



---

# JunosE™ Software for E Series™ Broadband Services Routers

## Remote Access Services

Release

13.3.x



---

Published: 2012-09-24

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

Copyright © 2012, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

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

*JunosE™ Software for E Series™ Broadband Services Routers Remote Access Services*  
Release 13.3.x  
Copyright © 2012, Juniper Networks, Inc.  
All rights reserved.

Revision History  
October 2012—FRS JunosE 13.3.x

The information in this document is current as of the date on the title page.

#### YEAR 2000 NOTICE

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

#### END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

	About the Documentation . . . . .	xvii
	E Series and JunosE Documentation and Release Notes . . . . .	xvii
	Audience . . . . .	xvii
	E Series and JunosE Text and Syntax Conventions . . . . .	xvii
	Obtaining Documentation . . . . .	xix
	Documentation Feedback . . . . .	xix
	Requesting Technical Support . . . . .	xix
	Self-Help Online Tools and Resources . . . . .	xx
	Opening a Case with JTAC . . . . .	xx
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Understanding Remote Access . . . . .</b>	<b>3</b>
	Remote Access Overview . . . . .	3
	B-RAS Data Flow . . . . .	3
	Configuring IP Addresses for Remote Clients . . . . .	4
	AAA Overview . . . . .	4
	Remote Access Platform Considerations . . . . .	4
	B-RAS Protocol Support . . . . .	5
	Remote Access References . . . . .	5
	DHCP Features . . . . .	5
<b>Chapter 2</b>	<b>How the Domain Map Feature Works . . . . .</b>	<b>7</b>
	Domain Name Aliases Overview . . . . .	7
	Overview of Mapping a User Domain to a Virtual Router . . . . .	7
	Mapping User Requests Without a Valid Domain Name . . . . .	8
	Mapping User Requests Without a Configured Domain Name . . . . .	8
	Using DNIS . . . . .	8
	Redirected Authentication . . . . .	9
	IP Hinting . . . . .	9
	Domain Name and Realm Name Overview . . . . .	9
	Using the Realm Name as the Domain Name . . . . .	10
	Using Delimiters Other Than @ . . . . .	10
	Using Either the Domain or the Realm as the Domain Name . . . . .	11
	Specifying the Domain Name or Realm Name Parse Direction . . . . .	11
	Stripping the Domain Name . . . . .	11
	Stripping the Domain Name Per Virtual Router . . . . .	12
	Subscriber User Name for RID, CoA Requests, and Lawful Intercepts	
	When Strip Domain Is Enabled . . . . .	12
	Using the Strip Domain Functionality Per Virtual Router When Strip	
	Domain Is Enabled for an AAA Domain Map . . . . .	12

	Redirected Authentication When Strip Domain Is Enabled . . . . .	13
<b>Chapter 3</b>	<b>Understanding Authentication and Accounting Servers Functions . . . . .</b>	<b>15</b>
	RADIUS Authentication and Accounting Servers Configuration Overview . . . . .	15
	Server Access . . . . .	16
	Server Request Processing Limit . . . . .	16
	Authentication and Accounting Methods . . . . .	17
	Supporting Exchange of Extensible Authentication Protocol Messages . . . . .	18
	Immediate Accounting Updates . . . . .	18
	Duplicate and Broadcast Accounting . . . . .	19
	UDP Checksums . . . . .	19
	Local Authentication Servers Configuration Overview . . . . .	19
	Tunnel Subscriber Authentication Configuration Overview . . . . .	20
<b>Chapter 4</b>	<b>Understanding Address Servers Functions . . . . .</b>	<b>23</b>
	Name Server Addresses Configuration Overview . . . . .	23
	Local Address Servers Configuration Overview . . . . .	23
	Local Address Pool Ranges . . . . .	24
	Local Address Pool Aliases . . . . .	24
	Shared Local Address Pools . . . . .	25
	SNMP Thresholds . . . . .	26
<b>Chapter 5</b>	<b>AAA Profiles . . . . .</b>	<b>27</b>
	AAA Profile Configuration Overview . . . . .	27
	AAA Logical Line Identifier for Subscriber Tracking Overview . . . . .	28
	How the Router Obtains and Uses the LLID . . . . .	28
	RADIUS Attributes in Preauthentication Request . . . . .	29
	Considerations for Using the LLID . . . . .	30
<b>Chapter 6</b>	<b>Route Download Servers for IPv4 and IPv6 Routes . . . . .</b>	<b>33</b>
	RADIUS Route-Download Server for Route Distribution Overview . . . . .	33
	Format of Downloaded Routes . . . . .	33
	Framed-Route (RADIUS attribute 22) . . . . .	34
	Framed-IPv6-Route (RADIUS attribute 99) . . . . .	34
	Cisco AV-Pair (Cisco VSA 26-1) . . . . .	34
	How the Route-Download Server Downloads Routes . . . . .	34
<b>Chapter 7</b>	<b>Termination of PPP and L2TP Subscriber Sessions . . . . .</b>	<b>37</b>
	Overview of Mapping Application Terminate Reasons and RADIUS Terminate Codes . . . . .	37
	Timeout Configuration Overview . . . . .	39
	Limiting Active Subscribers . . . . .	39
	AAA Failure Notification for RADIUS . . . . .	39
	Configuring AAA Session Timeout . . . . .	40

