlow(upDA, upDPort, downDA, downDPort, protType) #>

<# uid := app.servicemanager.getUniqueId #>
<# name := "SM-mgFlow-" $ uid #>
<# oname := "SM-O-mgFlow-" $ uid #>

classifier-list <# name #> <# protType #> any <#upDA #> 0.0.0.0 eq <# upDPort; '\n' #>
policy-list <# name; '\n' #>
 classifier-group <# name #> precedence 2000
 traffic-class voice
 forward

classifier-list <# oname #> <# protType #> any <#downDA #> 0.0.0.0 eq <# downDPort; '\n' #>
policy-list <# oname; '\n' #>
 classifier-group <# oname #> precedence 2000
 traffic-class voice
 forward

profile <# name; '\n' #>
 ip policy input <# name #> statistics enabled merge
 ip policy output <# oname #> statistics enabled merge

<# env.setResult("activate-profile", name) #>

<# endtmpl #>
```

### Sample RADIUS Attributes

| RADIUS Attribute | Tag  | Value                                               |
|------------------|------|-----------------------------------------------------|
| username         | none | client1@isp1.com                                    |
| activate-service | 1    | mgFlow(10.10.10.10, 1234, 192.168.45.54, 1234, udp) |

### Sample CLI Command

```
host1(config)#service-management subscriber-session client1@isp1.com
interface atm 4/0.1 service-session "mgFlow(10.10.10.10, 1234,
192.168.45.54, 1234, udp)"
```

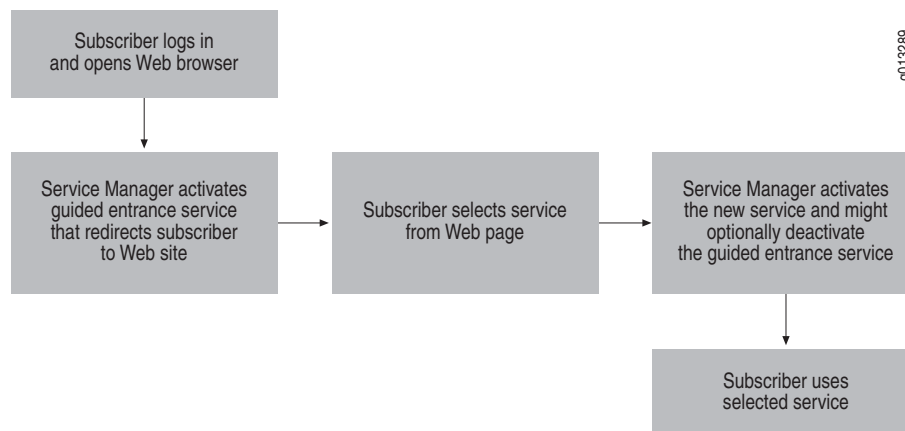
## Guided Entrance Service Example

The guided entrance service enables you to create a controlled Internet browsing environment. Guided entrance-based services, which are sometimes called *walled gardens* or *captive portals*, are becoming increasingly important offerings for service providers. When a subscriber logs in and opens a Web browser, the Service Manager guided entrance service transparently directs the subscriber to a specific Web site—at that Web site, the subscriber is presented with a selection of possible services to use. For example, a subscriber might be shown a Web site that offers services such as:

- **Predefined services**—A group of user-selectable services that meets a variety of needs of a single subscriber. The subscriber might select the high-priced highest access speed to perform critical financial transactions but select a lower speed (and lower cost) service for e-mail. For viewing a real-time sports event, the subscriber can select the video-on-demand service. The subscribers have control over the choice and cost of the services they need and use.
- **Prepaid services**—A group of specific services that have been prepaid by the subscriber. For example, a subscriber who has purchased the sports package service is presented with a Web page that lists the currently available sporting events. Or, a subscriber might prepay a VoIP service for a set amount of time.
- **Controlled-service**—An educational service that enables students at a school to access authorized research sites. Or, a limited service for young children that restricts access to safe, closely monitored, age-appropriate Web sites.

Figure 30 shows the sequence of actions that take place during a guided entrance service.

**Figure 30: Guided Entrance**



Service Manager requires additional configuration considerations for the guided entrance service.

- The `<# redirectUrlName := "http://" $ serverIp $ ":" $ serverPort #>` command in the service definition—Specifies the HTTP local service to which the subscriber is redirected after login. See [Guided Entrance Service Definition Example](#) on page 493 for a sample guided entrance service definition.



**NOTE:** You must also configure a policy that redirects packets. See [JUNOS Policy Management Configuration Guide, Chapter 2, Creating Policies](#) for information on creating redirect policies.

- HTTP local server application—Used by the policy in the activated service to direct a subscriber to a specific Web site when the subscriber logs in. See [Configuring the HTTP Local Server to Support Guided Entrance](#) on page 495 for information about the HTTP local server.
- RADIUS Dynamic Request Server and CoA messages—Enables RADIUS to dynamically activate the new service that the subscriber selects at the Web site. Can also optionally deactivate the original guided entrance service session that is used when the subscriber logs in. See [Chapter 3, Configuring RADIUS Dynamic-Request Server](#).

### Guided Entrance Service Definition Example

This example shows a guided entrance service. Upon login, the subscriber is redirected to a specific uniform resource locator (URL) at which the subscriber can choose from a list of available services.

```
!parameterizes server address and port
<# http(serverIp, serverPort) #>

<# serviceTag := "http-" #>
<# uid := app.servicemanager.getUniqueId #>
<# genericName := "SM-X-" $ serviceTag $ uid #>
<# genericInputName := "SM-I-" $ serviceTag $ uid #>
<# genericOutputName := "SM-O-" $ serviceTag $ uid #>
<# clacName := genericName #>

<# profileName := genericName #>
<# inputPolicyName := genericInputName #>
<# inputRateLimitName := genericInputName #>
<# outputPolicyName := genericOutputName #>
<# outputRateLimitName := genericOutputName #>

<# exceptionClacName := "exceptionClacPort" $ serverPort #>
<# serverClacName := "serverClacIp" $ serverIp #>
<# redirectUrlName := "http://" $ serverIp $ ":" $ serverPort #>

configure terminal

classifier-list <# serverClacName #> ip any host <# serverIp; '\n' #>

classifier-list <# exceptionClacName #> tcp any any eq <# serverPort; '\n' #>
```

```

ip policy-list <# inputPolicyName; '\n' #>
 classifier-group <# serverClacName; '\n' #>
 forward
 classifier-group <# exceptionClacName; '\n' #>
 exception http-redirect
 classifier-group *
 filter

profile <# profileName #>
 ip http redirectUrl <# redirectUrlName; '\n' #>
 ip policy input <# inputPolicyName #> statistics enabled merge

<# env.setResult("activate-profile", "" $ profileName) #>

<# endtmpl #>

```

#### Sample RADIUS Attributes

| RADIUS Attribute | Tag  | Value                  |
|------------------|------|------------------------|
| username         | none | client5@isp1.com       |
| activate-service | 1    | http(192.168.25.2, 80) |

#### Sample CLI Command

```

host1(config)#service-management subscriber-session client5@isp1.com
interface atm 5/0.1 service-session "http(192.168.25.2, 80)"

```

### Using CoA Messages with Guided Entrance Services

Typically, a guided entrance service directs a subscriber to a Web site, where the subscriber can select from a group of available services. When the subscriber selects a new service to use, Service Manager uses a RADIUS CoA message to activate the new service—you can also configure RADIUS to deactivate the original guided entrance service. To inform Service Manager to deactivate the original guided entry service, you must include the Deactivate-Service attribute in the RADIUS records of the services that can be selected from the Web site.

If you configure a guided entrance service, you must also ensure that the router's RADIUS dynamic-request server is enabled and supports CoA messages. See [Chapter 3, Configuring RADIUS Dynamic-Request Server](#), for information about the RADIUS dynamic-request server and CoA messages.

[Table 49](#) describes a partial RADIUS Access-Accept message for a guided entrance service and the CoA-Request message for the tiered service that the subscriber subsequently selects from the Web site. The CoA message for the tiered service includes the Deactivate-Service attribute that deactivates the guided entrance service.

**Table 49: Deactivating a Guided Entrance Service****Guided Entrance Service Activated at Login**

| <b>RADIUS Attribute</b> | <b>Tag</b> | <b>Value</b>           |
|-------------------------|------------|------------------------|
| username                | none       | client5@isp1.com       |
| activate-service        | 1          | http(192.168.25.2, 80) |

**Tiered Service Selected at Web Site**

| <b>RADIUS Attribute</b> | <b>Tag</b> | <b>Value</b>             |
|-------------------------|------------|--------------------------|
| username                | none       | client5@isp1.com         |
| activate-service        | 2          | tiered(1280000, 5120000) |
| deactivate-service      |            | http(192.168.25.2, 80)   |
| service-timeout         | 2          | 720                      |
| service-stats           | 2          | 2                        |

**Configuring the HTTP Local Server to Support Guided Entrance**

JUNOS software supports an embedded Web server, known as the HTTP local server, which is used to support the Service Manager application's guided entrance service. With guided entrance, subscribers are directed to a specific Web site when they log in. At the Web site, the subscribers can then select the service they want to use.

You can configure one HTTP local server per virtual router. The HTTP local server is disabled by default. To configure the HTTP local server:

1. Access the virtual router context.

```
host1(config)#virtual-router west400
host1:west400(config)#
```

2. Create the HTTP local server.

```
host1:west400(config)#ip http
```

3. (Optional) Specify a standard IP access list that defines which subscribers can connect to the HTTP local server.

```
host1:west400(config)#ip http access-class chicagoList
```

4. (Optional) Specify the port on which the HTTP local server receives connection attempts.

```
host1:west400(config)#ip http port 8080
```

5. (Optional) Specify the maximum number of connections that can exist between one IP address and the HTTP local server.

```
host1:west400(config)#ip http same-host-limit 20
```

6. Specify the maximum time that HTTP local servers maintain connections.

```
host1:west40(config)#ip http max-connection-time 1000
```

7. Enable the HTTP local server.

```
host1:west40(config)#ip http server
```

8. Configure the HTTP redirect feature for the profile, interface, or subinterface that will be referenced in the guided entrance service definition.

```
host1:west40(config)#profile guidEnt6
host1:west40(config-profile)#ip http redirectUrl http://ispsite.redirect.com
```

### **HTTP Local Server Commands**

This section describes the commands used to configure the HTTP local server application on the E-series router.

#### **ip http**

- Use to create the HTTP local server.
- Example  
host1(config)#**ip http**
- Use the **no** version to delete the HTTP local server.

#### **ip http access-class**

- Use to allow only subscribers on the specified standard IP access list to connect to the HTTP local server.
- Example  
host1(config)#**ip http access-class chicagoList**
- Use the **no** version to remove the association between the access list and the HTTP local server.

#### **ip http max-connection-time**

- Use to specify the maximum time that the HTTP local server maintains an inactive connection.
- Specify a time in the range 3–7200 seconds, or 0. A value of 0 causes the server to maintain an inactive connection indefinitely.
- Example  
host1(config)#**ip http max-connection-time 1000**
- Use the **no** version to restore the default time, 30 seconds.



***ip http port***

- Use to specify the port on which the HTTP local server receives connection attempts.
- Specify a port number in the range 1–65535.
- Example  
host1(config)#**ip http port 8080**
- Use the **no** version to restore the default port number, 80.

***ip http redirectUrl***

- Use to specify the URL to which a subscriber's HTTP access session is redirected.
- The first access session is typically used by the Service Manager application to provide initial provisioning and service selection for the subscriber.
- HTTP redirect is per-interface; use the command in Profile Configuration mode for dynamic interfaces; use the command in Interface Configuration mode or Subinterface Configuration mode for static interfaces.
- The redirect URL can be a maximum of 64 characters.



**NOTE:** The HTTP local server must be configured and enabled in the virtual router for the interface on which you use the **ip http redirectUrl** command. Otherwise, the URL redirect operation will fail.

---

- Example  
host1(config-if)#**ip http redirectUrl http://ispsite.redirect.com**
- Use the **no** version to restore the default, which disables the HTTP redirect feature.

***ip http same-host-limit***

- Use to specify the maximum number of connections that can exist between one IP address and the HTTP local server.
- Specify a number in the range 0–1000.
- Example  
host1(config)#**ip http same-host-limit 20**
- Use the **no** version to restore the default number of allowed connections, 3.

***ip http server***

- Use to enable the HTTP local server.
- Example  
host1(config)#**ip http server**
- Use the **no** version to disable the HTTP local server

## Monitoring the HTTP Local Server

This section describes the **show ip http** commands for monitoring the HTTP local server. You can set a statistics baseline for the HTTP local server using the **baseline ip http** command. Use the **delta** keyword with the **show ip http statistics** command to display statistics with the baseline values subtracted.

### **baseline ip http**

- Use to set a baseline for HTTP server statistics.
- The system implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.
- Example  
host1#**baseline ip http**
- There is no **no** version.

### **show ip http scalar**

- Use to display HTTP local server information.
- Field descriptions
  - Maximum connection length—Maximum time that the HTTP local server maintains an inactive connection, in seconds
  - Current number of http servers—Number of configured Web servers
  - Number of enabled http servers—Number of Web servers enabled
  - Current number of http connections—Number of connections from subscribers to HTTP local servers
  - Peak number of http connections—Highest number of connections from subscribers to HTTP local servers
  - Maximum number of http connections—Maximum number of connections allowed from subscribers to HTTP local servers
- Example  
host1#**show ip http scalar**  
Maximum connection length: 1000 seconds  
Current number of http servers: 5  
Number of enabled http servers: 2  
Current number of http connections: 15  
Peak number of http connections: 125  
Maximum number of http connections: 1000

### **show ip http server**

- Use to display information about the HTTP local server.
- Field descriptions
  - Admin status—Status of the HTTP local server in the software: enabled or disabled
  - Access class—Name of a standard IP access list that determines which hosts can log on to the HTTP local server

- Listening port—Port that the HTTP local server uses to track requests for connection
- Same host limit—Maximum number of connections allowed between one IP address and the DHCP local server
- Example
 

```
host1#show ip http server
Admin status: enabled
Access class: not defined
Listening port: 80
Same host limit: 3
```

### **show ip http statistics**

- Use to display statistics about the connections to the HTTP local server.
- Field descriptions
  - Server enable count—Total number of enabled HTTP local servers
  - Server disable count—Total number of disabled HTTP local servers
  - Same host enforced—Number of connections dropped because the limit for connections from one IP address to the HTTP local server was exceeded
  - Access class denies—Number of connections dropped because of a problem with the standard IP access list that defines the hosts that can access the HTTP local server
  - No resource failures—Number of connections dropped because of system memory limitations
  - Http connections created—Total number of HTTP connections established
  - Http connections terminated—Total number of HTTP connections ended
  - Http connections aged out—Total number of HTTP connections that expired because they exceeded the maximum allowed connection time
  - Urls successfully served—Total number of Web pages displayed
  - Malformed http requests—Number of HTTP requests that failed because the format was incorrect
  - Urls not found—Number of Web pages not found
- Example
 

```
host1#show ip http statistics delta
Server enable count: 1
Server disable count: 0
Same host enforced: 0
Access class denies: 0
No resource failures: 0
Http connections created: 2
Http connections terminated: 2
Http connections aged out: 1
Urls successfully served: 0
Malformed http requests: 0
Urls not found: 0
```

**show profile**

- Use to display information about profiles. Use with the **name** keyword to display information about the redirect URL used for guided entrance services.
- To display information about a specific profile, use the **name** keyword.
- To display a list of profiles configured on the router, use the **brief** keyword.
- The following example is a partial **show profile** display that shows the HTTP local server's redirect configuration.
- Field descriptions
  - Ip http redirect Url—URL of the Web page used for Service Manager guided entrance services

## ■ Example

```
host1#show profile name guidedProfile2
Profile : guidedProfile2
.
.
.
Auto Detect : Disabled
Auto Configure : Disabled
IP FlowStats : Disabled
```

```
Ip http redirect Url : myredirect.html
```

## Monitoring Service Manager

---

Use the commands in this section to display information about the Service Manager application and subscriber service sessions. The **show** commands display information for RADIUS-created and CLI-created service sessions.

**show license service-management**

- Use to display whether the Service Manager license is enabled (set) or disabled (not set).
- Example

```
host1#show license service-management
service management license is set
```

**show profile**

- Use to display information about the policies and QoS configurations referenced in profiles.
- To display information about a specific profile, use the **name** keyword.
- To display a list of profiles configured on the router, use the **brief** keyword.
- Field descriptions
  - Input Policy—Name of input policy and whether statistics are enabled or disabled
  - Output Policy—Name of output policy and whether statistics are enabled or disabled

- qos-parameter—Name and value of the QoS parameter assigned to the profile
- qos-profile—Name of the QoS profile assigned to the profile

■ Example 1

```
host1#show profile name video
IP Output Policy : video statistics disabled
IP Secondary Input Policy : video statistics disabled
qos-parameter vidburst 1000
qos-parameter vidrate 500000
qos-profile vid512k
```

■ Example 2

```
host1#show profile name

IP Policy Parameter foo : 100000 increase, reference rate
IP Input Policy : p1 statistics disabled

ERX-00-16-c2#show profile name p2

IP Policy Parameter foo : 100000, reference rate
IP Input Policy : p1 statistics disabled
```

### **show qos-parameter**

- Use to display the parameters for QoS clients.
- Use the **references** keyword to display information about the QoS parameters attached to an interface or port type. If you do not specify the QoS profile name, attachment data for all QoS profiles is displayed.  
Optionally, use the **references** keyword with one of the following:
  - **interface**—Interface for which to display attachments and hierarchical parameter instances. Use one of the following to display statistics for the atm-vp or S-VLAN nodes and queues:
    - *atmVpi*—Virtual path identifier of the PVC
    - *s-vlanIdValue*—S-VLAN ID number
  - **l2tp session**—Name of L2TP session
  - **tunnel-server**—Name of the interface at the root of the scheduler hierarchy located on the tunnel-service interface or at the same hierarchy for LNS GRE tunnel traffic.
- Use the **full** keyword to display information in expanded format, including Service Manager references.
- Field descriptions
  - interface—Location of the interface to which the parameter instance is assigned; global indicates that the parameter is assigned to the chassis
  - parameter name—Name of the parameter instance
  - value—Value assigned to the parameter instance

- source—Source of the parameter instance
  - dcm—Parameter instance was created in a profile
  - radius—Parameter instance was created through RADIUS
  - service manager—Parameter instance was created through Service Manager
  - default—Parameter instance was created through the CLI or SNMP
- service manager refs—Number of references of this parameter instance created through Service Manager
- persistence—Status of the persistence of a parameter instance in the system
  - persistent—Parameter instance is stored in NVS and is restored after a chassis reset
  - non-persistent—Parameter instance is not stored in NVS and are deleted after a chassis reset
- Global parameter instances—Number of parameter instances assigned to the chassis
- Parameter instances reported—Total number of parameter instances assigned
- Explicit parameter instances—Total number of explicit parameter instances assigned
- Hierarchical parameter instances—Total number of hierarchical parameter instances assigned
- IP multicast parameter instances—Total number of parameter instances associated with the IP multicast bandwidth adjustment application
- Example