<b>Chapter 8</b>	<b>DHCPv6 Prefix Delegation and IPv6 Neighbor Discovery for AAA Subscribers</b> . . . . .	<b>41</b>
	Standard RADIUS IPv6 Attributes for IPv6 Neighbor Discovery Router Advertisements and DHCPv6 Prefix Delegation Configuration . . . . .	41
	Maximum Number of IPv6 Prefixes Assigned to Clients Using Both DHCPv6 Local Server and Neighbor Discovery Router Advertisements . . . . .	42
	Delegation of a Unique IPv6 Prefix per Subscriber Example . . . . .	42
	Delegation of the Same IPv6 Prefix for Multiple Subscribers Example . . . . .	43
	Maximum Number of IPv6 Prefixes Assigned to Clients Using Only the DHCPv6 Local Server . . . . .	43
	DHCPv6 Local Address Pools for Allocation of IPv6 Prefixes Overview . . . . .	44
	IPv6 Prefix Allocation Using Neighbor Discovery Router Advertisements from IPv6 Address Pools Overview . . . . .	46
	Allocation of Neighbor Discovery Prefixes for IPv6 Subscribers over PPP Links . . . . .	46
	Order of Preference in Determining the Local Address Pool for Allocating Prefixes for Neighbor Discovery Router Advertisements . . . . .	46
	Order of Preference in Assigning Prefixes when Neighbor Discovery Router Advertisements are Configured on an Interface . . . . .	47
	Guidelines for Allocating Neighbor Discovery Prefixes Using IPv6 Address Pools . . . . .	47
<b>Chapter 9</b>	<b>Validation of Duplicate Prefixes and Addresses</b> . . . . .	<b>51</b>
	Duplicate IPv6 Prefix Check Overview . . . . .	51
	Duplicate IPv6 Prefix Detection in the AAA User Profile Database Overview . . . . .	51
	Guidelines for Duplicate Address Verification . . . . .	52
<b>Chapter 10</b>	<b>Interoperation with SRC Software</b> . . . . .	<b>55</b>
	SRC Client Configuration Overview . . . . .	55
	SRC Client and COPS Terminology . . . . .	55
	Retrieval of DSL Line Rate Information from Access Nodes Overview . . . . .	58
<b>Chapter 11</b>	<b>Application Terminate Reasons</b> . . . . .	<b>61</b>
	AAA Terminate Reasons . . . . .	61
	L2TP Terminate Reasons . . . . .	62
	PPP Terminate Reasons . . . . .	79
	RADIUS Client Terminate Reasons . . . . .	86
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 12</b>	<b>Configuring B-RAS Services</b> . . . . .	<b>89</b>
	Remote Access Configuration Tasks . . . . .	89
<b>Chapter 13</b>	<b>Enabling the B-RAS Application</b> . . . . .	<b>91</b>
	Configuring a B-RAS License . . . . .	91
<b>Chapter 14</b>	<b>Configuration Tasks for AAA Accounting</b> . . . . .	<b>93</b>
	Configuring AAA Duplicate Accounting . . . . .	93
	Configuring AAA Broadcast Accounting . . . . .	93
	Overriding AAA Accounting NAS Information . . . . .	94
	Collecting Accounting Statistics . . . . .	94

<b>Chapter 15</b>	<b>Configuration Tasks for AAA Servers . . . . .</b>	<b>95</b>
	Configuring RADIUS AAA Servers . . . . .	95
	Configuring DNS Primary and Secondary NMS . . . . .	97
	Configuring WINS Primary and Secondary NMS . . . . .	98
<b>Chapter 16</b>	<b>Configuration Tasks for AAA Authentication and User Database . . . . .</b>	<b>99</b>
	Creating the AAA Local Authentication Environment . . . . .	99
	Creating AAA Local User Databases . . . . .	100
	Adding AAA User Entries to Default Local User Databases . . . . .	100
	Adding AAA User Entries to Local User Databases . . . . .	101
	Configuring AAA User Entries in Local User Databases . . . . .	101
	Assigning a Local User Database to a Virtual Router . . . . .	102
	Enabling Local Authentication on the Virtual Router . . . . .	103
<b>Chapter 17</b>	<b>Configuration Tasks for Local Address Pools . . . . .</b>	<b>105</b>
	Configuring a Local Address Server . . . . .	105
	Configuring the DHCPv6 Local Address Pools . . . . .	106
	Configuring IPv6 Neighbor Discovery Local Address Pools . . . . .	108
<b>Chapter 18</b>	<b>Configuring Clients Logging In to Interfaces . . . . .</b>	<b>111</b>
	Creating an IP Interface . . . . .	111
	Configuring Single PPP Clients per ATM Subinterface . . . . .	111
	Configuring Multiple PPP Clients per ATM Subinterface . . . . .	112
	Configuring Single PPP Clients per ATM Subinterface . . . . .	113
	Configuring Multiple PPP Clients per ATM Subinterface . . . . .	114
<b>Chapter 19</b>	<b>Configuration Tasks for AAA Profiles . . . . .</b>	<b>117</b>
	Controlling Access to Domain Names . . . . .	117
	Configuring an AAA Per-Profile Attribute List . . . . .	118
	Configuring the NAS-Port-Type Attribute Manually . . . . .	119
	Configuring a Service Description for the AAA Profile . . . . .	120
	Configuring the Router to Obtain the LLID for a Subscriber . . . . .	120
<b>Chapter 20</b>	<b>Configuration Task for Route-Download Servers for IPv4 and IPv6 . . . . .</b>	<b>123</b>
	Configuring the Route-Download Server to Download Routes . . . . .	123
<b>Chapter 21</b>	<b>Configuration Tasks for Duplicate Prefixes Detection . . . . .</b>	<b>127</b>
	Configuring Duplicate IPv6 Prefix Check . . . . .	127
	Configuring Detection of Duplicate IPv6 Prefixes in the AAA User Profile Database . . . . .	127
<b>Chapter 22</b>	<b>Configuring COPS Interworking with SRC Client . . . . .</b>	<b>129</b>
	Configuring the SRC Client . . . . .	129
	Configuring the Forwarding of COPS Requests to the SRC Server Based on DCM Profiles . . . . .	131
<b>Chapter 23</b>	<b>Configuration Commands . . . . .</b>	<b>133</b>
	aaa dhcpv6-ndra-pool override . . . . .	134
	aaa dns . . . . .	135
	aaa ipv6-dns . . . . .	136
	aaa accounting duplication . . . . .	137
	aaa accounting broadcast . . . . .	138

aaa accounting statistics	139
aaa accounting vr-group	140
aaa authentication default	141
aaa domain-map	142
aaa duplicate-address-check	143
aaa duplicate-prefix-check	144
aaa duplicate-prefix-check-extension	145
aaa local select database	146
aaa local username	147
dns-domain-search	148
dns-server	149
exclude-prefix	150
exclude-ndraprefix	151
ip send-cops-request	152
ipv6 address	153
ipv6 nd	154
ipv6 unnumbered	155
prefix	156
ipv6 address-pool local	158
ipv6 local pool	159
ipv6-prefix-pool-name	160
ipv6 address-pool ndra	161
ipv6 local ndra-pool	162
license b-ras	163
ndraprefix	164
radius override nas-info	165
radius accounting server	166
radius authentication server	167
radius rollover-on-reject	168
radius tunnel-accounting	169
radius udp-checksum	170
radius trap acct-server-responding	171
radius trap acct-server-not-responding	172
radius trap no-acct-server-responding	173
radius trap auth-server-responding	174
radius trap auth-server-not-responding	175
radius trap no-auth-server-responding	176
retransmit	177
snmp-server	178
snmp-server community	179
snmp-server enable traps	180
snmp-server host	183
snmp-server trap-source	186
sscc address	187
sscc enable	188
sscc option	189
timeout	191
udp-port	192
virtual-router	193