```
host1#show qos-parameter video references full
```

| interface          | parameter<br>name | value | source  | service<br>manager<br>refs | persistence |
|--------------------|-------------------|-------|---------|----------------------------|-------------|
| GigabitEthernet6/0 | video             | 50    | default | none                       | persistent  |

```
Global parameter instances: 0
Parameter instances reported: 1
```

**show service-management service-definition**

- Use to display information about the service definitions configured on your router.
- Specify the name of a service definition macro file, including the .mac extension, to display information for the particular service definition.
- Use the **brief** keyword without a macro file name to display summary information for all service definitions.
- Field descriptions
  - Filename—Name of the service definition macro file
  - Service—Name of the service, with the parameter specifications in parentheses
  - Installed—Status of definition; True = installed, False = not installed
  - Reference Count—Number of times the service definition has been used to instantiate a unique service instance (which identifies the policy, QoS, and profile objects for a service). For example, if one service session—such as, `tiered(40000,40000)`—is activated by multiple subscribers, the reference count is 1. However, if one subscriber activates `tiered(40000,40000)` and another subscriber activates `tiered(75000,75000)`—the reference count is 2.
  - Timestamp—Day, date, and time the service definition was copied to NVS.

## ■ Example 1

```
host1#show service-management service-definition brief
Service Definitions

```

| Filename   | Service                   | Installed | Reference Count |
|------------|---------------------------|-----------|-----------------|
| video.mac  | video(inputbw, outputbw)  | True      | 0               |
| tiered.mac | tiered(inputbw, outputbw) | True      | 0               |

```

Filename Timestamp

video.mac TUE NOV 15 15:22:00 2005
tiered.mac WED DEC 14 14:41:20 2005
```

## ■ Example 2

```
host1#show service-management service-definition tiered.mac
tiered.mac - WED DEC 14 14:41:20 2005
Installed: True
Service: tiered(inputbw, outputbw)
Reference Count: 0
```

**show service-management service-session-profile**

- Use to display information about service session profiles configured on your router.
- Specify the name of a particular service session profile or use the **brief** keyword to display summary information for all service session profiles.
- Field descriptions
  - Name—Name of the service session profile
  - Volume—Volume threshold, in MB, for the service session
  - Time—Time threshold, in seconds, for the service session
  - Statistics—Type of statistics that are captured; Disabled (none), Time, Volume-Time, or Time and Volume
- Example 1

```
host1#show service-management service-session-profile brief
Service Session Profiles

```

| Name    | Volume | Time | Statistics  |
|---------|--------|------|-------------|
| tiered1 | 20000  | 1000 | Volume-Time |
| tiered2 | 20000  | 1000 | Time        |
| video1  | 15000  | 1000 | Volume-Time |
| video4  | 0      | 0    | Disabled    |

- Example 2
- ```
host1#show service-management service-session-profile tiered1
tiered1
Time      : 1000
Volume    : 20000
Statistics : Time and Volume
```

show service-management owner-session

- Use to display information about active subscriber sessions, by owner.
- Specify an owner's name to display information for that particular owner.
- Use the **brief** keyword to display summary information for all active owner sessions.
- Field descriptions
 - Name—Name of the subscriber or name of the service session
 - Interface—Type and IP address of the subscriber's interface
 - Owner/Id—Method used to activate the subscriber session (CLI, AAA) and ID number generated by the owner
 - State—Status of the subscriber session (active or inactive), or status of the service session
 - Non-volatile—Indicates whether the service session is stored in NVS; RADIUS-based service sessions are not stored in NVS
 - Service Sessions—Number of service sessions currently active for this subscriber
 - Operation—Last operation that Service Manager performed

- Service—Name of the service, with parameter values in parentheses
- Activate—Indicates whether the last operation was activate (True) or deactivate (False)
- Statistics Type—Type of statistics collected; none, time, or volume-time
- Statistics Complete—Whether statistics have been successfully collected; True or False
- Poll Interval—Interval, in seconds, that interim statistics reports are sent
- Poll Expire—Number of seconds until the next statistics report is sent
- Activate Time—Day, date, and time when the service session was activated
- Time—Time threshold value set by service session profile or RADIUS VSA
- Time Expire—Time left until the threshold expires; this value starts as the time threshold value and is decremented as time passes
- Volume—Volume threshold value set by service session profile or RADIUS VSA
- Volume Expire—Volume left until the threshold is exceeded; this value starts as the volume threshold value and is decremented as the service statistics measure volume
- Input Bytes—Current value of input bytes that the statistics configuration is measuring
- Output Bytes—Current value of output bytes that the statistics configuration is measuring
- Input Packets—Current value of input packets that the statistics configuration is measuring
- Output Packets—Current value of output packets that the statistics configuration is measuring
- Example 1

host1#show service-management owner-session brief
Subscriber Sessions

Name	Interface	Id	Owner/Id	State	Non-volatile	Service Sessions
CLIENT1@ISP.COM	ip192.168.0.3	1	AAA 4194326	Active	False	1
CLIENT2@ISP.COM	ip192.168.0.7	2	AAA 4194327	Active	False	1
CLIENT3@ISP.COM	ip192.168.0.4	3	AAA 4194328	Active	False	1
CLIENT4@ISP.COM	ip192.168.0.5	4	AAA 4194329	Active	False	1
CLIENT5@ISP.COM	ip192.168.0.6	5	AAA 4194330	Active	False	1
CLIENT6@ISP.COM	ip192.168.0.8	6	AAA 4194331	Active	False	1
CLIENT7@ISP.COM	ip192.168.0.1	7	AAA 4194332	Active	False	1
CLIENT8@ISP.COM	ip192.168.0.9	8	AAA 4194333	Active	False	1

■ Example 2

```

host1#show service-management owner-session aaa 4194326
User Name: CLIENT1@ISP.COM, Interface: ip 192.168.0.1
Owner/Id: AAA/4194326
Non-volatile: False
State: Active
ServiceSessions:
      Name                Owner/ID      State                Operation
-----
tiered(2000000,3000000)  AAA 4194326  Config ApplySuccess  Activate
      Name                Non-volatile
-----
tiered(2000000,3000000)  False

```

■ Example 3

```

host1#show service-management owner-session aaa 4194326 service-session
User Name: client1@isp.COM, Interface: ip192.168.0.1
Service : tiered(2000000,3000000)
Non-volatile : False
Owner : AAA 4194326
State : Config ApplySuccess
Activate : True
Statistics Type : time-based and volume-based
Statistics Complete : False
Poll Interval : 0
Poll Expire : 0
Activate Time : THU MAR 02 01:21:26 2006
Time : 0
Time Expire : 0
Volume MBytes: 2
Volume Expire MBytes : 1
Input Bytes : 594
Output Bytes : 1196
Input Packets : 1
Output Packets : 2

```

show service-management subscriber-session

- Use to display information about active subscriber sessions on your router.
- Specify a subscriber's name to display information for that particular subscriber.
- Use the **brief** keyword to display summary information for all active subscriber sessions.
- Field descriptions
 - Name—Name of the subscriber or name of the service session
 - Interface—Type and IP address of the subscriber's interface
 - Id—ID number of the subscriber session
 - mutex—Index number of the mutex group to which the service session belongs
 - Owner/Id—Method used to activate the subscriber session (CLI, AAA) and ID number generated by the owner (Acct-Session-ID for AAA)
 - State—Status of the subscriber session (active or inactive), or status of the service session

- Non-volatile—Indicates whether the service session is stored in NVS; RADIUS-based service sessions are not stored in NVS
- Service Sessions—Number of service sessions currently active for this subscriber
- Operation—Last operation that Service Manager performed
- Service—Name of the service, with parameter values in parentheses
- Activate—Indicates whether the last operation was activate (True) or deactivate (False)
- Statistics Type—Type of statistics collected; none, time, or volume-time
- Statistics Complete—Whether statistics have been successfully collected; True or False
- Poll Interval—Interval, in seconds, that interim statistics reports are sent
- Poll Expire—Number of seconds until the next statistics report is sent
- Activate Time—Day, date, and time when the service session was activated
- Time—Time threshold value set by service session profile or RADIUS VSA
- Time Expire—Time left until the threshold expires; this value starts as the time threshold value and is decremented as time passes
- Volume—Volume threshold value set by service session profile or RADIUS VSA
- Volume Expire—Volume left until the threshold is exceeded; this value starts as the volume threshold value and is decremented as the service statistics measure volume
- Input Bytes—Current value of input bytes that the statistics configuration is measuring
- Output Bytes—Current value of output bytes that the statistics configuration is measuring
- Input Packets—Current value of input packets that the statistics configuration is measuring
- Output Packets—Current value of output packets that the statistics configuration is measuring

■ Example 1

```
host1#show service-management subscriber-session brief
Subscriber Sessions
```

Name	Interface	Id	Owner/Id	State	Non-volatile	Service Sessions
CLIENT1@ISP.COM	ip192.168.0.3	1	AAA 4194326	Active	False	1
CLIENT2@ISP.COM	ip192.168.0.7	2	AAA 4194327	Active	False	1
CLIENT3@ISP.COM	ip192.168.0.4	3	AAA 4194328	Active	False	1
CLIENT4@ISP.COM	ip192.168.0.5	4	AAA 4194329	Active	False	1
CLIENT5@ISP.COM	ip192.168.0.6	5	AAA 4194330	Active	False	1
CLIENT6@ISP.COM	ip192.168.0.8	6	AAA 4194331	Active	False	1
CLIENT7@ISP.COM	ip192.168.0.1	7	AAA 4194332	Active	False	1
CLIENT8@ISP.COM	ip192.168.0.9	8	AAA 4194333	Active	False	1
CLIENT9@ISP.COM	ip192.168.0.2	9	AAA 4194334	Active	False	1
CLIENT10@ISP.COM	ip192.168.0.10	10	AAA 4194335	Active	False	1

■ Example 2

host1#show service-management subscriber-session client1@isp.com interface ip 192.168.0.1

User Name: CLIENT1@ISP.COM, Interface: ip 192.168.0.1

Id: 1

Owner: AAA 4194326

Non-volatile: False

State: Active

ServiceSessions:

Name	mutex	Owner/Id	State	Operation
tiered(2000000,3000000)		AAA 4194326	ConfigApplySuccess	Activate
Name	Non-volatile			
tiered(2000000,3000000)	False			

■ Example 3

host1#show service-management subscriber-session client1@isp.COM interface ip 192.168.0.1 service-session tiered

User Name: client1@isp.COM, Interface: ip192.168.0.1

Service : tiered(2000000,3000000)

Non-volatile : False

Owner : AAA 41943236

State : Config ApplySuccess

Activate : True

Statistics Type : time-based and volume-based

Statistics Complete : False

Poll Interval : 0

Poll Expire : 0

Activate Time : THU MAR 02 01:21:26 2006

Time : 0

Time Expire : 0

Volume MBytes: 2

Volume Expire MBytes : 1

Input Bytes : 594

Output Bytes : 1196

Input Packets : 1

Output Packets : 2

■ Example 4

host1#show service-management subscriber-session 20

User Name: CLIENT50@ISP.COM, Interface: ip192.168.100.33

Id: 20

Owner/Id: CLI

Non-volatile: True

State: Active

ServiceSessions:

Name	mutex	Owner	State	Operation
internet(5000,8000)	12	CLI	Config ApplySuccess	Activate
Name	Non-volatile			
internet(5000,8000)	True			

show service-management summary

- Use to display summary information about subscriber and service sessions configured on your router.
- Field descriptions
 - Total Subscriber Sessions—Number of active subscriber sessions on the router
 - Total Service Sessions—Number of active service sessions on the router
- Example