<b>Chapter 24</b>	<b>Examples</b> . . . . .	<b>195</b>
	Example: Domain Name and Realm Name . . . . .	195
	Example: Stripping Domain Name Per Virtual Router for RADIUS Server Authentication . . . . .	196
	Example: Delegating the DHCPv6 Prefix . . . . .	198
	Order of Preference in Determining the Local Address Pool for Allocating Prefixes . . . . .	198
	Order of Preference in Allocating Prefixes and Assigning DNS Addresses to Requesting Routers . . . . .	199
	Example: Configuring AAA Local Authentication . . . . .	200
	Example: Associating all Subscribers of a PPP Interface with a Specific Domain Name . . . . .	203
	Example: Associating Multiple Domain Names with a Specific Domain Name . . . . .	204
	Example: Limiting the Number of Prefixes Used by DHCPv6 Clients . . . . .	205
	Example: Using DHCPv6 Local Address Pools for Prefix Delegation over non-PPP Links . . . . .	206
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 25</b>	<b>Monitoring AAA Server and Authentication Settings</b> . . . . .	<b>211</b>
	Setting Baselines for Remote Access . . . . .	211
	Setting a Baseline for AAA Statistics . . . . .	211
	Setting a Baseline for AAA Route Downloads . . . . .	212
	Setting a Baseline for COPS Statistics . . . . .	212
	Setting a Baseline for Local Address Pool Statistics . . . . .	212
	Setting a Baseline for RADIUS Statistics . . . . .	212
	Setting the Baseline for SRC Statistics . . . . .	212
	How to Monitor PPP Interfaces . . . . .	213
	Monitoring the AAA Model . . . . .	213
	Monitoring IP Addresses of Primary and Secondary DNS and WINS Name Servers . . . . .	214
	Monitoring AAA Server Attributes . . . . .	214
	Monitoring Configuration Information for AAA Local Authentication . . . . .	216
	Monitoring the B-RAS License . . . . .	217
<b>Chapter 26</b>	<b>Monitoring AAA Accounting Details</b> . . . . .	<b>219</b>
	Monitoring the AAA Accounting Configuration . . . . .	219
	Monitoring AAA Accounting Default . . . . .	220
	Monitoring the AAA Accounting Interval . . . . .	220
	Monitoring AAA Specific Virtual Router Groups . . . . .	220
<b>Chapter 27</b>	<b>Monitoring the Mapping of User Domains to Virtual Routers</b> . . . . .	<b>223</b>
	Monitoring the Default AAA Authentication Method List . . . . .	223
	Monitoring AAA Domain Name Stripping for a Domain Per Virtual Router . . . . .	223
	Monitoring Mapping Between User Domains and Virtual Routers . . . . .	224
	Monitoring Tunnel Subscriber Authentication . . . . .	226
<b>Chapter 28</b>	<b>Verifying Settings for Detection of Duplicate Prefixes</b> . . . . .	<b>229</b>
	Monitoring Routing Table Address Lookup . . . . .	229
	Monitoring the Routing Table . . . . .	229