```
host1#show service-management summary
```

```
Total Subscriber Sessions : 10
```

```
Total Service Sessions : 10
```


Appendix A

RADIUS Attribute Descriptions

This appendix lists the RADIUS attributes that are supported by JUNOS software. [Table 50](#) describes the supported RADIUS IETF attributes. [Table 51](#) describes the supported Juniper Networks vendor-specific attributes (VSAs). [Table 52](#) describes the DSL Forum VSA formats supported by JUNOS software. [Table 53](#) describes RADIUS attributes that are simply passed to their destination by the router.

RADIUS attributes are discussed in the following sections:

- [RADIUS IETF Attributes](#) on page 512
- [Juniper Networks VSAs](#) on page 517
- [DSL Forum VSAs](#) on page 523
- [Pass Through RADIUS Attributes](#) on page 524
- [References](#) on page 525

RADIUS IETF Attributes

[Table 50](#) describes the RADIUS IETF attributes supported by JUNOS software. The attributes are sorted by standard number.

Table 50: RADIUS IETF Attributes Supported by JUNOS Software

Attribute Number	Attribute Name	Description
[1]	User-Name	<ul style="list-style-type: none"> ■ Name of user to be authenticated ■ Configurable username override
[2]	User-Password	<ul style="list-style-type: none"> ■ Password of user to be authenticated ■ Configurable password override ■ Password Authentication Protocol (PAP)
[3]	CHAP-Password	Response value provided by a Point-to-Point Protocol (PPP) Challenge Handshake Authorization Protocol (CHAP) user in the response to an access challenge
[4]	NAS-IP-Address	<ul style="list-style-type: none"> ■ IP address of the network access server (NAS) that is requesting authentication of the user ■ You can use the radius update-source-addr command to override this behavior; see Chapter 1, Configuring Remote Access.
[5]	NAS-Port	<ul style="list-style-type: none"> ■ Physical port number of the NAS that is authenticating the user ■ See the radius nas-port-format, radius pppoe nas-port-format unique, and radius vlan nas-port-format stacked commands in Chapter 2, Configuring RADIUS Attributes.
[6]	Service-Type	<ul style="list-style-type: none"> ■ Type of service the user has requested or the type of service to be provided ■ Admin, Login, NAS Prompt, or Framed only
[7]	Framed-Protocol	<ul style="list-style-type: none"> ■ Framing protocol used for framed access ■ Standard value of 1 set for PPP ■ Nonstandard value of 1008 set for dynamic ATM
[8]	Framed-IP-Address	<ul style="list-style-type: none"> ■ IP address to be configured for the user ■ 0.0.0.0 or absence is interpreted as 255.255.255.254 ■ See the radius include framed-ip-add acct-start command in Chapter 2, Configuring RADIUS Attributes.
[9]	Framed-IP-Netmask	<ul style="list-style-type: none"> ■ IP network to be configured for the user when the user is a router to a network ■ Absence implies 255.255.255.255
[11]	Filter-Id	<ul style="list-style-type: none"> ■ Name of the filter list for the user ■ Interpreted as input policy name
[12]	Framed-MTU	<ul style="list-style-type: none"> ■ The maximum transmission unit to be configured for the user, when it is not negotiated by some other means (such as PPP). ■ When sent in an Access-Request with an EAP-Message, indicates the maximum size of the EAP-Message string that the external server supports.
[13]	Framed-Compression	Always set to none.
[18]	Reply-Message	<ul style="list-style-type: none"> ■ Text that may be displayed to the user ■ Only the first instance of this attribute is used

Table 50: RADIUS IETF Attributes Supported by JUNOS Software (continued)

Attribute Number	Attribute Name	Description
[22]	Framed-Route	String that provides routing information to be configured for the user on the NAS; in the format: < addr > [/ < maskLen >] [< nexthop > [< cost >]] [tag < tagValue >] [distance < distValue >]
[24]	State	<ul style="list-style-type: none"> ■ An arbitrary value that the router includes in new Access-Request packets from the previous Accept-Challenge ■ Applicable for CLI, telnet, or EAP message exchange
[25]	Class	An arbitrary value that the NAS includes in all accounting packets for the user if supplied by the RADIUS server
[26]	Vendor-Specific	Juniper Networks Enterprise number 0x0000130A
[27]	Session-Timeout	Maximum number of consecutive seconds of service to be provided to the user before termination of the session
[28]	Idle-Timeout	Maximum number of consecutive seconds of idle connection provided to the user before termination of the session
[30]	Called-Station-Id	<ul style="list-style-type: none"> ■ Allows the NAS to send the phone number that the user called ■ Not supported for nontunneled or LAC session side ■ For the LNS, the format is the string passed in the Called Number AVP ■ For RADIUS relay server, indicates the subscriber's wireless access point
[31]	Calling-Station-Id	<ul style="list-style-type: none"> ■ Allows the NAS to send the phone number from which the call originated ■ See the radius calling-station-format and the radius calling-station-delimiter commands in Chapter 2, Configuring RADIUS Attributes. ■ For RADIUS relay server, indicates the subscriber's MAC address
[32]	NAS-Identifier	<ul style="list-style-type: none"> ■ Identifies the NAS originating the request ■ System-wide configurable hostname or VR-sensitive configurable NAS-identifier name
[33]	Proxy-State	E-series router's port ID and IP address
[40]	Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (Start), the end (Stop), or the interim (Interim-Update)
[41]	Acct-Delay-Time	Indicates how many seconds the client has been trying to send a particular record
[42]	Acct-Input-Octets	<ul style="list-style-type: none"> ■ Indicates how many octets have been received from the port during the time this service has been provided ■ IP subscriber manager—Statistics are reported ■ PPP—Statistics are counted according to the rules of the generic interface MIB
[43]	Acct-Output-Octets	<ul style="list-style-type: none"> ■ Indicates how many octets have been sent to the port during the time this service has been provided ■ IP subscriber manager—Statistics are reported ■ PPP—Statistics are counted according to the rules of the generic interface MIB

Table 50: RADIUS IETF Attributes Supported by JUNOS Software (continued)

Attribute Number	Attribute Name	Description
[44]	Acct-Session-Id	<ul style="list-style-type: none"> ■ Unique accounting identifier that makes it easy to match start and stop records in a log file ■ See the radius acct-session-id-format and the radius include acct-session-id access-request commands in Chapter 2, Configuring RADIUS Attributes.
[45]	Acct-Authentic	<ul style="list-style-type: none"> ■ Indicates how the user was authenticated: whether by RADIUS, the NAS itself, or another remote authentication protocol ■ Always 1
[46]	Acct-Session-Time	Indicates how long in seconds that the user has received service
[47]	Acct-Input-Packets	<ul style="list-style-type: none"> ■ Indicates how many packets have been received from the port during the time this service has been provided to a framed user ■ IP subscriber manager—Statistics are reported ■ PPP—Statistics are counted according to the rules of the generic interface MIB
[48]	Acct-Output-Packets	<ul style="list-style-type: none"> ■ Indicates how many packets have been sent to the port in the course of delivering this service to a framed user ■ IP subscriber manager—Statistics are reported ■ PPP—Statistics are counted according to the rules of the generic interface MIB
[49]	Acct-Terminate-Cause	<p>Contains the reason the service (a PPP session) was terminated. The service can be terminated for the following reasons:</p> <ul style="list-style-type: none"> ■ User Request (1)—User initiated the disconnect (log out) ■ Idle Timeout (4)—Idle timer has expired ■ Session Timeout (5)—Client reached the maximum continuous time allowed on the service or session ■ Admin Reset (6)—System administrator terminated the session ■ Port Error (8)—PVC failed; no hardware or no interface ■ NAS Error (9)—Negotiation failures, connection failures, or address lease expiration ■ NAS Request (10)—PPP challenge timeout, PPP request timeout, tunnel establishment failure, PPP bundle failure, IP address lease expiration, PPP keep-alive failure, Tunnel disconnect, or an unaccounted-for error
[50]	Acct-Multi-Session-ID	<ul style="list-style-type: none"> ■ String constructed from the Acct-Session-ID of the first PPP link established for the Multilink PPP bundle and the internal Multilink PPP bundle ID. ■ This string is the hexadecimal ASCII characters for two 4-octet unsigned integers. Example: 0a34331200001249.
[51]	Acct-Link-Count	A value that increments with each link that joins the MLPPP bundle. This attribute does not indicate the number of active links. For more details, see RFC 2866—RADIUS Accounting (June 2000) .
[52]	Acct-Input-Gigawords	<ul style="list-style-type: none"> ■ Indicates how many times the Acct-Input-Octets counter has wrapped around 2³² during the time this service has been provided, and can be present in Accounting-Request records only where the Acct-Status-Type is set to Stop or Interim-Update ■ IP subscriber manager—Statistics are reported ■ PPP—Statistics are counted according to the rules of the generic interface MIB

Table 50: RADIUS IETF Attributes Supported by JUNOS Software (continued)

Attribute Number	Attribute Name	Description
[53]	Acct-Output-Gigawords	<ul style="list-style-type: none"> ■ Indicates how many times the Acct-Output-Octets counter has wrapped around 2^{32} in the course of delivering this service, and can be present in Accounting-Request records only where the Acct-Status-Type is set to Stop or Interim-Update ■ IP subscriber manager—Statistics are reported ■ PPP—Statistics are counted according to the rules of the generic interface MIB
[55]	Event-Timestamp	Records the time that this event occurred on the NAS, in seconds, since January 1, 1970 00:00 UTC
[60]	CHAP-Challenge	Contains the CHAP challenge sent by the NAS to a PPP CHAP user
[61]	NAS-Port-Type	<ul style="list-style-type: none"> ■ Indicates the type of physical port the NAS is using to authenticate the user ■ See the radius dsl-port-type and the radius ethernet-port-type commands in Chapter 2, Configuring RADIUS Attributes.
[62]	Port-Limit	Specifies the maximum number of MLPPP member links allowed for the subscriber
[64]	Tunnel-Type	<ul style="list-style-type: none"> ■ Which tunneling protocol to use (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator) ■ Only L2TP tunnels supported at this time
[65]	Tunnel-Medium-Type	<ul style="list-style-type: none"> ■ Transport medium to use when creating a tunnel for those protocols (such as L2TP) that can operate over multiple transports ■ Only IPv4 supported at this time
[66]	Tunnel-Client-Endpoint	Address of the initiator end of the tunnel
[67]	Tunnel-Server-Endpoint	Address of the server end of the tunnel
[68]	Acct-Tunnel-Connection	<ul style="list-style-type: none"> ■ Indicates the identifier assigned to the tunnel session ■ Value is L2TP call-serial number
[69]	Tunnel-Password	Password to be used to authenticate to a remote server
[77]	Connect-Info	Sent from the NAS to indicate the nature of the user's connection
[79]	EAP-Message	Encapsulates EAP packets, which allows the NAS to authenticate users through EAP without having to understand the EAP protocol
[80]	Message-Authenticator	Must be used in any Access-Request, Access-Accept, Access-Reject or Access-Challenge messages that include EAP-Message attributes
[82]	Tunnel-Assignment-Id	Indicates to the tunnel initiator the particular tunnel to which a session is to be assigned
[83]	Tunnel-Preference	<ul style="list-style-type: none"> ■ 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. ■ Included in the Tunnel-Link-Start, the Tunnel-Link-Reject, and the Tunnel-Link-Stop packets (LAC only)
[85]	Acct-Interim-Interval	Number of seconds between each interim accounting update for this session
[86]	Acct-Tunnel-Packets-Lost	Number of packets lost on a given link

Table 50: RADIUS IETF Attributes Supported by JUNOS Software (continued)

Attribute Number	Attribute Name	Description
[87]	NAS-Port-Id	<ul style="list-style-type: none"> ■ Text string that identifies the physical interface of the NAS that is authenticating the user ■ If the PPP user connects via ATM slot 12, port 2, subinterface 3, vpi 100, vci 101, then the NAS-Port-Id value in the RADIUS packets will be atm 12/2.3:100.101 ■ If the user is a PPP user that started as a result of the E-series LNS feature (that is, no physical port), then the NAS-Port-Id value is as follows: <i>media:local address:peer address:local tunnel id:peer tunnel id:local session id:peer session id:call serial number</i> <ul style="list-style-type: none"> ■ For example: ip:172.81.1.98:172.81.1.99:18d:cb8:ce6:9f4:6 ■ In this case, the local information refers to the LNS, and the peer information refers to the LAC ■ NAS-Port-Id usually contains one of the following: <ul style="list-style-type: none"> ■ atm < slot > / < port > < .subinterface > : < vpi > . < vci > ■ FastEthernet < slot > / < port > < .subinterface > [: < vlan >] ■ GigabitEthernet < slot > / < port > < .subinterface > [: < vlan >] ■ serial < slot > / < port > [: < sonetPath > [/ < sonetTributary (x/x/x) > [/ < fractionalInterface >]]] ■ from LNS—ip:local ip:peer ip:local tid:peer tid:local sid:peer sid:call serial number <p>tid—tunnel id sid—session id</p> <p>NOTE: Releases before 4.0.0 did not pass the subinterface number to RADIUS for inclusion in the NAS-Port-Id. If you do not want the subinterface number to be included, you must enter the aaa intf-desc-format include sub-intf disable command to omit the subinterface.</p>
[88]	Framed-Pool	Name of an assigned address pool that should be used to assign an address for the user
[90]	Tunnel-Client-Auth-Id	Name used by the tunnel initiator during the authentication phase of tunnel establishment
[91]	Tunnel-Server-Auth-Id	Name used by the tunnel terminator during the authentication phase of tunnel establishment
[96]	Framed-Interface-Id	IPv6 interface identifier configured by the user
[97]	Framed-Ipv6-Prefix	IPv6 prefix and corresponding route configured by the user
[99]	Framed-Ipv6-Route	Provides routing information to be configured for the user on the NAS
[101]	Error-Cause	4-octet field that contains an integer that specifies the cause of the error
[135]	Ascend-Primary-DNS	<ul style="list-style-type: none"> ■ Indicates the IP address of the primary DNS ■ The format is 1 byte of type (135), 1 byte of length (length = 6), 4 bytes of value (IPv4 address)
[136]	Ascend-Secondary-DNS	<ul style="list-style-type: none"> ■ Indicates the IP address of the secondary DNS ■ The format is 1 byte of type (136), 1 byte of length (length = 6), 4 bytes of value (IPv4 address)
[188]	Ascend-Num-In-Multilink	Current number of links in a multilink bundle
[242]	Ascend-Data-Filter	RADIUS policy definitions used to configure a policy to classify packet flows and perform filter, forward, packet marking, rate-limit profile, and traffic class actions

Juniper Networks VSAs

Table 51 lists Juniper Networks VSA formats for RADIUS. JUNOS software uses the vendor ID assigned to Juniper Networks (vendor ID 4874) by the Internet Assigned Numbers Authority (IANA).

Table 51: Juniper Networks (Vendor ID 4874) VSA Formats

Attribute Number	Attribute Name	Description	Length	Subtype Length	Value
[26-1]	Virtual-Router	<ul style="list-style-type: none"> Virtual router name for the Broadband Remote Access Server (B-RAS) user's IP interface. Allowed only from RADIUS server in default virtual router context. For restricted users, specifies the only virtual router that the user can access. For nonrestricted users, specifies the initial virtual router that the user accesses. See the enable command in JUNOS System Basics Configuration Guide, Chapter 8, Passwords and Security. 	len	sublen	string: virtual-router-name
[26-2]	Local-Address-Pool	<ul style="list-style-type: none"> Name of an assigned address pool that should be used to assign an address for the user Same as RADIUS attribute 88, Framed-Pool 	len	sublen	string: address-pool-name
[26-3]	Local-Interface	Interface to apply to the E-series side of the connection	len	sublen	string: local-interface
[26-4]	Primary-DNS	<ul style="list-style-type: none"> B-RAS user's DNS address negotiated during IPCP 4-octet IP address 	12	6	integer: 4-byte primary-dns-address
[26-5]	Secondary-DNS	<ul style="list-style-type: none"> B-RAS user's DNS address negotiated during IPCP 4-octet IP address 	12	6	integer: 4-byte secondary-dns-address
[26-6]	Primary-WINS (NBNS)	<ul style="list-style-type: none"> B-RAS user's WINS (NBNS) address negotiated during IPCP 4-octet IP address 	12	6	integer: 4-byte primary-wins-address
[26-7]	Secondary-WINS (NBNS)	<ul style="list-style-type: none"> B-RAS user's WINS (NBNS) address negotiated during IPCP 4-octet IP address 	12	6	integer: 4-byte secondary-wins-address
[26-8]	Tunnel-Virtual-Router	Virtual router name for tunnel connection	len	sublen	string: tunnel-virtual-router
[26-9]	Tunnel-Password	Tunnel password in cleartext	len	sublen	string: tunnel-password
[26-10]	Ingress-Policy-Name	Input policy name to apply to B-RAS user's interface	len	sublen	string: input-policy-name
[26-11]	Egress-Policy-Name	Output policy name to apply to B-RAS user's interface	len	sublen	string: output-policy-name

Table 51: Juniper Networks (Vendor ID 4874) VSA Formats (continued)

Attribute Number	Attribute Name	Description	Length	Subtype Length	Value
[26-12]	Ingress-Statistics	Enable or disable input statistics on B-RAS user's interface	12	6	integer: 0 = disable, 1 = enable
[26-13]	Egress-Statistics	Enable or disable output statistics on B-RAS user's interface	12	6	integer: 0 = disable, 1 = enable
[26-14]	Service-Category	ATM service category to apply to B-RAS user's interface	12	6	integer: 1 = UBR, 2 = UBR PCR, 3 = NRT VBR, 4 = CBR, 5 = RT VBR,
[26-15]	PCR	<ul style="list-style-type: none"> ■ Peak cell rate ■ 4-octet integer 	12	6	integer: 4-octet
[26-16]	SCR	<ul style="list-style-type: none"> ■ Sustained cell rate ■ 4-octet integer 	12	6	integer: 4-octet
[26-17]	Mbs	<ul style="list-style-type: none"> ■ Maximum burst rate ■ 4-octet integer 	12	6	integer: 4-octet
[26-18]	Init-CLI-Access-Level	<ul style="list-style-type: none"> ■ Specifies the initial level of access to CLI commands ■ See the enable command in JUNOS System Basics Configuration Guide, Chapter 8, Passwords and Security. 	len	sublen	single attribute: enter 0, 1, 5, 10, or 15
[26-19]	Allow-All-VR-Access	<ul style="list-style-type: none"> ■ Specifies user access to all virtual routers ■ See the enable command in JUNOS System Basics Configuration Guide, Chapter 8, Passwords and Security. 	len	sublen	integer: 0 = disable, 1 = enable
[26-20]	Alt-CLI-Access-Level	<ul style="list-style-type: none"> ■ Specifies other levels of access to CLI commands ■ See the enable command in JUNOS System Basics Configuration Guide, Chapter 8, Passwords and Security. 	len	sublen	single attribute; enter 0, 1, 5, 10, or 15
[26-21]	Alt-CLI-Vrouter-Name	<ul style="list-style-type: none"> ■ For restricted users, specifies other VRs that the user may access. ■ See the enable command in JUNOS System Basics Configuration Guide, Chapter 8, Passwords and Security. 	len	sublen	string: virtual-router-name
[26-22]	Sa-Validate	<ul style="list-style-type: none"> ■ Enable or disable source address validation on a user's interface ■ 4-octet integer 	len	sublen	integer: 0 = disable, 1 = enable
[26-23]	Igmp-Enable	<ul style="list-style-type: none"> ■ Enable or disable IGMP on a user's interface ■ Allows the end user to register for the reception of multicast services ■ 4-octet integer 	len	sublen	integer: 0 = disable, 1 = enable