<b>Chapter 29</b>	<b>Monitoring AAA Profiles and Subscriber Sessions . . . . .</b>	<b>231</b>
	Monitoring AAA Profile Configuration . . . . .	231
	Monitoring the Number of Active Subscribers Per Port . . . . .	232
	Monitoring the Maximum Number of Active Subscribers Per Virtual Router . . . . .	232
	Monitoring Session Timeouts . . . . .	233
<b>Chapter 30</b>	<b>Monitoring Route-Download Server Settings . . . . .</b>	<b>235</b>
	Monitoring Statistics about the RADIUS Route-Download Server . . . . .	235
	Monitoring Routes Downloaded by the RADIUS Route-Download Server . . . . .	237
	Monitoring Chassis-Wide Routes Downloaded by the RADIUS Route-Download Server . . . . .	239
<b>Chapter 31</b>	<b>Monitoring AAA Accounting Details . . . . .</b>	<b>243</b>
	Monitoring AAA Statistics . . . . .	243
	Monitoring Interim Accounting for Users on the Virtual Router . . . . .	245
	Monitoring Virtual Router Groups Configured for AAA Broadcast Accounting . . . . .	245
<b>Chapter 32</b>	<b>Monitoring COPS Layer Settings . . . . .</b>	<b>247</b>
	Monitoring the COPS Layer Over SRC Connection . . . . .	247
	Monitoring Statistics About the COPS Layer . . . . .	249
<b>Chapter 33</b>	<b>Monitoring SRC Client Settings . . . . .</b>	<b>253</b>
	Monitoring SRC Client Connection Status . . . . .	253
	Monitoring SRC Client Connection Statistics . . . . .	255
	Monitoring SRC Client Connection Statistics . . . . .	257
	Monitoring the SRC Client Version Number . . . . .	259
<b>Chapter 34</b>	<b>Monitoring the IP Local Address Pools Configuration . . . . .</b>	<b>261</b>
	Monitoring Local Address Pools . . . . .	261
	Monitoring Local Address Pool Aliases . . . . .	263
	Monitoring Local Address Pool Statistics . . . . .	263
	Monitoring Shared Local Address Pools . . . . .	263
<b>Chapter 35</b>	<b>Monitoring RADIUS Servers and Services for AAA Features . . . . .</b>	<b>265</b>
	Monitoring the RADIUS Server Algorithm . . . . .	265
	Monitoring the RADIUS Attribute Used for DHCPv6 Prefix Delegation . . . . .	265
	Monitoring the RADIUS Attribute Used for IPv6 Neighbor Discovery Router Advertisements . . . . .	266
	Monitoring the RADIUS Rollover Configuration . . . . .	266
	Monitoring RADIUS Override Settings . . . . .	266
	Monitoring RADIUS Server Information . . . . .	267
	Monitoring RADIUS Accounting for L2TP Tunnels . . . . .	269
	Monitoring RADIUS Services Statistics . . . . .	269
	Monitoring RADIUS SNMP Traps . . . . .	273
	Monitoring RADIUS UDP Checksums . . . . .	273
	Monitoring RADIUS Server IP Addresses . . . . .	273
<b>Chapter 36</b>	<b>Verifying Active Subscriber Session Details . . . . .</b>	<b>275</b>
	Monitoring Subscriber Information . . . . .	275
<b>Chapter 37</b>	<b>Investigating Causes for Termination of User Sessions . . . . .</b>	<b>283</b>
	Monitoring Application Terminate Reason Mappings . . . . .	283

<b>Chapter 38</b>	<b>Monitoring IPv6 Local Address Pool Settings . . . . .</b>	<b>285</b>
	Monitoring IPv6 Local Pools for Neighbor Discovery Router Advertisements for all Configured Pools . . . . .	285
	Monitoring IPv6 Local Pools for Neighbor Discovery Router Advertisements by Pool Name . . . . .	286
	Monitoring IPv6 Local Pool Statistics for Neighbor Discovery Router Advertisements Allocation of Prefixes . . . . .	287
	Monitoring IPv6 Local Pools for DHCP Prefix Delegation By All Configured Pools . . . . .	288
	Monitoring IPv6 Local Pools for DHCP Prefix Delegation By Pool Name . . . . .	289
	Monitoring IPv6 Local Pool Statistics for DHCP Prefix Delegation . . . . .	291
<b>Chapter 39</b>	<b>Monitoring Commands . . . . .</b>	<b>293</b>
	baseline aaa . . . . .	294
	baseline aaa route-download . . . . .	295
	baseline cops . . . . .	296
	baseline local pool . . . . .	297
	baseline radius . . . . .	298
	baseline ssc . . . . .	299
	show aaa accounting . . . . .	300
	show aaa accounting default . . . . .	301
	show aaa authentication default . . . . .	302
	show aaa delimiters . . . . .	303
	show aaa strip-domain . . . . .	304
	show aaa domain-map . . . . .	305
	show aaa duplicate-address-check . . . . .	306
	show aaa duplicate-prefix-check-extension . . . . .	307
	show aaa ipv6-nd-ra-prefix . . . . .	308
	show aaa dhcpv6-delegated-prefix . . . . .	309
	show aaa model . . . . .	310
	show aaa name-servers . . . . .	311
	show aaa profile . . . . .	312
	show aaa route-download . . . . .	313
	show aaa route-download routes . . . . .	314
	show aaa route-download ipv6 routes . . . . .	315
	show aaa route-download routes global . . . . .	316
	show aaa route-download ipv6 routes global . . . . .	317
	show aaa statistics . . . . .	318
	show aaa subscriber per-port-limit . . . . .	319
	show aaa subscriber per-vr-limit . . . . .	320
	show aaa timeout . . . . .	321
	show aaa user accounting interval . . . . .	322
	show cops info . . . . .	323
	show cops statistics . . . . .	324
	show ip local alias . . . . .	325
	show ip local pool . . . . .	326
	show ip local shared-pool . . . . .	327
	show ip route . . . . .	328
	show ipv6 local pool . . . . .	330