[26-24]	Pppoe-Description	The string <i>pppoe <mac addr></i> sent to the RADIUS server supplied by PPPoE	len	sublen	string: pppoe <mac addr>

Table 51: Juniper Networks (Vendor ID 4874) VSA Formats (continued)

Attribute Number	Attribute Name	Description	Length	Subtype Length	Value
[26-25]	Redirect-Vrouter-Name	<ul style="list-style-type: none"> Virtual router name indicating the VR context in which to authenticate the user Behavior is similar to that of a remote domain-map lookup. 	len	sublen	authentication-redirection
[26-26]	QoS-Profile-Name	Name of the QoS profile to attach to the user's interface	len	sublen	string: qos-profile-name
[26-28]	Pppoe-Url	PPPoE URL that is passed to PPPoE subscribers	len	sublen	string:URL
[26-30]	Tunnel-Nas-Port-Method	Conveys nasPort and nasPort type in tunnel	12	6	4-octet integer: 0 = none, 1 = Cisco CLID
[26-31]	Service-Bundle	Specifies the SDX service bundle	len	sublen	string
[26-33]	Tunnel-Max-Sessions	Maximum number of sessions allowed in a tunnel	12	6	integer: 4-octet
[26-34]	Framed-Ip-Route-Tag	Route tag to apply to returned framed-ip-address	12	6	integer: 4-octet
[26-35]	Tunnel-Dialout-Number	Dial number in L2TP dial-out	len	sublen	string:dial-out-number
[26-36]	PPP-Username	Username used in PPP L2TP dial-out sessions at the LNS for L2TP dial-out	len	sublen	string: ppp-username
[26-37]	PPP-Password	Password used in PPP L2TP dial-out sessions at the LNS for L2TP dial-out	len	sublen	string: ppp-password
[26-38]	PPP-Protocol	PPP authentication protocol used for L2TP dial-out sessions at the LNS	12	6	integer: 0 = none; 1 = PAP; 2 = CHAP; 3 = PAP-CHAP; 4 = CHAP-PAP
[26-39]	Tunnel-Min-Bps	Minimum line speed for L2TP dial-out	12	6	integer
[26-40]	Tunnel-Max-Bps	Maximum line speed for L2TP dial-out	12	6	integer
[26-41]	Tunnel-Bearer-Type	Bearer capability required for L2TP dial-out	12	6	integer: 0 = none; 1 = analog; 2 = digital
[26-42]	Input-GigaPkts	Number of times input-packets attribute rolls over its 4-octet field	12	6	integer
[26-43]	Output-GigaPkts	Number of times output-packets attribute rolls over its 4-octet field	12	6	integer
[26-44]	Tunnel-Interface-Id	Tunnel interface selector that AAA caches as part of the tunnel-session profile and the user's profile. This attribute is available to the RADIUS authentication and accounting servers.	len	sublen	string: tunnel selector
[26-45]	Ipv6-Virtual-Router	Virtual router name for B-RAS user's IPv6 interface	len	sublen	string: virtual-router-name
[26-46]	Ipv6-Local-Interface	Local IPv6 interface to apply to the E-series side of the connection	len	sublen	string: ipv6-local-interface
[26-47]	Ipv6-Primary-DNS	B-RAS user's primary IPv6 DNS address negotiated by DHCP	len	sublen	hexadecimal string: ipv6-primary-dns-address

Table 51: Juniper Networks (Vendor ID 4874) VSA Formats (continued)

Attribute Number	Attribute Name	Description	Length	Subtype Length	Value
[26-48]	Ipv6-Secondary-DNS	B-RAS user's secondary IPv6 DNS address negotiated by DHCP	len	sublen	hexadecimal string: ipv6-primary-dns-address
[26-51]	Disconnect-Cause	L2TP PPP disconnect cause information received by the LAC	len	sublen	string:l2tp-ppp-disconnect-cause
[26-52]	Radius-Client-Address	RADIUS relay server's IP address	12	6	integer:4-octet
[26-53]	Service-Description	AAA profile service description string	len	sublen	string:profile-service-description
[26-54]	L2tp-Recv-Window-Size	<ul style="list-style-type: none"> ■ L2TP receive window size (RWS) for a tunnel on the LAC ■ Number of packets that the peer can transmit without receiving an acknowledgment from the router ■ 4-octet integer 	12	6	integer:4-octet
[26-55]	DHCP-Options	Client's DHCP options	len	sublen	string:dhcp-options
[26-56]	DHCP-MAC-Address	Client's MAC address	len	sublen	string:mac-address
[26-57]	DHCP-GI-Address	DHCP relay agent's IP address	12	6	integer:4-octet
[26-58]	LI-Action	Packet mirroring action	len	sublen	Salt encrypted integer: 0 = stop monitoring; 1 = start monitoring; 2 = no action
[26-59]	Med-Dev-Handle	Link to which packet mirroring is applied	len	sublen	Salt encrypted string; contains an ASCII-encoded unsigned integer
[26-60]	Med-Ip-Address	IP address of analyzer device to which mirrored packets are forwarded	len	sublen	Salt encrypted IP address
[26-61]	Med-Port-Number	UDP port in the analyzer device to which mirrored packets are forwarded	len	sublen	Salt encrypted integer
[26-62]	MLPPP-Bundle-Name	Text string that identifies the Multilink PPP bundle name	len	sublen	string:mlppp-bundle-name
[26-63]	Interface-Desc	Text string that identifies the subscriber's access interface	len	sublen	string:interface-description
[26-64]	Tunnel-Group	Name of the tunnel group assigned to a domain map	len	sublen	string:tunnel-group-name
[26-65]	Activate-Service	Service to activate for the subscriber	len	sublen	string:service-name
[26-66]	Deactivate-Service	Service to deactivate for the subscriber	len	sublen	string:service-name
[26-67]	Service-Volume-tagX	Amount of traffic, in MB, that can use the service; service is deactivated when the volume is exceeded	12	6	integer: volume in MB; 0 = infinite volume
[26-68]	Service-Timeout-tagX	Number of seconds that the service can be active; service is deactivated when the timeout expires	12	6	integer: time in seconds; 0 = no timeout

Table 51: Juniper Networks (Vendor ID 4874) VSA Formats (continued)

Attribute Number	Attribute Name	Description	Length	Subtype Length	Value
[26-69]	Service-Statistics-tagX	Enable or disable statistics for the service	12	6	integer: 0 = disable; 1 = enable time statistics; 2 = enable time and volume statistics
[26-70]	Ignore-DF-Bit	Enable or disable the ignore don't fragment (DF) bit feature on a B-RAS user's interface	12	6	integer: 0 = disable; 1 = enable
[26-71]	IGMP-Access-Name	Access List to use for the group (G) filter	len	sublen	string:32-octet
[26-72]	IGMP-Access-Src-Name	Access List to use for the source-group (S,G) filter	len	sublen	string:32-octet
[26-73]	IGMP-OIF-Map-Name	Multicast OIF (outgoing interface) mapping	len	sublen	string:32-octet
[26-74]	MLD-Access-Name	Access List to use for the group (G) filter	len	sublen	string:32-octet
[26-75]	MLD-Access-Src-Name	Access List to use for the source-group (S,G) filter	len	sublen	string:32-octet
[26-76]	MLD-OIF-Map-Name	Multicast OIF (outgoing interface) mapping	len	sublen	string:32-octet
[26-77]	MLD-Version	MLD Protocol Version (MLD Version 1 = 1; MLD Version 2 = 2)	12	6	integer:1-octet
[26-78]	IGMP-Version	IGMP Protocol Version (IGMP Version 1 = 1; IGMP Version 2 = 2; IGMP Version 3 = 3)	12	6	integer:1-octet
[26-79]	IP-Mcast-Adm-Bw-Limit	The maximum multicast bandwidth that will be admitted on an IP interface, in Kbps	12	6	integer:4-octet
[26-80]	IPv6-Mcast-Adm-Bw-Limit	The maximum multicast bandwidth that will be admitted on an IPv6 interface, in Kbps	12	6	integer:4-octet
[26-81]	L2c-Information	Series of type length value (tlv) fields (binary) representing the access loop parameters as defined in GSMP extensions for layer2 control (L2C) Topology Discovery and Line Configuration—draft-wadhwa-gsmp-l2control-configuration-00.txt (July 2006 expiration)	len	sublen	string: format is a series of type length value (tlv) fields (binary) representing the access loop parameters
[26-82]	Qos-Parameters	Name of the QoS parameter instance to create on the user's interface, followed by the value of the parameter. For example, the max-bandwidth 4000000 parameter instance represents the parameter name that was defined using the qos-parameter-define command (max-bandwidth) and the value to assign to the parameter (4000000). Multiple instances of this VSA can be returned from RADIUS using this format.	len	sublen	string: format is <i>parameter name parameter value</i> , where <i>parameter name</i> is ASCII name of a parameter name found in the QoS parameter definition and <i>parameter value</i> is the ASCII representation of 0–21474836470; multiple instances of this VSA can be returned from RADIUS using this format

Table 51: Juniper Networks (Vendor ID 4874) VSA Formats (continued)

Attribute Number	Attribute Name	Description	Length	Subtype Length	Value
[26-83]	Service-Session	Name of the service (including parameter values) that is associated with service manager statistics	len	sublen	string;service-name
[26-90]	L2TP-Resynch-Method	L2TP peer resynchronization method	12	6	integer: 0 = disabled; 1 = failover protocol; 2 = silent failover; 3 = failover protocol with silent failover as backup
[26-91]	Tunnel-Switch-Profile	<ul style="list-style-type: none"> ■ Name of the L2TP tunnel switch profile ■ The L2TP tunnel switch profile defines the L2TP tunnel switching behavior for the interfaces to which this profile is assigned 	len	sublen	string; tunnel-switch-profile
[26-92]	L2C-Up-Stream-Data	Actual upstream rate access loop parameter (ASCII encoded) as defined in GSMP extensions for layer2 control (L2C) Topology Discovery and Line Configuration—draft-wadhwa-gsmp-l2control-configuration-00.txt (July 2006 expiration).	len	sublen	string: actual upstream rate access loop parameter (ASCII encoded)
[26-93]	L2C-Down-Stream-Data	Actual downstream rate access loop parameter (ASCII encoded) as defined in GSMP extensions for layer2 control (L2C) Topology Discovery and Line Configuration—draft-wadhwa-gsmp-l2control-configuration-00.txt (July 2006 expiration).	len	sublen	string: actual downstream rate access loop parameter (ASCII encoded)
[26-94]	Tunnel-Tx-Speed-Method	The method that the router uses to calculate the transmit connect speed of the subscriber's access interface. This speed is reported in L2TP Transmit (TX) Speed AVP 24. During the establishment of an L2TP tunnel session, the LAC sends AVP 24 to the LNS to convey the transmit speed of the subscriber's access interface.	12	6	integer: 1 = static-layer2, TX speed based on static layer 2 settings; 2 = dynamic-layer2, TX speed based on dynamic layer 2 settings; 3 = qos, TX speed based on QoS settings; 4 = actual, TX speed that is the lesser of the dynamic-layer2 value or the qos value
[26-95]	IGMP-Query-Interval	IGMP Query Interval	12	6	integer: 4-octet
[26-96]	IGMP-Max-Resp-Time	IGMP Maximum Response Time	12	6	integer: 4-octet
[26-97]	IGMP-Immediate-Leave	IGMP Immediate Leave	12	6	4-octet integer: 0 = disabled 1 = enabled

Table 51: Juniper Networks (Vendor ID 4874) VSA Formats (continued)

Attribute Number	Attribute Name	Description	Length	Subtype Length	Value
[26-98]	MLD-Query-Interval	MLD Query Interval	12	6	integer: 4-octet
[26-99]	MLD-Max-Resp-Time	MLD Maximum Response Time	12	6	integer: 4-octet
[26-100]	MLD-Immediate-Leave	MLD Immediate Leave	12	6	4-octet integer: 0 = disabled 1 = enabled

DSL Forum VSAs

[Table 52](#) describes the DSL Forum VSAs supported by JUNOS software for RADIUS. JUNOS software uses the vendor ID assigned to the DSL Forum (3561, or DE9 in hexadecimal format) by the Internet Assigned Numbers Authority (IANA).

Table 52: JUNOS Software DSL Forum (Vendor ID 3561) VSA Formats

Attribute Number	Attribute Name	Description	Length	Subtype Length	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	len	sublen	string: agent-circuit-id
[26-2]	Agent-Remote-Id	Unique identifier for the subscriber associated with the DSLAM interface from which requests are initiated	len	sublen	string: agent-remote-id
[26-129]	Actual-Data-Rate-Upstream	Actual upstream data rate of the subscriber's synchronized DSL link	12	6	integer: 4-octet
[26-130]	Actual-Data-Rate-Downstream	Actual downstream data rate of the subscriber's synchronized DSL link	12	6	integer: 4-octet
[26-131]	Minimum-Data-Rate-Upstream	Minimum upstream data rate configured for the subscriber	12	6	integer: 4-octet
[26-132]	Minimum-Data-Rate-Downstream	Minimum downstream data rate configured for the subscriber	12	6	integer: 4-octet
[26-133]	Attainable-Data-Rate-Upstream	Upstream data rate that the subscriber can attain	12	6	integer: 4-octet
[26-134]	Attainable-Data-Rate-Downstream	Downstream data rate that the subscriber can attain	12	6	integer: 4-octet
[26-135]	Maximum-Data-Rate-Upstream	Maximum upstream data rate configured for the subscriber	12	6	integer: 4-octet
[26-136]	Maximum-Data-Rate-Downstream	Maximum downstream data rate configured for the subscriber	12	6	integer: 4-octet

Table 52: JUNOS Software DSL Forum (Vendor ID 3561) VSA Formats (continued)

Attribute Number	Attribute Name	Description	Length	Subtype Length	Value
[26-137]	Minimum-Data-Rate-Upstream-Low-Power	Minimum upstream data rate in low power state configured for the subscriber	12	6	integer: 4-octet
[26-138]	Minimum-Data-Rate-Downstream-Low-Power	Minimum downstream data rate in low power state configured for the subscriber	12	6	integer: 4-octet
[26-139]	Maximum-Interleaving-Delay-Upstream	Maximum one-way upstream interleaving delay configured for the subscriber	12	6	integer: 4-octet
[26-140]	Actual-Interleaving-Delay-Upstream	Subscriber's actual one-way upstream interleaving delay	12	6	integer: 4-octet
[26-141]	Maximum-Interleaving-Delay-Downstream	Maximum one-way downstream interleaving delay configured for the subscriber	12	6	integer: 4-octet
[26-142]	Actual-Interleaving-Delay-Downstream	Subscriber's actual one-way downstream interleaving delay	12	6	integer: 4-octet
[26-144]	Access-Loop-Encapsulation	Encapsulation used by the subscriber associated with the DSLAM interface from which requests are initiated	11	5	string: 3-byte
[26-254]	IWF-Session	Indication that the interworking function (IWF) has been performed for the subscriber's session to enable the transport of PPP over ATM traffic on a PPPoE interface	8	2	No data field required

Pass Through RADIUS Attributes

[Table 53](#) describes the RADIUS attribute that is not processed by JUNOS software. The router simply passes this attribute to its destination.

Table 53: RADIUS Attribute Passed Through by JUNOS Software

Standard Number	Attribute Name	Description
[79]	EAP-Message	<ul style="list-style-type: none"> ■ Used by RADIUS relay servers ■ Passed through to the RADIUS server

References

For more information about RADIUS attributes, see the following RFCs:

- [RFC 2661—Layer Two Tunneling Protocol “L2TP” \(August 1999\)](#)
- [RFC 2865—Remote Authentication Dial In User Service \(RADIUS\) \(June 2000\)](#)
- [RFC 2866—RADIUS Accounting \(June 2000\)](#)
- [RFC 2867—RADIUS Accounting Modifications for Tunnel Protocol Support \(June 2000\)](#)
- [RFC 2868—RADIUS Attributes for Tunnel Protocol Support \(June 2000\)](#)
- [RFC 2869—RADIUS Extensions \(June 2000\)](#)
- [RFC 3748—Extensible Authentication Protocol \(EAP\) \(June 2004\)](#)
- [DSL Forum Vendor-Specific RADIUS Attributes—draft-mammoliti-radius-dsl-vsa-02.txt \(September 2006 expiration\)](#)



NOTE: IETF drafts are valid for only 6 months from the date of issuance. They must be considered as works in progress. Please refer to the IETF Web site at <http://www.ietf.org> for the latest drafts.

Appendix B

L2TP Disconnect Cause Codes

Table 54 describes the Point-to-Point Protocol (PPP) disconnect cause codes that are displayed by the **show l2tp received-disconnect-cause-summary** command, sorted by code number. For additional information, see RFC 3145.

Table 54: PPP Disconnect Cause Codes

Code	Name	Description
0	no info	<p>Code 0 includes disconnect causes that are not specifically identified by other codes. This code is generated in the following circumstances:</p> <ul style="list-style-type: none">■ Internal resource constraints (for example, excessive load or reduced resource availability) have prevented the generation of a more specific disconnect code.■ RFC 3145 does not define a disconnect code that corresponds to the cause of the disconnection. <p>The following list shows current disconnection causes on an E-series LNS that do not have a specific disconnect cause codes:</p> <ul style="list-style-type: none">■ The peer initiated termination of LCP after the completion of LCP negotiations, but prior to proceeding to authentication of NCP negotiation. No conditions occurred that enabled the LNS to infer a more informative disconnect code.■ The peer initiated renegotiation of LCP.■ Invalid local MRU (for example, MRU negotiation has been disabled, but the lower MRU is less than the default MRU of 1500).■ Unexpected local MLPPP MRRU for existing bundle (RFC 3145 code 10 covers peer MRRU mismatches, but not local mismatches).■ Authentication failures not covered by any of the authentication-related codes (codes 13-16), such as:<ul style="list-style-type: none">■ Authentication denial of the local LCP by the peer■ Local authentication failure due to no resources■ Local authentication failure due to no authenticator
1	admin disconnect	<p>The disconnection was a result of direct administrative action, including:</p> <ul style="list-style-type: none">■ The administrator shut down the network or link interface.■ The administrator logged out the subscriber.
2	renegotiation disabled	<p>Code 2 is not used; the E-series LNS is always capable of renegotiating LCP if proxy data is not available.</p>

Table 54: PPP Disconnect Cause Codes (continued)

Code	Name	Description
3	normal disconnect	<p>Indicates that one of the following events occurred:</p> <ul style="list-style-type: none"> ■ user-initiated logout (direction 1) ■ session timeout (direction 2) ■ inactivity timeout (direction 2) ■ address lease expired (direction 2) <p>The E-series LNS determines by inference that a normal disconnect has occurred for direction 1. The LNS does this when the peer initiates LCP termination after proceeding beyond the successful negotiation of LCP (that is, after starting authentication signaling or NCP negotiation).</p>
4	compulsory encryption refused	<p>Code 4 with direction 2 is generated if the following conditions are met:</p> <ul style="list-style-type: none"> ■ The peer initiates LCP termination without having proceeded beyond the completion of LCP negotiation, and ■ Prior to receiving the terminate request from the peer, the local LCP has sent a Protocol Reject in response to any packet for Encryption Control Protocol (ECP) protocols (protocol codes 0x8053, 0x8055) from the peer. <p>Code 4 with direction 1 is never generated, because the E-series LNS never requests ECP.</p>
5	lcp failed to converge	An LCP configuration error prevented LCP from converging; the two peers attempted to negotiate but did not agree on acceptable LCP parameters.
6	lcp peer silent	LCP negotiation timed out; the LNS did not receive any LCP packets from the LAC.
7	lcp magic number error	A magic number error was detected; this indicates a possible looped back link.
8	lcp keepalive error	The keepalive drop count was exceeded.
9	lcp mlppp endpoint discriminator mismatch	Code 9 is not used. Dynamic MLPPP bundling, which is the only kind of MLPPP bundling supported for MLPPP/L2TP, uses the endpoint discriminator as part of the key for bundle selection. Therefore, there will never be an unexpected endpoint discriminator for an existing MLPPP bundle.
10	lcp mlppp mrru not valid	The link attempted to join an existing MLPPP bundle whose peer maximum received reconstructed unit (MRRU) did not match the peer MRRU negotiated by the link.
11	lcp mlppp peer ssn invalid	Code 11 is not used; the short sequence number (SSN) option is not supported.
12	lcp callback refused	<p>Code 12 with direction 2 is generated when the following conditions are met:</p> <ul style="list-style-type: none"> ■ The peer initiates LCP termination without having proceeded to NCP negotiation, and ■ Prior to the termination, the local LCP has responded with a negative acknowledgement (NAK) to a callback option (LCP option 13) from the peer. <p>The E-series LNS never generates code 12 with direction 1 because the LNS never requests callback.</p>
13	authenticate timed out	Authentication failed because the authentication protocol timed out; either the CHAP Authenticate Response or the PAP Authenticate Request was not received.