	show ipv6 local ndra-pool . . . . .	331
	show license . . . . .	332
	show radius algorithm . . . . .	333
	show radius override . . . . .	334
	show radius rollover-on-reject . . . . .	335
	show radius servers . . . . .	336
	show radius statistics . . . . .	337
	show radius tunnel-accounting . . . . .	338
	show sssc info . . . . .	339
	show sssc options . . . . .	340
	show sssc statistics . . . . .	341
	show sssc version . . . . .	342
	show subscribers . . . . .	343
<b>Part 4</b>	<b>Troubleshooting</b>	
<b>Chapter 40</b>	<b>SNMP Traps and System Logs for Authentication Failures . . . . .</b>	<b>347</b>
	SNMP Traps and System Log Messages Overview . . . . .	347
	SNMP Traps . . . . .	347
	System Log Messages . . . . .	348
<b>Chapter 41</b>	<b>Configuring SNMP Traps . . . . .</b>	<b>349</b>
	Configuring SNMP Traps . . . . .	349
<b>Chapter 42</b>	<b>Troubleshooting RADIUS Preauthentication Failure . . . . .</b>	<b>351</b>
	Troubleshooting Subscriber Preauthentication . . . . .	351
<b>Part 5</b>	<b>Index</b>	
	Index . . . . .	355



# List of Figures

<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 4</b>	<b>Understanding Address Servers Functions . . . . .</b>	<b>23</b>
	Figure 1: Local Address Pool Hierarchy . . . . .	24
	Figure 2: Shared Local Address Pools . . . . .	25
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 18</b>	<b>Configuring Clients Logging In to Interfaces . . . . .</b>	<b>111</b>
	Figure 3: Single PPP Clients per ATM Subinterface . . . . .	111
	Figure 4: Multiple PPP Clients per ATM Subinterface . . . . .	112
	Figure 5: Single PPP Clients per ATM Subinterface . . . . .	113
	Figure 6: Multiple PPP Clients per ATM Subinterface . . . . .	114



# List of Tables

	<b>About the Documentation</b> . . . . .	<b>xvii</b>
	Table 1: Notice Icons . . . . .	xviii
	Table 2: Text and Syntax Conventions . . . . .	xviii
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 3</b>	<b>Understanding Authentication and Accounting Servers Functions</b> . . . . .	<b>15</b>
	Table 3: Local UDP Port Ranges by RADIUS Request Type . . . . .	17
<b>Chapter 5</b>	<b>AAA Profiles</b> . . . . .	<b>27</b>
	Table 4: RADIUS IETF Attributes in Preauthentication Request . . . . .	29
<b>Chapter 7</b>	<b>Termination of PPP and L2TP Subscriber Sessions</b> . . . . .	<b>37</b>
	Table 5: Supported RADIUS Acct-Terminate-Cause Codes . . . . .	37
<b>Chapter 10</b>	<b>Interoperation with SRC Software</b> . . . . .	<b>55</b>
	Table 6: SRC Client and COPS Terminology . . . . .	56
<b>Chapter 11</b>	<b>Application Terminate Reasons</b> . . . . .	<b>61</b>
	Table 7: Default AAA Mappings . . . . .	61
	Table 8: Default L2TP Mappings . . . . .	62
	Table 9: Default PPP Mappings . . . . .	79
	Table 10: Default RADIUS Client Mappings . . . . .	86
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 24</b>	<b>Examples</b> . . . . .	<b>195</b>
	Table 11: Username and Domain Name Examples . . . . .	195
	Table 12: aaa strip-domain Example . . . . .	197
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 25</b>	<b>Monitoring AAA Server and Authentication Settings</b> . . . . .	<b>211</b>
	Table 13: show configuration category aaa server-attributes include-defaults Output Fields . . . . .	215
	Table 14: show configuration category aaa local-authentication Output Fields . . . . .	217
<b>Chapter 26</b>	<b>Monitoring AAA Accounting Details</b> . . . . .	<b>219</b>
	Table 15: show aaa accounting Output Fields . . . . .	219
	Table 16: show aaa accounting vr-group Output Fields . . . . .	221
<b>Chapter 27</b>	<b>Monitoring the Mapping of User Domains to Virtual Routers</b> . . . . .	<b>223</b>
	Table 17: show aaa strip-domain Output Fields . . . . .	224