14	authenticate mlppp name mismatch	Code 14 is not used. Dynamic MLPPP bundling, which is the only kind of MLPPP bundling supported for MLPPP/L2TP, uses the authenticated name as part of the key for bundle selection. Therefore, there will never be an unexpected authenticated name for an existing MLPPP bundle.

Table 54: PPP Disconnect Cause Codes (continued)

Code	Name	Description
15	authenticate protocol refused	<p>No acceptable authentication protocol was negotiated by LCP.</p> <ul style="list-style-type: none"> ■ Code 15 with direction 1 is generated if the peer rejected all of the authentication protocols requested by the local LCP. ■ Code 15 with direction 2 is generated if the following conditions are met: <ul style="list-style-type: none"> ■ The peer initiates LCP termination without having proceeded beyond completion of NCP negotiation, and ■ During LCP negotiation, the local LCP responded with a NAK to the final authentication protocol requested by the peer.
16	authenticate failure	<ul style="list-style-type: none"> ■ Code 16 with direction 1 is generated if the local authentication of the peer fails (that is, the authenticator sent a PAP NAK or CHAP Failure packet) ■ Code 16 with direction 2 is generated if the peer authentication of the local LCP fails (that is, the authenticator received a PAP NAK or CHAP Failure packet). <p>Note that there are a variety of causes for authentication failures, including bad credentials (bad name, password or secret) and resource problems.</p>
17	ncp no negotiation completed	<p>Code 17 is generated only if an NCP configuration error has prevented NCP negotiation from converging. This occurs when the two peers do not agree on acceptable NCP parameters within the time allowed for upper-layer negotiation.</p> <p>Code 19 takes precedence over code 17 in situations related to address convergence failure.</p>
18	ncp no ncps available	<p>No NCPs were successfully enabled within the time allowed for upper-layer negotiation.</p>
19	ncp addresses failed to converge	<p>An NCP configuration error has prevented NCP negotiation from converging on acceptable addresses. This occurs if the two peers never agree on acceptable NCP addresses within the time allowed for upper-layer negotiation.</p> <ul style="list-style-type: none"> ■ Code 19 with direction 1 is generated if the peer denies address parameters requested by the local NCP. ■ Code 19 with direction 2 is generated if the local NCP denies address parameters requested by the peer. <p>The IPv6 interface identifier is considered an address for the purposes of code 19.</p> <p>Code 19 takes precedence over code 17 in situations related to address convergence failure.</p>
20	ncp negotiation inhibited	<ul style="list-style-type: none"> ■ Code 20 with direction 2 indicates that an upper layer negotiation was inhibited for any enabled NCP because the required network-layer parameters were not available as a result of the authentication stage. ■ Code 20 with direction 1 is never generated; the NCPs are never enabled if there is no non-null local address.

Appendix C

Application Terminate Reasons

This appendix lists the default mappings for application terminate reasons to RADIUS Acct-Terminate-Cause attributes. [Table 55](#) lists the default mappings for AAA, [Table 56](#) lists default mappings for L2TP, [Table 57](#) lists the default mappings for PPP, and [Table 58](#) lists default mappings for RADIUS client. See *Mapping Application Terminate Reasons to RADIUS Terminate Codes* on page 77 for information about configuring custom mappings for application terminate reasons to RADIUS Acct-Terminate-Cause attributes.

- [AAA Terminate Reasons](#) on page 531
- [L2TP Terminate Reasons](#) on page 532
- [PPP Terminate Reasons](#) on page 542
- [RADIUS Client Terminate Reasons](#) on page 547

AAA Terminate Reasons

[Table 55](#) lists the default AAA terminate mappings. The table indicates the supported AAA terminate and deny reasons and the RADIUS Acct-Terminate-Cause attributes they are mapped to by default.

Table 55: Default AAA Mappings

AAA Shutdown or Deny Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
deny address allocation failure	17	user error
deny address assignment failure	17	user error
deny application error	17	user error
deny authentication denied	17	user error
deny authentication failure	17	user error
deny authorization failure	17	user error
deny incompatible request	17	user error
deny invalid tunnel configuration	17	user error
deny limit exceeded	17	user error
deny mixed user types	10	nas request
deny no access challenge support	17	user error

Table 55: Default AAA Mappings (continued)

AAA Shutdown or Deny Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
deny no address allocation resources	17	user error
deny no resources	10	nas request
deny redirected authentication failure	17	user error
deny server not available	17	user error
deny server request timeout	17	user error
deny terminating user	10	nas request
deny unknown subscriber	17	user error
deny user termination	17	user error
shutdown address lease expiration	10	nas request
shutdown administrative reset	6	admin reset

L2TP Terminate Reasons

[Table 56](#) lists the default L2TP terminate mappings. The table indicates the supported L2TP terminate reasons and the RADIUS Acct-Terminate-Cause attributes they are mapped to by default.

Table 56: Default L2TP Mappings

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session access interface down	8	port error
session admin close	6	admin reset
session admin drain	6	admin reset
session call down	10	nas request
session call failed	15	service unavailable
session create failed limit reached	9	nas error
session create failed no resources	9	nas error
session create failed single shot tunnel already fired	9	nas error
session create failed too busy	9	nas error
session failover protocol resync disconnect	6	admin reset
session hardware unavailable	8	port error
session no resources server port	9	nas error
session not ready	9	nas error
session rx cdn	10	nas request
session rx cdn avp bad hidden	10	nas request
session rx cdn avp bad value assigned session id	10	nas request
session rx cdn avp duplicate value assigned session id	10	nas request
session rx cdn avp malformed bad length	10	nas request

Table 56: Default L2TP Mappings (continued)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx cdn avp malformed truncated	10	nas request
session rx cdn avp missing mandatory assigned session id	10	nas request
session rx cdn avp missing mandatory result code	10	nas request
session rx cdn avp missing random vector	10	nas request
session rx cdn avp missing secret	10	nas request
session rx cdn avp unknown	10	nas request
session rx cdn no resources	10	nas request
session rx iccn avp bad hidden	10	nas request
session rx iccn avp bad value framing type	10	nas request
session rx iccn avp bad value proxy authen type	10	nas request
session rx iccn avp bad value unsupported proxy authen type	10	nas request
session rx iccn avp malformed bad length	10	nas request
session rx iccn avp malformed truncated	10	nas request
session rx iccn avp missing mandatory connect speed	10	nas request
session rx iccn avp missing mandatory framing type	10	nas request
session rx iccn avp missing mandatory proxy authen challenge	10	nas request
session rx iccn avp missing mandatory proxy authen id	10	nas request
session rx iccn avp missing mandatory proxy authen name	10	nas request
session rx iccn avp missing mandatory proxy authen response	10	nas request
session rx iccn avp missing random vector	10	nas request
session rx iccn avp missing secret	10	nas request
session rx iccn avp unknown	10	nas request
session rx iccn no resources	10	nas request
session rx iccn unexpected	10	nas request
session rx icrp avp bad hidden	10	nas request
session rx icrp avp bad value assigned session id	10	nas request
session rx icrp avp duplicate value assigned session id	10	nas request
session rx icrp avp malformed bad length	10	nas request
session rx icrp avp malformed truncated	10	nas request
session rx icrp avp missing mandatory assigned session id	10	nas request
session rx icrp avp missing random vector	10	nas request
session rx icrp avp missing secret	10	nas request
session rx icrp avp unknown	10	nas request
session rx icrp no resources	10	nas request
session rx icrp unexpected	10	nas request

Table 56: Default L2TP Mappings (continued)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx icrq admin close	6	admin reset
session rx icrq authenticate failed host	10	nas request
session rx icrq avp bad hidden	10	nas request
session rx icrq avp bad value assigned session id	10	nas request
session rx icrq avp bad value bearer type	10	nas request
session rx icrq avp bad value cisco nas port	10	nas request
session rx icrq avp duplicate value assigned session id	10	nas request
session rx icrq avp malformed bad length	10	nas request
session rx icrq avp malformed truncated	10	nas request
session rx icrq avp missing mandatory assigned session id	10	nas request
session rx icrq avp missing mandatory call serial number	10	nas request
session rx icrq avp missing random vector	10	nas request
session rx icrq avp missing secret	10	nas request
session rx icrq avp unknown	10	nas request
session rx icrq no resources	10	nas request
session rx icrq unexpected	10	nas request
session rx occn avp bad hidden	10	nas request
session rx occn avp bad value framing type	10	nas request
session rx occn avp malformed bad length	10	nas request
session rx occn avp malformed truncated	10	nas request
session rx occn avp missing mandatory connect speed	10	nas request
session rx occn avp missing mandatory framing type	10	nas request
session rx occn avp missing random vector	10	nas request
session rx occn avp missing secret	10	nas request
session rx occn avp unknown	10	nas request
session rx occn no resources	10	nas request
session rx occn unexpected	10	nas request
session rx ocrp avp bad hidden	10	nas request
session rx ocrp avp bad value assigned session id	10	nas request
session rx ocrp avp duplicate value assigned session id	10	nas request
session rx ocrp avp malformed bad length	10	nas request
session rx ocrp avp malformed truncated	10	nas request
session rx ocrp avp missing mandatory assigned session id	10	nas request
session rx ocrp avp missing random vector	10	nas request
session rx ocrp avp missing secret	10	nas request
session rx ocrp avp unknown	10	nas request
session rx ocrp no resources	10	nas request

Table 56: Default L2TP Mappings (continued)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx ocrp unexpected	10	nas request
session rx ocrq admin close	10	admin reset
session rx ocrq authenticate failed host	10	nas request
session rx ocrq avp bad hidden	10	nas request
session rx ocrq avp bad value assigned session id	10	nas request
session rx ocrq avp bad value bearer type	10	nas request
session rx ocrq avp bad value framing type	10	nas request
session rx ocrq avp duplicate value assigned session id	10	nas request
session rx ocrq avp malformed bad length	10	nas request
session rx ocrq avp malformed truncated	10	nas request
session rx ocrq avp missing mandatory assigned session id	10	nas request
session rx ocrq avp missing mandatory bearer type	10	nas request
session rx ocrq avp missing mandatory call serial number	10	nas request
session rx ocrq avp missing mandatory called number	10	nas request
session rx ocrq avp missing mandatory framing type	10	nas request
session rx ocrq avp missing mandatory maximum bps	10	nas request
session rx ocrq avp missing mandatory minimum bps	10	nas request
session rx ocrq avp missing random vector	10	nas request
session rx ocrq avp missing secret	10	nas request
session rx ocrq avp unknown	10	nas request
session rx ocrq no resources	10	nas request
session rx ocrq unexpected	10	nas request
session rx ocrq unsupported	9	nas error
session rx sli avp bad hidden	10	nas request
session rx sli avp bad value accm	10	nas request
session rx sli avp malformed bad length	10	nas request
session rx sli avp malformed truncated	10	nas request
session rx sli avp missing mandatory accm	10	nas request
session rx sli avp missing random vector	10	nas request
session rx sli avp missing secret	10	nas request
session rx sli avp unknown	10	nas request
session rx sli no resources	10	nas request
session rx unexpected packet lac incoming	10	nas request
session rx unexpected packet lac outgoing	10	nas request
session rx unexpected packet lns incoming	10	nas request
session rx unexpected packet lns outgoing	10	nas request
session rx unknown session id	10	nas request

Table 56: Default L2TP Mappings (continued)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx wen avp bad hidden	10	nas request
session rx wen avp malformed bad length	10	nas request
session rx wen avp malformed truncated	10	nas request
session rx wen avp missing mandatory call errors	10	nas request
session rx wen avp missing random vector	10	nas request
session rx wen avp missing secret	10	nas request
session rx wen avp unknown	10	nas request
session rx wen no resources	10	nas request
session timeout connection	10	nas request
session timeout inactivity	4	idle timeout
session timeout session	5	session timeout
session timeout upper create	9	nas error
session transmit speed unavailable	9	nas error
session tunnel down	15	service unavailable
session tunnel failed	15	service unavailable
session tunnel switch profile deleted	6	admin reset
session tunneled interface down	8	port error
session unknown cause	9	nas error
session upper create failed	9	nas error
session upper removed	15	service unavailable
session warmstart not operational	15	service unavailable
session warmstart recovery error	15	service unavailable
session warmstart upper not restacked	10	nas request
tunnel admin close	6	admin reset
tunnel admin drain	6	admin reset
tunnel control channel failed	15	service unavailable
tunnel created no sessions	1	user request
tunnel destination address changed	6	admin reset
tunnel destination down	10	nas request
tunnel failover protocol no resources for recovery tunnel	15	service unavailable
tunnel failover protocol no resources for session resync	15	service unavailable
tunnel failover protocol not supported	15	service unavailable
tunnel failover protocol not supported by peer	15	service unavailable
tunnel failover protocol recovery control channel failed	15	service unavailable
tunnel failover protocol recovery tunnel failed	15	service unavailable
tunnel failover protocol recovery tunnel finished	1	user request
tunnel failover protocol recovery tunnel primary down	1	user request

Table 56: Default L2TP Mappings (continued)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel failover protocol session resync failed	15	service unavailable
tunnel host profile changed	6	admin reset
tunnel host profile deleted	6	admin reset
tunnel rx sccn authenticate failed challenge	17	user error
tunnel rx sccn avp bad hidden	15	service unavailable
tunnel rx sccn avp bad value challenge response	15	service unavailable
tunnel rx sccn avp malformed bad length	15	service unavailable
tunnel rx sccn avp malformed truncated	15	service unavailable
tunnel rx sccn avp missing challenge response	17	user error
tunnel rx sccn avp missing random vector	15	service unavailable
tunnel rx sccn avp missing secret	15	service unavailable
tunnel rx sccn avp unexpected challenge response	15	service unavailable
tunnel rx sccn avp unknown	15	service unavailable
tunnel rx sccn no resources	15	service unavailable
tunnel rx sccn session id not null	15	service unavailable
tunnel rx sccn unexpected	15	service unavailable
tunnel rx sccrp authenticate failed challenge	17	user error
tunnel rx sccrp authenticate failed host	17	user error
tunnel rx sccrp avp bad hidden	15	service unavailable
tunnel rx sccrp avp bad value assigned tunnel id	15	service unavailable
tunnel rx sccrp avp bad value bearer capabilities	15	service unavailable
tunnel rx sccrp avp bad value challenge	15	service unavailable
tunnel rx sccrp avp bad value challenge response	15	service unavailable
tunnel rx sccrp avp bad value failover capability	15	service unavailable
tunnel rx sccrp avp bad value framing capabilities	15	service unavailable
tunnel rx sccrp avp bad value protocol version	15	service unavailable
tunnel rx sccrp avp bad value receive window size	15	service unavailable
tunnel rx sccrp avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx sccrp avp malformed bad length	15	service unavailable
tunnel rx sccrp avp malformed truncated	15	service unavailable
tunnel rx sccrp avp missing challenge response	17	user error
tunnel rx sccrp avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx sccrp avp missing mandatory framing capabilities	15	service unavailable
tunnel rx sccrp avp missing mandatory host name	15	service unavailable
tunnel rx sccrp avp missing mandatory protocol version	15	service unavailable
tunnel rx sccrp avp missing random vector	15	service unavailable
tunnel rx sccrp avp missing secret	15	service unavailable

Table 56: Default L2TP Mappings (continued)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx sccrp avp unexpected challenge response	15	service unavailable
tunnel rx sccrp avp unexpected challenge without secret	15	service unavailable
tunnel rx sccrp avp unknown	15	service unavailable
tunnel rx sccrp no resources	15	service unavailable
tunnel rx sccrp session id not null	15	service unavailable
tunnel rx sccrp unexpected	15	service unavailable
tunnel rx sccrq admin close	6	admin reset
tunnel rx sccrq authenticate failed host	17	user error
tunnel rx sccrq avp bad hidden	15	service unavailable
tunnel rx sccrq avp bad value assigned tunnel id	15	service unavailable
tunnel rx sccrq avp bad value bearer capabilities	15	service unavailable
tunnel rx sccrq avp bad value challenge	15	service unavailable
tunnel rx sccrq avp bad value failover capability	15	service unavailable
tunnel rx sccrq avp bad value framing capabilities	15	service unavailable
tunnel rx sccrq avp bad value protocol version	15	service unavailable
tunnel rx sccrq avp bad value receive window size	15	service unavailable
tunnel rx sccrq avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx sccrq avp malformed bad length	15	service unavailable
tunnel rx sccrq avp malformed truncated	15	service unavailable
tunnel rx sccrq avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx sccrq avp missing mandatory framing capabilities	15	service unavailable
tunnel rx sccrq avp missing mandatory host name	15	service unavailable
tunnel rx sccrq avp missing mandatory protocol version	15	service unavailable
tunnel rx sccrq avp missing random vector	15	service unavailable
tunnel rx sccrq avp missing secret	15	service unavailable
tunnel rx sccrq avp unexpected challenge without secret	15	service unavailable
tunnel rx sccrq avp unknown	15	service unavailable
tunnel rx sccrq bad address	15	service unavailable
tunnel rx sccrq no resources	15	service unavailable
tunnel rx sccrq no resources max tunnels	15	service unavailable
tunnel rx sccrq session id not null	15	service unavailable
tunnel rx sccrq unexpected	15	service unavailable
tunnel rx stopccn	1	user request
tunnel rx stopccn avp bad hidden	15	service unavailable
tunnel rx stopccn avp bad value assigned tunnel id	15	service unavailable
tunnel rx stopccn avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx stopccn avp malformed bad length	15	service unavailable

Table 56: Default L2TP Mappings (continued)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx stopccn avp malformed truncated	15	service unavailable
tunnel rx stopccn avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx stopccn avp missing mandatory result code	15	service unavailable
tunnel rx stopccn avp missing random vector	15	service unavailable
tunnel rx stopccn avp missing secret	15	service unavailable
tunnel rx stopccn avp unknown	15	service unavailable
tunnel rx stopccn no resources	15	service unavailable
tunnel rx stopccn session id not null	15	service unavailable
tunnel rx frs avp malformed truncated	15	service unavailable
tunnel rx frs avp missing mandatory failover session state	15	service unavailable
tunnel rx frs avp missing random vector	15	service unavailable
tunnel rx frs avp missing secret	15	service unavailable
tunnel rx frs avp unknown	15	service unavailable
tunnel rx frs no resources	15	service unavailable
tunnel rx frs session id not null	15	service unavailable
tunnel rx fsq avp bad hidden	15	service unavailable
tunnel rx fsq avp malformed bad length	15	service unavailable
tunnel rx fsq avp malformed truncated	15	service unavailable
tunnel rx fsq avp missing mandatory failover session state	15	service unavailable
tunnel rx fsq avp missing random vector	15	service unavailable
tunnel rx fsq avp missing secret	15	service unavailable
tunnel rx fsq avp unknown	15	service unavailable
tunnel rx fsq no resources	15	service unavailable
tunnel rx fsq session id not null	15	service unavailable
tunnel rx fsr avp bad hidden	15	service unavailable
tunnel rx fsr avp malformed bad length	15	service unavailable
tunnel rx unexpected packet	15	service unavailable
tunnel rx unexpected packet for session	15	service unavailable
tunnel rx unknown packet message type indecipherable	15	service unavailable
tunnel rx unknown packet message type unrecognized	15	service unavailable
tunnel rx recovery sccn authenticate failed challenge	17	user error
tunnel rx recovery sccn avp bad hidden	15	service unavailable
tunnel rx recovery sccn avp bad value challenge response	15	service unavailable
tunnel rx recovery sccn avp malformed bad length	15	service unavailable
tunnel rx recovery sccn avp malformed truncated	15	service unavailable
tunnel rx recovery sccn avp missing challenge response	17	user error
tunnel rx recovery sccn avp missing random vector	15	service unavailable

Table 56: Default L2TP Mappings (continued)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx recovery sccn avp missing secret	15	service unavailable
tunnel rx recovery sccn avp unexpected challenge response	15	service unavailable
tunnel rx recovery sccn avp unknown	15	service unavailable
tunnel rx recovery sccn no resources	15	service unavailable
tunnel rx recovery sccn session id not null	15	service unavailable
tunnel rx recovery sccrp authenticate failed challenge	17	user error
tunnel rx recovery sccrp avp bad hidden	15	service unavailable
tunnel rx recovery sccrp avp bad value assigned tunnel id	15	service unavailable
tunnel rx recovery sccrp avp bad value bearer capabilities	15	service unavailable
tunnel rx recovery sccrp avp bad value challenge	15	service unavailable
tunnel rx recovery sccrp avp bad value challenge response	15	service unavailable
tunnel rx recovery sccrp avp bad value framing capabilities	15	service unavailable
tunnel rx recovery sccrp avp bad value protocol version	15	service unavailable
tunnel rx recovery sccrp avp bad value receive window size	15	service unavailable
tunnel rx recovery sccrp avp bad value suggested control sequence	15	service unavailable
tunnel rx recovery sccrp avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx recovery sccrp avp malformed bad length	15	service unavailable
tunnel rx recovery sccrp avp malformed truncated	15	service unavailable
tunnel rx recovery sccrp avp mismatched host name	15	service unavailable
tunnel rx recovery sccrp avp mismatched vendor name	15	service unavailable
tunnel rx recovery sccrp avp missing challenge response	17	user error
tunnel rx recovery sccrp avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx recovery sccrp avp missing mandatory framing capabilities	15	service unavailable
tunnel rx recovery sccrp avp missing mandatory host name	15	service unavailable
tunnel rx recovery sccrp avp missing mandatory protocol version	15	service unavailable
tunnel rx recovery sccrp avp missing random vector	15	service unavailable
tunnel rx recovery sccrp avp missing secret	15	service unavailable
tunnel rx recovery sccrp avp unexpected challenge response	15	service unavailable
tunnel rx recovery sccrp avp unexpected challenge without secret	15	service unavailable
tunnel rx recovery sccrp avp unknown	15	service unavailable
tunnel rx recovery sccrp no resources	15	service unavailable
tunnel rx recovery sccrp session id not null	15	service unavailable
tunnel rx recovery sccrp admin close	6	admin reset

Table 56: Default L2TP Mappings (continued)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx recovery sccrq avp bad hidden	15	service unavailable
tunnel rx recovery sccrq avp bad value assigned tunnel id	15	service unavailable
tunnel rx recovery sccrq avp bad value bearer capabilities	15	service unavailable
tunnel rx recovery sccrq avp bad value challenge	15	service unavailable
tunnel rx recovery sccrq avp bad value framing capabilities	15	service unavailable
tunnel rx recovery sccrq avp bad value protocol version	15	service unavailable
tunnel rx recovery sccrq avp bad value receive window size	15	service unavailable
tunnel rx recovery sccrq avp bad value tunnel recovery	15	service unavailable
tunnel rx recovery sccrq avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx recovery sccrq avp duplicate value tie breaker	15	service unavailable
tunnel rx recovery sccrq avp malformed bad length	15	service unavailable
tunnel rx recovery sccrq avp malformed truncated	15	service unavailable
tunnel rx recovery sccrq avp mismatched host name	15	service unavailable
tunnel rx recovery sccrq avp mismatched vendor name	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory framing capabilities	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory host name	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory protocol version	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory tunnel recovery	15	service unavailable
tunnel rx recovery sccrq avp missing random vector	15	service unavailable
tunnel rx recovery sccrq avp missing secret	15	service unavailable
tunnel rx recovery sccrq avp missing tie breaker	15	service unavailable
tunnel rx recovery sccrq avp unexpected challenge without secret	15	service unavailable
tunnel rx recovery sccrq avp unknown	15	service unavailable
tunnel rx recovery sccrq no resources	15	service unavailable
tunnel rx recovery sccrq session id not null	15	service unavailable
tunnel rx recovery sccrq tunnel id not null	15	service unavailable
tunnel rx recovery stopccn avp bad hidden	15	service unavailable
tunnel rx recovery stopccn avp bad value assigned tunnel id	15	service unavailable
tunnel rx recovery stopccn avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx recovery stopccn avp malformed bad length	15	service unavailable
tunnel rx recovery stopccn avp malformed truncated	15	service unavailable

Table 56: Default L2TP Mappings (continued)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx recovery stopccn avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx recovery stopccn avp missing mandatory result code	15	service unavailable
tunnel rx recovery stopccn avp missing random vector	15	service unavailable
tunnel rx recovery stopccn avp missing secret	15	service unavailable
tunnel rx recovery stopccn avp unknown	15	service unavailable
tunnel rx recovery stopccn no resources	15	service unavailable
tunnel rx recovery stopccn session id not null	15	service unavailable
tunnel rx recovery unexpected packet	15	service unavailable
tunnel rx recovery unknown packet message type indecipherable	15	service unavailable
tunnel rx recovery unknown packet message type unrecognized	15	service unavailable
tunnel rx session packet null sid invalid	15	service unavailable
tunnel rx session packet null sid without assigned session id	15	service unavailable
tunnel timeout connection	15	service unavailable
tunnel timeout connection recovery tunnel	15	service unavailable
tunnel timeout idle	1	user request
tunnel unknown cause	9	nas error
tunnel warmstart not operational	15	service unavailable
tunnel warmstart recovery error	15	service unavailable

PPP Terminate Reasons

Table 57 lists the default PPP terminate mappings. The table indicates the supported PPP terminate reasons and the RADIUS Acct-Terminate-Cause attributes they are mapped to by default.

Table 57: Default PPP Mappings

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
authenticate authenticator timeout	17	user error
authenticate challenge timeout	10	nas request
authenticate chap no resources	10	nas request
authenticate chap peer authenticator timeout	17	user error
authenticate deny by peer	17	user error
authenticate inactivity timeout	4	idle timeout
authenticate max requests	10	nas request
authenticate no authenticator	10	nas request

Table 57: Default PPP Mappings (continued)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
authenticate pap peer authenticator timeout	17	user error
authenticate pap request timeout	10	nas request
authenticate session timeout	5	session timeout
authenticate too many requests	10	nas request
authenticate tunnel fail immediate	10	nas request
authenticate tunnel unsupported tunnel type	10	nas request
bundle fail create	10	nas request
bundle fail engine add	10	nas request
bundle fail fragment size mismatch	10	nas request
bundle fail fragmentation location	10	nas request
bundle fail fragmentation mismatch	10	nas request
bundle fail join	10	nas request
bundle fail link selection mismatch	10	nas request
bundle fail local mped not set yet	10	nas request
bundle fail local mrru mismatch	10	nas request
bundle fail local mru mismatch	10	nas request
bundle fail peer mrru mismatch	10	nas request
bundle fail reassembly location	10	nas request
bundle fail reassembly mismatch	10	nas request
bundle fail record network	10	nas request
bundle fail server location mismatch	10	nas request
bundle fail static link	10	nas request
failover during authentication	6	admin reset
interface admin disable	6	admin reset
interface down	2	lost carrier
interface no hardware	8	port error
ip admin disable	10	nas request
ip inhibited by authentication	10	nas request
ip link down	10	nas request
ip max configure exceeded	10	nas request
ip no local ip address	10	nas request
ip no local ip address mask	10	nas request
ip no local primary dns address	10	nas request
ip no local primary nbns address	10	nas request
ip no local secondary dns address	10	nas request
ip no local secondary nbns address	10	nas request
ip no peer ip address	10	nas request

Table 57: Default PPP Mappings (continued)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
ip no peer ip address mask	10	nas request
ip no peer primary dns address	10	nas request
ip no peer primary nbns address	10	nas request
ip no peer secondary dns address	10	nas request
ip no peer secondary nbns address	10	nas request
ip no service	10	nas request
ip peer renegotiate rx conf ack	10	nas request
ip peer renegotiate rx conf nak	10	nas request
ip peer renegotiate rx conf rej	10	nas request
ip peer renegotiate rx conf req	10	nas request
ip peer terminate term ack	10	nas request
ip peer terminate code rej	10	nas request
ip peer terminate term req	10	nas request
ip service disable	10	nas request
ip stale stacking	10	nas request
ipv6 admin disable	10	nas request
ipv6 inhibited by authentication	10	nas request
ipv6 link down	10	nas request
ipv6 local and peer interface ids identical	10	nas request
ipv6 max configure exceeded	10	nas request
ipv6 no local ipv6 interface id	10	nas request
ipv6 no peer ipv6 interface id	10	nas request
ipv6 no service	10	nas request
ipv6 peer renegotiate rx conf ack	10	nas request
ipv6 peer renegotiate rx conf nak	10	nas request
ipv6 peer renegotiate rx conf rej	10	nas request
ipv6 peer renegotiate rx conf req	10	nas request
ipv6 peer terminate code rej	10	nas request
ipv6 peer terminate term ack	10	nas request
ipv6 peer terminate term req	10	nas request
ipv6 service disable	10	nas request
ipv6 stale stacking	10	nas request
lcp authenticate terminate hold	10	nas request
lcp configured mrru too small	10	nas request
lcp configured mru invalid	10	nas request
lcp configured mru too small	10	nas request
lcp dynamic interface hold	10	nas request

Table 57: Default PPP Mappings (continued)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
lcp keepalive failure	10	nas request
lcp loopback rx conf req	10	nas request
lcp loopback rx echo reply	10	nas request
lcp loopback rx echo req	10	nas request
lcp max configure exceeded	10	nas request
lcp mru changed	10	nas request
lcp negotiation timeout	10	nas request
lcp no localacm	10	nas request
lcp no localacfc	10	nas request
lcp no local authentication	10	nas request
lcp no local endpoint discriminator	10	nas request
lcp no local magic number	10	nas request
lcp no local mrru	10	nas request
lcp no local mru	10	nas request
lcp no localpfc	10	nas request
lcp no peer accm	10	nas request
lcp no peer authentication	10	nas request
lcp no peer endpoint discriminator	10	nas request
lcp no peer magicnumber	10	nas request
lcp no peer mrru	10	nas request
lcp no peer mru	10	nas request
lcp no peer pfc	10	nas request
lcp peer terminate code rej	1	user request
lcp peer terminate term ack	1	user request
lcp peer terminate term req	1	user request
lcp peer terminate protocol reject	1	user request
lcp peer renegotiate rx conf ack	1	user request
lcp peer renegotiate rx conf nak	1	user request
lcp peer renegotiate rx conf rej	1	user request
lcp peer renegotiate rx conf req	1	user request
lcp tunnel disconnected	10	nas request
lcp tunnel failed	10	nas request
link interface no hardware	8	port error
lower interface attach failed	2	lost carrier
lower interface teardown	2	lost carrier
mpls admin disable	10	nas request
mpls link down	10	nas request

Table 57: Default PPP Mappings (continued)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
mpls max configure exceeded	10	nas request
mpls no service	10	nas request
mpls peer renegotiate rx conf ack	10	nas request
mpls peer renegotiate rx conf nak	10	nas request
mpls peer renegotiate rx conf rej	10	nas request
mpls peer renegotiate rx conf req	10	nas request
mpls peer terminate code rej	10	nas request
mpls peer terminate term ack	10	nas request
mpls peer terminate term req	10	nas request
mpls service disable	10	nas request
mpls stale stacking	10	nas request
network interface admin disable	6	admin reset
no bundle	10	nas request
no interface	8	port error
no link interface	8	port error
no ncps available	10	nas request
no network interface	10	nas request
no upper interface	9	nas error
osi admin disable	10	nas request
osi link down	10	nas request
osi max configure exceeded	10	nas request
osi no local align npdu	10	nas request
osi no peer align npdu	10	nas request
osi no service	10	nas request
osi peer renegotiate rx conf ack	10	nas request
osi peer renegotiate rx conf nak	10	nas request
osi peer renegotiate rx conf rej	10	nas request
osi peer renegotiate rx conf req	10	nas request
osi peer terminate code rej	10	nas request
osi peer terminate term ack	10	nas request
osi peer terminate term req	10	nas request
osi service disable	10	nas request
osi stale stacking	10	nas request

RADIUS Client Terminate Reasons

[Table 58](#) lists the default RADIUS client terminate mappings. The table indicates the supported RADIUS client terminate reasons and the RADIUS Acct-Terminate-Cause attributes they are mapped to by default.

Table 58: Default RADIUS Client Mappings

RADIUS Client Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
no-acct-server	10	nas request
system-reboot	10	nas request
virtual-router-deletion	10	nas request

Index

Numerics

- 10-Gigabit Ethernet interfaces
 - specifying an interface 441

A

AAA (authentication, authorization, accounting)

- DSL Forum VSAs 136, 171
- EAP authentication 18
- failure, notifying RADIUS of 82
- L2TP tunnel switch profiles, applying 266, 267
- overview 3, 198
- services
 - accounting 198
 - and TACACS + 197
 - authentication 198, 199
 - authorization 198
 - overview 198

aaa commands

- aaa accounting acct-stop on-aaa-failure 82
- aaa accounting acct-stop on-access-deny 82
- aaa accounting broadcast 23
- aaa accounting commands 204
- aaa accounting default 23
- aaa accounting duplication 24
- aaa accounting exec 204
- aaa accounting immediate-update 24
- aaa accounting interval 25
- aaa accounting statistics 25
- aaa accounting suppress null-username 205
- aaa accounting tacacs + 206
- aaa accounting vr-group 25
- aaa authentication default 26, 40
- aaa authentication enable default 199, 205
- aaa authentication login 205
- aaa delimiter 12
- aaa dns primary 48
- aaa dns secondary 48, 49
- aaa domain-map 7, 9, 15, 228
- aaa duplicate-address-check 26
- aaa intf-desc-format include 160
- aaa local database 40
- aaa local select database 41
- aaa local username 41
- aaa new-model 199, 206
- aaa parse-direction 13

- aaa parse-order 13
- aaa profile 61, 63, 64, 73
- aaa route-download 67
- aaa route-download now 68
- aaa route-download suspend 68
- aaa subscriber limit per-port 81
- aaa subscriber limit per-vr 81
- aaa timeout 80
- aaa tunnel assignment-id-format 228
- aaa tunnel calling-number-format 223
- aaa tunnel calling-number-format fallback 223
- aaa tunnel client-name 229
- aaa tunnel ignore 229
- aaa tunnel nas-port-method 229
- aaa tunnel password 230
- aaa tunnel switch-profile 269
- aaa tunnel tx-connect-speed-method 278
- aaa tunnel-group 229
- aaa virtual-router 27
- aaa wins primary 49
- aaa wins secondary 49
- See also* show aaa commands
- AAA default tunnel parameters
 - L2TP transmit connect speed 277
- AAA domain maps
 - L2TP transmit connect speed 274
- AAA LLID (logical line identifier)
 - configuration steps 72
 - how it works 70
 - monitoring 93, 97, 109, 110
 - preauthentication considerations 72
 - RADIUS attributes in preauthentication
 - request 71
 - troubleshooting 75
 - using to track subscribers 69
- AAA logical line identifier (LLID). *See* AAA LLID 69
- AAA profile commands
 - aaa profile 63, 64
 - allow 61
 - deny 61
 - nas-port-type atm 63
 - nas-port-type ethernet 64
 - ppp aaa-profile 62, 74
 - service-description 65
 - translate 62

AAA profiles	57	agent-circuit-id	
allowing or denying domain names	58	including in Calling Number AVP	221
configuring	57	including in PPPoE remote circuit ID format	321
creating domain name aliases	59	agent-remote-id	
manually setting NAS-Port-Type	63	including in Calling Number AVP	221
setting Service-Description	64	including in PPPoE remote circuit ID format	321
AAA tunnel groups		allow command	61
L2TP transmit connect speed	275	Ascend-Num-In-Multilink (RADIUS attribute 188) ...	162
Access-Accept messages	125	ATM (Asynchronous Transfer Mode)	
Access-Challenge messages	126, 137	E320 routers	423
Access-Reject messages	126, 137	atm commands	
Access-Request messages	125	atm	76
DSL Forum VSAs	136, 171	atm pvc	440
accounting		ATM subinterface	
broadcast	19	configuring multiple clients	56, 57
configuring servers	16	configuring single clients	55, 56
configuring TACACS +	197	attribute value pair. <i>See</i> AVP	
description	3	audience for documentation	xvii
duplicate	19	authentication	
server access	17	AAA overview	198
server request processing limit	17	configuring servers	16
SNMP traps	33	configuring TACACS +	197
specifying methods	17	description	3
TACACS +	199	EAP	18
accounting statistics		preauthenticating users	8
tunneled PPP session	279	redirected authentication	8
Acct-Authentic (RADIUS attribute 45)	153	server access	17
Acct-Delay-Time (RADIUS attribute 41)	151	server request processing limit	17
Acct-Input-Gigapackets (RADIUS attribute 26-35) ...	166	SNMP traps	33
Acct-Input-Gigawords (RADIUS attribute 52)	154	specifying methods	17