	Table 18: show aaa domain-map Output Fields . . . . .	225
<b>Chapter 29</b>	<b>Monitoring AAA Profiles and Subscriber Sessions . . . . .</b>	<b>231</b>
	Table 19: show aaa profile Output Fields . . . . .	231
<b>Chapter 30</b>	<b>Monitoring Route-Download Server Settings . . . . .</b>	<b>235</b>
	Table 20: show aaa route-download Output Fields . . . . .	236
	Table 21: show aaa route-download routes Output Fields . . . . .	238
	Table 22: show aaa route-download routes global Output Fields . . . . .	241
<b>Chapter 31</b>	<b>Monitoring AAA Accounting Details . . . . .</b>	<b>243</b>
	Table 23: show aaa statistics Output Fields . . . . .	244
	Table 24: show configuration category aaa global-attributes Output Fields . . . . .	246
<b>Chapter 32</b>	<b>Monitoring COPS Layer Settings . . . . .</b>	<b>247</b>
	Table 25: show cops info Output Fields . . . . .	248
	Table 26: show cops statistics Output Fields . . . . .	250
<b>Chapter 33</b>	<b>Monitoring SRC Client Settings . . . . .</b>	<b>253</b>
	Table 27: show ssc info Output Fields . . . . .	254
	Table 28: show ssc statistics Output Fields . . . . .	256
	Table 29: show ssc statistics Output Fields . . . . .	258
<b>Chapter 34</b>	<b>Monitoring the IP Local Address Pools Configuration . . . . .</b>	<b>261</b>
	Table 30: show ip local pool Output Fields . . . . .	262
	Table 31: show ip local alias Output Fields . . . . .	263
	Table 32: show ip local shared-pool Output Fields . . . . .	264
<b>Chapter 35</b>	<b>Monitoring RADIUS Servers and Services for AAA Features . . . . .</b>	<b>265</b>
	Table 33: show radius override Output Fields . . . . .	266
	Table 34: show radius servers Output Fields . . . . .	268
	Table 35: show radius statistics Output Fields . . . . .	271
<b>Chapter 36</b>	<b>Verifying Active Subscriber Session Details . . . . .</b>	<b>275</b>
	Table 36: show subscribers Output Fields . . . . .	280
<b>Chapter 37</b>	<b>Investigating Causes for Termination of User Sessions . . . . .</b>	<b>283</b>
	Table 37: show terminate-code Output Fields . . . . .	284
<b>Chapter 38</b>	<b>Monitoring IPv6 Local Address Pool Settings . . . . .</b>	<b>285</b>
	Table 38: show ipv6 local ndra-pool Output Fields . . . . .	286
	Table 39: show ipv6 local ndra-pool poolName Output Fields . . . . .	287
	Table 40: show ipv6 local ndra-pool statistics Output Fields . . . . .	288
	Table 41: show ipv6 local pool Output Fields . . . . .	289
	Table 42: show ipv6 local pool poolName Output Fields . . . . .	290
	Table 43: show ipv6 local pool statistics Output Fields . . . . .	291

# About the Documentation

- E Series and JunosE Documentation and Release Notes on page xvii
- Audience on page xvii
- E Series and JunosE Text and Syntax Conventions on page xvii
- Obtaining Documentation on page xix
- Documentation Feedback on page xix
- Requesting Technical Support on page xix

## E Series and JunosE Documentation and Release Notes

---

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

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

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

## Audience

---

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

## E Series and JunosE Text and Syntax Conventions

---

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

Table 1: Notice Icons

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

Table 2 on page xviii defines text and syntax conventions that we use throughout the E Series and JunosE documentation.