Acct-Link-Count (RADIUS attribute 51)	154	authentication and accounting servers	
Acct-Multi-Session-Id (RADIUS attribute 50)	153	configuring	16
Acct-Off messages	131	authentication login, TACACS +	198
Acct-On messages	131	authentication, authorization, accounting. <i>See</i> AAA	
Acct-Output-Gigapackets		authorization	
(RADIUS attribute 26-36)	166	AAA overview	198
Acct-Session-ID (RADIUS attribute 44)	470, 475	description	3
Acct-Session-Id (RADIUS attribute 44)	152	TACACS +	199
Acct-Start messages	131	authorization change command	182
DSL Forum VSAs	136, 171	AVP (attribute value pair)	213
Acct-Stop messages	131	Bearer Type (AVP 18)	
DSL Forum VSAs	136, 171	relaying in L2TP tunnel-switched	
Acct-Terminate-Cause (RADIUS attribute 49)	153	network	264, 266
Acct-Tunnel-Connection (RADIUS attribute 68)	158	Calling Number (AVP 22)	
Activate-Service (RADIUS attribute 26-65)	469	formatting and preventing in	
address command, L2TP	230	ICRQ packets	220
address pool		relaying in L2TP tunnel-switched	
mapping to domain name	53	network	264, 266
ranges	50	Cisco NAS Port Info (AVP 100)	
address-pool-name command	53	relaying in L2TP tunnel-switched	
agent circuit ID (suboption 1)	328	network	264, 266
agent remote ID (suboption 2)	328	Transmit (TX) Speed (AVP 24)	
		reporting transmit connect speed in	270
		avp command	266

B

- backoff algorithm 32
 - baseline commands
 - baseline aaa 87
 - baseline aaa route-download 87
 - baseline cops 87
 - baseline dhcp relay 372
 - baseline dhcp server 372
 - baseline dhcp-local 373
 - baseline dhcpv6-local 373
 - baseline ip dhcp-external 372
 - baseline ip http 498
 - baseline local pool 87
 - baseline radius 87
 - baseline radius dynamic-request 183
 - baseline radius relay 193
 - baseline ssc 87
 - baseline tacacs 208
 - Bearer Type AVP
 - relaying in L2TP tunnel-switched network 264, 266
 - BOOTP (bootstrap protocol) 318
 - bootstrap protocol. *See* BOOTP
 - B-RAS applications
 - AAA profiles 57
 - allowing or denying domain names 58
 - client to server interaction 16
 - configuring
 - authentication and accounting servers 16
 - B-RAS license 6
 - DHCP features 314
 - IP addresses for remote clients 3
 - local address servers 49
 - name server addresses 47
 - SDX client 82
 - timeout 80
 - UDP checksums 21
 - creating an IP interface 55
 - creating domain name aliases 59
 - DHCP (Dynamic Host Configuration Protocol)
 - proxy client and server 3
 - IP hinting 9
 - limiting active subscribers 81
 - local address server 3
 - manually setting NAS-Port-Type 63
 - mapping address pool to domain 53
 - mapping user domain names to a virtual router 7
 - mapping user requests
 - without a valid domain name 7
 - without configured domain name 7
 - monitoring 88
 - multiple clients per ATM subinterface 56
 - overview 2
 - preauthenticating users 8
 - protocol support 4
 - redirected authentication 8
 - references 125, 525
 - SDX client. *See* SDX software
 - setting Service-Description 64
 - single clients per ATM subinterface 55
 - SNMP traps 33
 - specifying a single name for a domain 15
 - system log messages 33
 - virtual router 7
 - B-RAS licenses
 - configuring 6
 - bridged Ethernet and dynamic subscriber interfaces 436
 - Broadband Remote Access Server. *See* B-RAS
 - applications
 - broadcast AAA accounting 19
 - configuring 20
 - broadcast flag, DHCP
 - controlling transmission of DHCP reply packets 322
 - interaction with layer 2 unicast transmission method 323
 - bundled session commands
 - bundled-group-id 246
 - bundled-group-id-overrides-mlppp-ed 246
 - bundled sessions 244
- C**
- cable modem DHCP relay 370
 - cable modem networks 420
 - Called-Station-Id (RADIUS attribute 30) 144
 - Calling Number AVP
 - descriptive formats 221
 - fixed format 221
 - fixed format configuration 222
 - formatting in L2TP ICRQ packets 220
 - including agent-circuit-id and agent-remote-id 221
 - preventing in L2TP ICRQ packets 220
 - relaying in L2TP tunnel-switched network 264, 266
 - Calling-Station-Id (RADIUS attribute 31) 144
 - including IOA number in format 145
 - captive portal. *See* guided entrance
 - Change-of-Authorization-Request messages 126
 - Cisco NAS Port Info AVP
 - relaying in L2TP tunnel-switched network 264, 266
 - Class (RADIUS attribute 25) 144
 - clear ip commands
 - clear ip dhcp-local binding 359
 - clear ip routes download 68

CLI (command-line interface)	
authorization and authentication messages	137
commands used to modify	
RADIUS attributes	138
client-name command	230
CoA-Request messages	126
guided entrance	494
Service Manager	494
command-line interface. <i>See</i> CLI	
Common Open Policy Service. <i>See</i> COPS	
Connect-Info (RADIUS attribute 77)	158
conventions defined	
icons	xviii
text and syntax	xix
COPS	
(Common Open Policy Service)	82, 86, 88, 102, 103
COPS-PR (COPS usage for policy provisioning)	82
customer support, contacting	xxiv
D	
Deactivate-Service	
(RADIUS attribute 26-66)	469, 472, 494
deadtime command	27
default domain name	7
default-router command	440
default-upper-type mlppp command	241
deny command	61
descriptive formats	
Calling Number AVP	221
destination	
changing	213
DHCP (Dynamic Host Configuration Protocol)	
access model	316
configuring BOOTP Relay	318
configuring DHCP relay	318
configuring DHCP relay proxy	337, 338
configuring proxy client and server	316
features	55
giaddr	318, 341
option 82	318, 319, 321, 326, 327, 331, 332, 355, 356
overview	55, 313
per-interface logging	371
PPPoE remote circuit ID	321
source IP address	318
trust-all	318
DHCP access model	
configuring	314
DHCP address binding	
clearing	359
DHCP broadcast flag	
controlling transmission of DHCP	
reply packets	322
interaction with layer 2 unicast transmission	
method	323
DHCP client bindings	
deleting	370
managing	370
viewing	370
DHCP commands	
ip auto-detect ip-subscriber	443
ip dhcp-capture	371
ip inactivity-timer	443
set ip interface-profile	409
set ip source-prefix	410
<i>See also</i> show dhcp commands	
dhcp delete-binding command	371
DHCP external server	
and DHCP relay proxy	363
configuring	363, 365, 403
monitoring	384
overview	363
DHCP local server	
configuring	346
configuring authentication	355
equal-access mode	341
address allocation	341
configuring	346
connection process	342
local pool selection	341
overview	341
SDX (Service Deployment System)	314
linking local address pools	344
local address pool group	344, 351, 392
local pool selection, equal-access	341
using domain name	341
using framed IP address	341
using giaddr	341
using pool name	341
local pool selection, standalone	343
using giaddr	343
using received interface IP address	343
logging information	
modes	340
monitoring	387, 388
overview	339
RADIUS accounting support for	340
standalone mode	
address allocation	343, 355
authentication	355
configuring	346
local pool selection	343
overview	343
DHCP local server commands	
ip dhcp-local	351
DHCP local server traps	
logging	345
DHCP logging	383

- DHCP option 60
 - cable modem DHCP relay 370
- DHCP option 60 strings 367, 368
- DHCP options and RADIUS
 - configuring 314
- DHCP packets
 - logging 383
- DHCP per-interface information
 - logging 371
- DHCP pool commands
 - default-router 348, 440
 - dns-server 348
 - domain-name 349
 - grace-period 354
 - ip dhcp-local pool 443
 - lease 351
 - link 351
 - netbios-name-server 351
 - netbios-node-type 352
 - network 352
 - reserve 352
 - server-address 352
 - snmpTrap 353
 - use-release-grace-period 354
 - warning 353
- DHCP proxy client
 - configuring 316
- DHCP relay
 - configuring 318
 - creating 324
 - in same VR as dynamic
 - subscriber interfaces 425
 - logging information 321
 - preventing host route installation 319
 - removing 324
 - spoofed giaddr 319
 - spoofed relay agent option 319
- DHCP relay agent information option
 - agent circuit ID (suboption 1) 328
 - agent remote ID (suboption 2) 328
 - vendor-specific (suboption 9) 328
- DHCP relay and BOOTP relay
 - configuring 318
- DHCP relay proxy
 - best offer 338
 - bound clients and address renewals 324
 - configuring 337
 - first offer 338
- DHCP server
 - dynamic subscriber interfaces 424
- DHCP vendor class identifier option 367
- dhcp-external delete-binding command 365
- DHCP-GI-Address (RADIUS attribute 26-57) 168
- DHCP-MAC-Address (RADIUS attribute 26-56) 168
- DHCP-Options (RADIUS attribute 26-55) 168
- DHCPv6 local server
 - configuring 361
 - IPv6 340
- diald number identification service. *See* DNIS
- digital subscriber line access multiplexers. *See* DSLAMs
- digital subscriber lines. *See* DSLs
- disable proxy lcp command 241
- Disconnect-Cause (RADIUS attribute 26-51) 167
- Disconnect-Request messages 126
- DNIS (diald number identification service) 8, 240
- DNS (Domain Name System)
 - assigning IP addresses 92
 - overview 47
- documentation set, E-series and JUNOS xx
 - comments on xxiv
 - obtaining xxiii
- domain command 405
- Domain Name System. *See* DNS
- domain names
 - allowing or denying 58
 - configuring 10
 - default 7
 - mapping to virtual routers 7, 90, 97, 280
 - mapping user requests without domain name 7
 - none 7
 - specifying single name for users 15
 - stripping domain name 12
 - using aliases 59
 - using delimiters other than @ 11
 - using either domain or realm as
 - domain name 11
 - using realm name as domain name 11
- DSL Forum VSAs
 - controlling inclusion of 171
 - descriptions 523
 - in AAA access and accounting messages 136
- DSLAMs (digital subscriber line access multiplexers) 2
- DSLs (digital subscriber lines) 2
- duplicate AAA accounting 19
 - configuring 20
- Dynamic Host Configuration Protocol. *See* DHCP
- dynamic IP interfaces 75
- dynamic subscriber interfaces
 - commands 440
 - configuring 424, 433
 - DHCP server 424
 - framed routes 426
 - GRE tunnel configuration 437
 - in same VR as DHCP relay 425
 - IP over bridged Ethernet configuration 436

IP over Ethernet configuration	433
IP over VLAN over Ethernet configuration	434
monitoring	445
overview	424
packet detection	426
E	
E120 routers	xviii, xx
E320 routers	xviii, xx
ATM interfaces	423
EAP	18
EAP-Message (RADIUS attribute 79)	19
Egress-Policy-Name (RADIUS attribute 26-11)	164
enable proxy authenticate command	241
encapsulation commands	
encapsulation bridge1483	440
encapsulation vlan	440
endpoint discriminator	244
equal-access DHCP local server	341
ERX-14xx models	xviii
ERX-310 router	xviii
ERX-7xx models	xviii
E-series and JUNOS documentation set	xx
comments on	xxiv
obtaining	xxiii
E-series router models	xviii
Ethernet	
configuring dynamic subscriber interfaces	433
Ethernet interfaces	
commands	
interface tenGigabitEthernet	441
Event-Timestamp (RADIUS attribute 55)	155
EAP	18, 19, 18
F	
fixed format	
Calling Number AVP	221
fragmentation	
and reassembly	215
packet	215
framed routes	
dynamic subscriber interfaces	426
Framed-Compression (RADIUS attribute 13)	143
Framed-IP-Address (RADIUS attribute 8)	142
Framed-IP-Netmask (RADIUS attribute 9)	143
Framed-MTU (RADIUS attribute 12)	19
G	
giaddr	318, 341
GRE (Generic Routing Encapsulation) tunnels	
dynamic subscriber interfaces	426, 437
guided entrance	450, 492
CoA-Request messages	494
H	
HTTP local server	493, 495
guided entrance service	495
Service Manager	495
I	
I/O adapters. <i>See</i> IOAs	
icons defined, notice	xviii
identification command	230
idle timeout for B-RAS	
configuring	80
idle timeout, range for	80
include commands	
include circuit-id	405
include dhcp-option 82	405
include hostname	405
include ip-address	406
include mac-address	406
include virtual-router-name	406
Ingress-Policy-Name (RADIUS attribute 26-10)	163
interface commands	
interface atm	441
interface fastEthernet	441
interface gigabitEthernet	441
interface ip	431
interface loopback	442
interface tenGigabitEthernet	441
Interface-Desc (RADIUS attribute 26-63)	169
interfaces	
configuring for DHCP local server	345
moving	419
Interim-Acct messages	131
DSL Forum VSAs	136, 171
Internet Protocol. <i>See</i> IP	
IOAs	
including in RADIUS Calling-Station-Id format	145
IP	
hinting	9
IP addresses	
assigning to name servers	47, 92
configuring for remote client	3
ip commands	
clear ip demux	404
ip address	442
ip address-pool dhcp	53, 317
ip address-pool local	53
ip auto-configure ip-subscriber	406, 425, 442
ip auto-detect ip-subscriber	407
ip demux-type	431
ip destination-prefix	407, 431, 432
ip dhcp-local pool	443
ip inactivity-timer	407
ip local alias	53
ip local pool	54

- ip local pool snmpTrap 54
- ip local pool warning 54
- ip local shared-pool 54
- ip route-map ip-subscriber 408
- ip service-profile 408
- ip share-interface 432
- ip share-nexthop 432
- ip source-prefix 409, 426, 433, 443
- ip unnumbered 444
- ip use-framed-routes ip-subscriber 409, 426, 444
- ip-hint 9
- ip dhcp-external commands
 - ip dhcp-external auto-configure 366
 - ip dhcp-external disregard-giaddr-next-hop 366
 - ip dhcp-external server-address 366
 - ip dhcp-external server-sync 367
 - See also* show ip dhcp-external commands
- ip dhcp-local auth domain command 356
- ip dhcp-local auth include command 356
- ip dhcp-local auth password 357
- ip dhcp-local auth user-prefix command 357
- ip dhcp-local commands
 - ip dhcp-local auto-configure
 - agent-circuit-identifier 349
 - ip dhcp-local excluded-address 349
 - ip dhcp-local inhibit-roaming 358
 - ip dhcp-local limit 350
 - ip dhcp-local pool 350
 - ip dhcp-local unique-client-ids 358
- ip dhcp-server commands
 - ip dhcp-server 317
- ip http commands
 - ip http 496
 - ip http access-class 496
 - ip http max-connection-time 496
 - ip http port 497
 - ip http redirecturl 497
 - ip http same-host-limit 497
 - ip http server 497
- IP interfaces
 - creating 431
- IP interfaces that support PPP clients
 - configuring 55
- IP spoofing
 - preventing 420
- ipv6 commands
 - ipv6 virtual-router 9
 - ipv6-local-interface 9
- IPv6 DHCP local server 340
 - monitoring 396
- ipv6 dhcpv6-local commands
 - ipv6 dhcpv6-local delegated-prefix 362
 - ipv6 dhcpv6-local dns-domain-search 362
 - ipv6 dhcpv6-local dns-server 362
 - ipv6 dhcpv6-local prefix-lifetime 362
- J**
 - JUNOS software CD xxii
- K**
 - key command 27, 73, 182, 192
- L**
 - L2C-Down-Stream-Data (RADIUS attribute 26-93) .. 170
 - L2C-Information (RADIUS attribute 26-81) 170
 - L2C-Up-Stream-Data (RADIUS attribute 26-92) 170
 - L2TP (Layer 2 Tunneling Protocol)
 - defining 212
 - high availability considerations 218
 - implementation 213
 - license 218
 - managing 250
 - monitoring 280
 - peer resynchronization 259
 - sessions supported 218
 - silent failover 260
 - tunnel selection 247
 - tunnel switch profiles 262
 - L2TP access concentrator. *See* LAC
 - l2tp commands
 - disconnect-cause 254
 - failover-resync 260
 - l2tp checksum 219
 - l2tp destination lockout-test 237
 - l2tp destination lockout-timeout 237
 - l2tp destination profile 242
 - l2tp destruct-timeout 220
 - l2tp disable calling-number avp 224
 - l2tp disable challenge 231
 - l2tp disconnect-cause 255
 - l2tp drain 251
 - l2tp drain destination 251
 - l2tp drain tunnel 251
 - l2tp failover-resync 261
 - l2tp fail-over-within-preference 249
 - l2tp ignore-receive-data-sequencing 231
 - l2tp ignore-transmit-address-change 238
 - l2tp reject-transmit-address-change 239
 - l2tp retransmission 220, 252
 - l2tp short-drain-timeout 252
 - l2tp shutdown 252
 - l2tp shutdown destination 253
 - l2tp shutdown session 253
 - l2tp shutdown tunnel 253

l2tp switch-profile	266	L2TP transmit connect speed	
l2tp tunnel default-receive-window	257	and Transmit (TX) Speed AVP 24	270
l2tp tunnel idle-timeout	250	calculation methods	
l2tp tunnel test	250	actual	272
l2tp tunnel-switching	247, 265	dynamic layer 2	271
l2tp unlock destination	237	examples	272
l2tp unlock-test destination	238	how to configure	270
max-sessions command	242	QoS	271
<i>See also</i> show l2tp commands		static layer 2	271
L2TP dial-out		configuring	
before configuring	303	AAA default tunnel parameters	277
configuring	303	AAA domain maps	274
dial-out process	297	AAA tunnel groups	275
monitoring	305	RADIUS	276
network model	296	monitoring	90, 280, 281
operational states	298	reporting considerations	273
outgoing call setup details	300	L2TP tunnel switch profiles	
Access-Accept message	301	applying default profile	269
Access-Request message	300	applying through AAA domain maps	266
mutual authentication	302	applying through AAA tunnel groups	267
outgoing call successful	301	applying through RADIUS	268
route installation	302	AVP relay, configuring	264, 266
overview	295	configuration guidelines	263
references	302	configuring	265
route	296	how to apply	263, 264
session	296	monitoring	290
target	296	LAC (L2TP access concentrator)	213
trigger	296	before configuring	219
L2TP dial-out commands		configuring	219
l2tp dial-out connecting-timer-value	304	configuring receive window size (RWS)	257
l2tp dial-out dormant-timer-value	304	function	212
l2tp dial-out max-buffered-triggers	304	sequence of events	214
l2tp dial-out session delete	304	Layer 2 Tunneling Protocol. <i>See</i> L2TP	
l2tp dial-out session reset	305	license commands	
l2tp dial-out target	305	license b-ras	6
<i>See also</i> show l2tp dial-out commands		license l2tp-session	218
L2TP network server. <i>See</i> LNS		license service-manager	466
L2TP RWS (receive window size)		<i>See also</i> show license commands	
configuring global default	256	licenses	
configuring on LAC	257	B-RAS	6
configuring on LNS	258	L2TP	218
l2tp tunnel default-receive-window		Service Manager	466
command	257	line command	207
overview	255	LLID (logical line identifier)	
receive-window command (for LAC)	258	configuration steps	72
receive-window command (for LNS)	259	how it works	70
show l2tp command	91, 283	monitoring	93, 97, 109, 110
show l2tp destination profile command	285	preauthentication considerations	72
l2tp rx-connect-speed-when-equal command	235	RADIUS attributes in preauthentication	
		request	71
		troubleshooting	75
		using to track subscribers	69

LNS (L2TP network server)	213
before configuring	219
configuring	239
configuring receive window size (RWS)	258
installing multiple tunnel-service modules	244
modules supported	246
sequence of events	214
local address pool	
alias names	50
mapping to domain name	53
ranges	50
local address server	49
alias names	50
configuring	49, 52
pool ranges	50
shared local address pools	51
SNMP thresholds	52
local authentication commands	
aaa authentication default	40
aaa local database	40
aaa local select database	41
aaa local username	41
ip-address	41
ip-address-pool	42
operational-virtual-router	42
password	42
secret	43
username	43
local host command	242
local-interface command	10
logging. <i>See specific feature, product, or protocol</i>	
logical line identifier, AAA. <i>See LLID</i>	69
login authentication command	207
logout subscribers name command	28, 359

M

MAC (media access control) addresses	
duplicate	344, 345
macros	
service definitions	450
Service Manager statistics	486
manuals, E-series and JUNOS	xx
comments on	xxiv
max sessions command, L2TP	231
max-sessions command	28, 249
MBS (RADIUS attribute 26-17)	165
medium ipv4 command	231
merging policies	
naming conventions	457
Message-Authenticator (RADIUS attribute 80)	19
MIBs (Management Information Bases)	xxiii
MLPPP Bundle Name (RADIUS attribute 26-62)	169

models	
E120	xviii
E320	xviii
ERX-14xx	xviii
ERX-310	xviii
ERX-7xx	xviii
monitoring. <i>See specific feature, product, or protocol</i>	
mutex service	450, 473

N

name server addresses	
configuring	47, 92
naming conventions	
merged policies	457
NAS (network access server)	197, 198
NAS-Identifier (RADIUS attribute 32)	149
NAS-IP-Address (RADIUS attribute 4)	138
NAS-Port (RADIUS attribute 5)	139
NAS-Port-Id (RADIUS attribute 87)	160
NAS-Port-Type (RADIUS attribute 61)	155
nas-port-type atm command	63
NAS-Port-Type attribute, manually setting	63
nas-port-type ethernet command	64
network access server. <i>See NAS</i>	
network commands	
network	444
no radius client command	29
none domain name	7
non-PPP equal access	
configuration example	360
requirements	341
notice icons defined	xviii

O

operational states, L2TP	298
chassis	298
sessions	299
targets	298
virtual router	298
option 60 strings	367, 368
option 82	318, 319, 326, 327, 331, 332, 355, 356
Output-Gigawords (RADIUS attribute 53)	154
override-user command	15, 16

P

packet detection	
dynamic subscriber interfaces	426
packet fragmentation	215
packet mirroring	179
packets	
demultiplexing	418
transmitting	212
password command	232, 409
PCR (RADIUS attribute 26-15)	165

peer	213
peer resynchronization	259
persistent tunnels, creating	250
PIB (Policy Information Base)	83
platform considerations	
PPP	201
Point-to-Point Protocol. <i>See</i> PPP	
Policy Information Base. <i>See</i> PIB	
policy management	
on subscriber interfaces	420
PPP (Point-to-Point Protocol)	
accounting statistics for tunneled sessions	279
B-RAS service support	4
platform considerations	201
ppp commands	
ppp aaa-profile	62, 74
PPPoE remote circuit ID	321
Pppoe-Description (RADIUS attribute 26-24)	166
pre-authenticate command	74
preauthentication	
AAA LLID	70
B-RAS users	8
preference	247
preference command	232
primary authentication/accounting	
RADIUS server	21, 66
primary IP interface	418
privilege authentication, TACACS +	199
profile commands	
profile	458

Q

QoS (quality of service)	
calculation method for L2TP transmit connect	
speed	271
on subscriber interfaces	420
QoS commands	
qos-parameter	460
qos-profile	459

R

RADIUS (Remote Authentication Dial-In User Service)	
AAA failure	82
accounting methods	17
attribute descriptions	19, 124, 511
attributes supported	511
authentication and accounting servers	16
authentication methods	17, 18
Calling-Station-Id formats supported	145
change of authority messages	175
CLI AAA messages	137
client to server interaction	16
configuring servers	16
description	123, 124

direct server access	17
disconnect messages	175
EAP authentication	18
IETF attributes supported	512
Juniper Networks VSAs supported	517
L2TP transmit connect speed	276
L2TP tunnel switch profiles, applying	268
message types supported	125
RADIUS dynamic-request server	175
round-robin server access	17
server access	17
server request processing limit	17
Service Manager attributes	469
Service Manager tags	471
services	124
SNMP traps	33
system log messages	33
traffic shaping for PPP over ATM interfaces	76
VSAs (vendor-specific attributes)	
for dynamic IP interfaces	75
formats	517
radius commands	
radius acct-session-id-format	152, 514
radius algorithm	17, 29
radius calling-station-delimiter	147, 513
radius calling-station-format	145, 513
radius client	29
radius connect-info-format	158
radius disconnect client	182
radius dsl-port-type	155, 156, 515
radius dynamic-request server	183
radius ethernet-port-type	155, 156, 515
radius ignore atm-mbs	165
radius ignore atm-pcr	165
radius ignore atm-scr	165
radius ignore atm-service-category	164
radius ignore egress-policy-name	164
radius ignore framed-ip-netmask	143
radius ignore ingress-policy-name	163
radius ignore virtual-router	163
radius include access-loop-parameters	170
radius include acct-authentic	153
radius include acct-delay-time	151
radius include acct-link-count	154
radius include acct-multi-session-id	153
radius include acct-session-id	152
radius include acct-session-id access-request	514
radius include acct-terminate-cause	79, 153
radius include acct-tunnel-connection	158
radius include ascend-num-in-multilink	162
radius include called-station-id	144
radius include calling-station-id	148
radius include class	144
radius include connect-info	159

- radius include dhcp-gi-address 168
- radius include dhcp-mac-address 168
- radius include dhcp-options 168
- radius include dsl-forum-attributes 172
- radius include egress-policy-name 164
- radius include event-timestamp 155
- radius include framed-compression 143
- radius include framed-ip-add acct-start 512
- radius include framed-ip-addr 142
- radius include framed-ip-netmask 143
- radius include ingress-policy-name 163
- radius include input-gigapkts 166
- radius include input-gigawords 154
- radius include interface-description 169
- radius include l2c-downstream-data 170
- radius include l2c-upstream-data 170
- radius include
 - l2tp-ppp-disconnect-cause 167, 255
- radius include mlppp-bundle-name 169
- radius include nas-identifier 149
- radius include nas-port 139
- radius include nas-port-id 160
- radius include nas-port-type 156
- radius include output-gigapkts 166
- radius include output-gigawords 154
- radius include pppoe-description 166
- radius include profile-service-description 167
- radius include tunnel-assignment-id 159
- radius include tunnel-client-auth-id 161
- radius include tunnel-client-endpoint 157
- radius include tunnel-interface-id 167
- radius include tunnel-medium-type 157
- radius include tunnel-preference 160
- radius include tunnel-server-attributes 162
- radius include tunnel-server-auth-id 162
- radius include tunnel-server-endpoint 157
- radius include tunnel-type 156
- radius include
 - framed-ip-netmask 79, 143, 151, 153
- radius nas-identifier 149
- radius nas-port-format 140, 512
- radius nas-port-format extended atm 140
- radius nas-port-format extended ethernet 140
- radius override calling-station-id
 - remote-circuit-id 148
- radius override nas-info 29, 139, 149
- radius override nas-ip-addr
 - tunnel-client-endpoint 138
- radius override nas-port-id remote-circuit-id 161
- radius pppoe nas-port-format unique 141, 512
- radius pre-authentication server 74
- radius relay server 192
- radius relay udp-checksum 192
- radius remote-circuit-id-delimiter 150
- radius remote-circuit-id-format 150
- radius rollover-on-reject 29
- radius route-download server 69
- radius server 30
- radius trap acct-server-not-responding 35
- radius trap acct-server-responding 35
- radius trap auth-server-not-responding 36
- radius trap auth-server-responding 36
- radius trap no-acct-server-responding 36
- radius trap no-auth-server-responding 36
- radius tunnel-accounting 30
- radius udp-checksum 30
- radius update-source-addr 30, 124, 512
- radius vlan nas-port-format stacked 512
- See also* show radius commands
- RADIUS dynamic-request server
 - change of authorization messages 180
 - disconnect messages 177
 - how it works 177
 - message exchange 178, 180
 - monitoring 183
 - overview 175
 - qualifications for disconnect 178
 - security and authentication 179
 - Service Manager 493
- RADIUS relay server
 - configuring 191
 - monitoring 193
- RADIUS route-download server 65
 - configuring 66
 - format of routes 65
 - how it works 65, 66
 - per chassis 65
 - supported attributes 65
- RADIUS-initiated change of authorization
 - qualifications for disconnect 181
- RADIUS-initiated disconnect
 - configuring 179, 181
 - references 177
 - sample network 176
 - security and authentication 181
- realm names
 - configuring 10
 - usage 10
- Receive speed AVP 283
- receive window size (RWS). *See* L2TP RWS
- receive-window command 232, 258, 259
- redirected authentication 8
- release notes xxii
- remote access
 - monitoring 88
- remote access (B-RAS). *See* B-RAS applications
- Remote Authentication Dial-In User Service. *See* RADIUS

remote clients, IP addresses for.....	3
remote host command	243
remote system	213
retransmit command	31
router-name command.....	10, 233
RX speed AVP	234

S

SCR (RADIUS attribute 26-16)	165
SDX (Service Deployment System)	
application	
configuring.....	360
client	
configuring.....	82, 84
SDX (Service Deployment System)	
software	102, 103, 314, 360
configuring the client.....	82
monitoring the client	113, 115
server-name command	233
service commands	
service dhcp-external	367
service dhcp-local.....	352, 444
service dhcp-local authenticate	357
service dhcpv6-local	361
service-description	65
service definition	450, 451, 453
copying.....	456
creating	453, 454
installing.....	456, 457
modifying.....	456
specifying QoS profiles.....	458
uninstalling	456
service definitions	
modifying QoS configurations.....	461
specifying parameter instances	459
Service Deployment System. <i>See</i> SDX software	
service instance	451
Service Manager	
CLI support	466
CoA-Request messages	493, 494
configuring	
Service Manager license.....	466
deactivating	471
setting thresholds.....	472
guided entrance	450, 492, 494
license sessions	466
macros.....	450
multiple services	473
mutex service	450, 473
overview.....	450
parameter values	469
preprovisioning services	477, 480

QoS

considerations	465
modifying configurations of	461
referencing configurations of	458
removing references of	464
RADIUS dynamic-request server	493
RADIUS support	466
RADIUS tags.....	471
service definition.....	450, 451, 453
parameters.....	478
service instance.....	451
service session.....	451
forcing deactivation	484
profiles	480
service session profiles.....	451
session thresholds.....	485
statistics.....	470, 481, 482, 485
macro command.....	486
using RADIUS	487
using the CLI.....	487
subscriber session ID	484
subscriber sessions	479
supported platforms	451
tasks.....	452
testing services	477
Service Manager commands	
no service-management	
owner-session force.....	484
no service-management	
subscriber-session force.....	484
service-management install	457
service-management owner-session.....	478
service-management service-session-profile	482
service-management subscriber-session	
service-session	479
statistics.....	482
time.....	482
volume.....	483
Service Manager license	
configuring.....	466
service session	451
Service-Category (RADIUS attribute 26-14).....	164
Service-Description (RADIUS attribute 26-53)	167
setting.....	64
Service-Session (RADIUS attribute 26-83)	470, 475
Service-Stats (RADIUS attribute 26-69).....	470, 487
Service-Timeout (RADIUS attribute 26-68).....	469, 472
Service-Volume (RADIUS attribute 26-67)	469, 472
session	213
session timeout	
configuring.....	80
interpreting default value	81
range for.....	80
sessions, L2TP.....	218

Session-Timeout (RADIUS attribute 27)	19	show dhcp binding command	373
set dhcp relay command	324	show dhcp commands	
set dhcp relay commands		show dhcp relay	375
set dhcp relay	324	show dhcp relay proxy statistics	379
set dhcp relay agent	331	show dhcp relay statistics	376
set dhcp relay agent sub-option	332	show dhcp server	380
set dhcp relay assign-giaddr-source-ip	325	show dhcp server statistics	381
set dhcp relay broadcast-flag-replies	322, 325	show dhcp summary command	382
set dhcp relay giaddr-selects-interface	325, 445	show dhcp vendor-option command	382
set dhcp relay layer2-unicast-replies	321, 326	show ip commands	
set dhcp relay options	326	show ip demux interface	445
set dhcp relay override	327	show ip local alias	105
set dhcp relay preserve-trusted-client-option	327	show ip local pool	105
set dhcp relay proxy	338	show ip local-pool statistics command	107
set dhcp relay trust-all	327	show ip service-profile	413
set dhcp relay proxy commands		show ip-subscriber	414, 446
set dhcp relay proxy	338	show ip dhcp-capture command	383
set dhcp relay proxy send-first-offer	339	show ip dhcp-external commands	
set dhcp relay proxy timeout	339	show ip dhcp-external binding	384
set dhcp vendor-option command	368	show ip dhcp-external client-id	384
shared IP interfaces	418	show ip dhcp-external configuration	385
shared local address pools	51	show ip dhcp-external statistics	385
shared tunnel-server ports	217, 244	show ip dhcp-local commands	
show aaa commands		show ip dhcp-local	386
show aaa accounting	89	show ip dhcp-local binding	387
show aaa accounting default	89	show ip dhcp-local duplicate-clients	388
show aaa accounting interval	89	show ip dhcp-local excluded	388
show aaa accounting vr-group	90	show ip dhcp-local limits	390
show aaa authentication default	90	show ip dhcp-local pool	391
show aaa delimiters	90	show ip dhcp-local reserved	393
show aaa domain-map	90, 280	show ip dhcp-local statistics	389, 393
show aaa duplicate-address-check	92	show ip dhcpv6-local commands	
show aaa intf-desc-format	161	show ip dhcpv6-local binding	396
show aaa model	92	show ip dhcpv6-local dns-domain-searchlist	396
show aaa name-servers	92	show ip dhcpv6-local dns-servers	396
show aaa profile	93	show ip dhcpv6-local prefix-lifetime	396
show aaa route-download routes	95	show ip dhcpv6-local statistics	397
show aaa route-download routes global	95	show ip http commands	
show aaa statistics	97	show ip http scalar	498
show aaa subscriber per-port-limit	98	show ip http server	498
show aaa subscriber per-vr-limit	98	show ip http statistics	499
show aaa timeout	99	show ip local shared-local command	107
show aaa tunnel-group	281	show l2tp commands	
show aaa tunnel-parameters	281	show l2tp	282
show radius route-download	93	show l2tp destination	284
show configuration commands		show l2tp destination lockout	285
show configuration category aaa		show l2tp destination profile	285
global-attributes	99	show l2tp destination summary	287
show configuration category aaa		show l2tp session	288
local-authentication	99	show l2tp session summary	289
show configuration category aaa		show l2tp switch-profile	290
server-attributes include-defaults	100	show l2tp tunnel	290
show cops info command	102	show l2tp tunnel summary	293
show cops statistics command	103		

show l2tp dial-out commands	
show l2tp dial-out	306
show l2tp dial-out session	310
show l2tp dial-out target	310
show l2tp dial-out virtual-router	311
show license commands	
show license b-ras	108
show license service-management	500
show profile commands	
show profile	500
show profile name	500
show qos commands	
show qos-parameter	501
show radius commands	
show radius accounting servers	109
show radius accounting statistics	110
show radius acct-session-id-format	152
show radius algorithm	108
show radius attributes-included	174
show radius authentication servers	109
show radius authentication statistics	110
show radius calling-station-delimiter	148
show radius calling-station-format	145, 148
show radius connect-info-format	159
show radius dsl-port-type	156
show radius dynamic-request servers	184
show radius dynamic-request statistics	184
show radius ethernet-port-type	156
show radius nas-identifier	150
show radius nas-port-format	142
show radius override	139, 148, 151, 161
show radius pppoe nas-port-format	142
show radius remote-circuit-id-delimiter	151
show radius remote-circuit-id-format	151
show radius rollover-on-reject	108
show radius route-download statistics	109
show radius servers	109, 184
show radius statistics	109, 110, 111, 184
show radius trap	112
show radius tunnel-accounting	113
show radius udp-checksum	113
show radius update-source-address	113
show radius vlan nas-port-format	142
show radius override	139
show radius relay commands	
show radius relay servers	193
show radius relay statistics	194
show radius relay udp-checksum	195
show service-management commands	
show service-management service-definition	503
show service-management summary	509
show service-management	
owner-session	504
show service-management	
service-session-profile	504
show service-management	
subscriber-session	506
show ssc commands	
show ssc info	113
show ssc statistics	115
show ssc version	116
show statistics tacacs command	209
show subscribers command	116
show tacacs commands	
show statistics tacacs	209
show tacacs	210
show terminate-code command	120
SNMP traps	
configuring for DHCP local servers	345
configuring for RADIUS servers	34
overview	33
software, installing or updating	xvii
source-address command	233
ssc commands	
ssc address	85
ssc enable	85
ssc protocol ipv6	85
ssc retryTimer	85, 86
ssc sourceAddress	86
ssc transportRouter	86
<i>See also</i> show ssc commands	
standalone DHCP local server	343
State (RADIUS attribute 24)	19
statistics	482
strip-domain command	14
subscriber disconnect command	183
subscriber interface commands	
set dhcp relay giaddr-selects-interface	325, 445
subscriber interfaces	
applications	420
commands	
configuring dynamic	440
configuring static	427
configuring	424
multicast routing protocols	420
policies and QoS	420
routing protocols	420
dynamic	433
GRE tunnel configuration	437
IP over bridged Ethernet configuration	436
IP over Ethernet configuration	433
IP over VLAN over Ethernet configuration	434
monitoring	445
overview	
dynamic	424
static	419
static	427

subscribers	
accounting messages	131
authorization and authentication messages	125
E-series routers	116
limiting active subscribers	81
preauthentication and AAA LLID	70
support, requesting	xxiv
switch-profile command	267, 268
system log messages	34

T

TACACS +	
AAA services	198
accounting	199
authentication login process	198
authorization	199
configuring	202
daemon	198
host	198
NAS (network access server)	197, 198
privilege authentication	199
TACACS + commands	
aaa accounting commands	204
aaa accounting exec	204
aaa accounting suppress null-username	205
aaa accounting tacacs +	206
aaa authentication enable default	199, 205
aaa authentication login	205
aaa new-model	199, 206
baseline tacacs	208
tacacs-server host	207
tacacs-server key	208
tacacs-server source-address	208
tacacs-server timeout	208
<i>See also show tacacs commands</i>	
TCP and TACACS +	197
technical support, requesting	xxiv
Terminal Access Controller Access	
Control System + . <i>See</i> TACACS +	
terminate-code command	80
test aaa command	31
text and syntax conventions defined	xix
timeout command	32
timeout, configuring for B-RAS applications	80
traffic shaping for PPP over ATM	76
translate command	62
transmit connect speed, L2TP. <i>See</i> L2TP transmit	
connect speed	
tunnel	
defined	212, 213
selection, L2TP	247
switching	246
tunnel commands, L2TP	
tunnel	234
tunnel group	234
tunnel password	243
tunnel group mode, mapping to L2TP tunnel	227
tunnel selection, L2TP	247
failover between preference levels	247
failover within preference levels	248
maximum sessions per tunnel	249
weighted load balancing	249
tunnel switch profiles, L2TP	
applying default profile	269
applying through AAA domain maps	266
applying through AAA tunnel groups	267
applying through RADIUS	268
AVP relay, configuring	264, 266
configuration guidelines	263
configuring	265
how to apply	263, 264
monitoring	290
Tunnel-Assignment-Id (RADIUS attribute 82)	159
Tunnel-Client-Auth-Id (RADIUS attribute 90)	161
Tunnel-Client-Endpoint (RADIUS attribute 66)	157
tunneled PPP session accounting statistics	279
Tunnel-Interface-Id (RADIUS attribute 26-44)	167
Tunnel-Medium-Type (RADIUS attribute 65)	157
Tunnel-Preference (RADIUS attribute 83)	160
tunnels, IP	
shared tunnel-server ports	217
tunnel-server ports	
shared	217
tunnel-server ports, shared	217
Tunnel-Server-Auth-Id (RADIUS attribute 91)	162
Tunnel-Server-Endpoint (RADIUS attribute 67)	157
tunnel-service modules	
installing multiple for LNS sessions	244
Tunnel-Type (RADIUS attribute 64)	156
tx-connect-speed-method command	275, 276
type command, L2TP	234

U

UDP (User Datagram Protocol)	
checksums	21, 23, 30, 113
udp-port command	32, 183, 193
user domain, mapping to L2TP tunnel	225
User-Name (RADIUS attribute 1)	8
user-name command	410
usernames and passwords from a domain	
configuring	15
user-prefix command	410

V

vendor class identifier option	367
vendor-specific (suboption 9)	328
vendor-specific attributes. <i>See</i> VSAs	
virtual routers	
mapping user domain names	7, 90, 97, 280
redirected authentication	8
Virtual-Router (RADIUS attribute 26-1)	163
vlan commands	
vlan id	445
VLANs (virtual local area networks)	
configuring dynamic subscriber interfaces	434
VPNs (virtual private networks)	
connecting subscribers	421
VSAs (vendor-specific attributes)	
DSL Forum	
controlling inclusion of	171
descriptions	523
in AAA access and accounting messages	136
for dynamic IP interfaces	75
formats	517

W

walled garden. <i>See</i> guided entrance	
Web access to E-series router	314
Windows Internet Name Service. <i>See</i> WINS	
WINS, assigning IP addresses	47, 49, 92