Table 2: Text and Syntax Conventions

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

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

Convention	Description	Examples
(pipe symbol)	Represents a choice to select one keyword or variable to the left or to the right of this symbol. (The keyword or variable can be either optional or required.)	diagnostic   line
[ ] (brackets)	Represent optional keywords or variables.	[ internal   external ]
[ ]* (brackets and asterisk)	Represent optional keywords or variables that can be entered more than once.	[ level1   level2   l1 ]*
{ } (braces)	Represent required keywords or variables.	{ permit   deny } { in   out }  { clusterId   ipAddress }

## Obtaining Documentation

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

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

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

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

## Documentation Feedback

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

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

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf> .
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/> .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

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

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

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

## Opening a Case with JTAC

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

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

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

## PART 1

# Overview

- [Understanding Remote Access on page 3](#)
- [How the Domain Map Feature Works on page 7](#)
- [Understanding Authentication and Accounting Servers Functions on page 15](#)
- [Understanding Address Servers Functions on page 23](#)
- [AAA Profiles on page 27](#)
- [Route Download Servers for IPv4 and IPv6 Routes on page 33](#)
- [Termination of PPP and L2TP Subscriber Sessions on page 37](#)
- [DHCPv6 Prefix Delegation and IPv6 Neighbor Discovery for AAA Subscribers on page 41](#)
- [Validation of Duplicate Prefixes and Addresses on page 51](#)
- [Interoperation with SRC Software on page 55](#)
- [Application Terminate Reasons on page 61](#)



## CHAPTER 1

# Understanding Remote Access

- [Remote Access Overview on page 3](#)
- [Remote Access Platform Considerations on page 4](#)
- [Remote Access References on page 5](#)
- [DHCP Features on page 5](#)

## Remote Access 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.

The following sections provide an overview of remote access:

- [B-RAS Data Flow on page 3](#)
- [Configuring IP Addresses for Remote Clients on page 4](#)
- [AAA Overview on page 4](#)

## 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 the *Configuring RADIUS Attributes* chapter..

---

## 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 the *DHCP Overview* chapter.

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.

### Related Documentation

- [Remote Access Configuration Tasks on page 89](#)

---

## Remote Access 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 ERX7xx models, ERX14xx models, and the ERX310 Broadband Services Router.
- See the *E120 and E320 Module Guide* for modules supported on the Juniper Networks E120 and E320 Broadband Services Routers.
- [B-RAS Protocol Support on page 5](#)

## 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)

## Remote Access 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 3317—Differentiated Services Quality of Service Policy Information Base (DIFFSERV-PIB)
- RFC 3318—Framework Policy Information Base (March 2003)

*JunosE 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.

## 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

**Related  
Documentation**

- DHCP Overview Information

## CHAPTER 2

# How the Domain Map Feature Works

- [Domain Name Aliases Overview on page 7](#)
- [Overview of Mapping a User Domain to a Virtual Router on page 7](#)
- [Domain Name and Realm Name Overview on page 9](#)

### Domain Name Aliases Overview

---

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.

### Overview of Mapping a User Domain 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.

The following sections describe how to map a user domain to a virtual router:

- [Mapping User Requests Without a Valid Domain Name on page 8](#)
- [Mapping User Requests Without a Configured Domain Name on page 8](#)
- [Using DNIS on page 8](#)
- [Redirected Authentication on page 9](#)
- [IP Hinting on page 9](#)

## 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 `vruter_88`, while a user calling 8005554433 is terminated in `vruter_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.

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.

### Related Documentation

- [Domain Name and Realm Name Overview on page 9](#)

---

## Domain Name and Realm Name Overview

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.

The following sections describe domain name and realm name:

- [Using the Realm Name as the Domain Name on page 10](#)
- [Using Delimiters Other Than @ on page 10](#)
- [Using Either the Domain or the Realm as the Domain Name on page 11](#)
- [Specifying the Domain Name or Realm Name Parse Direction on page 11](#)
- [Stripping the Domain Name on page 11](#)
- [Stripping the Domain Name Per Virtual Router on page 12](#)

## 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.

## Stripping the Domain Name Per Virtual Router

The **aaa domain-map** command maps a domain name to a virtual router. It determines the authentication and accounting access for all subscribers belonging to a particular domain. However, if a subscriber profile is configured for a virtual router using the **ppp authentication** command, the authentication for the virtual router configured at the profile level takes priority over the one configured at the domain level. If multiple profiles from the same domain are being used, the subscribers may end up in different virtual routers for authentication.

In such a scenario, you can use the **aaa strip-domain** command to strip a part of the user name of the subscriber. The resulting user name is then used as the new user name for that subscriber for RADIUS authentication and accounting.



**NOTE:** The **aaa strip-domain** command can be configured on non-default virtual routers only.

---

### Subscriber User Name for RID, CoA Requests, and Lawful Intercepts When Strip Domain Is Enabled

---

When strip domain is enabled for a virtual router, the user name used to identify the subscriber session for RADIUS Initiated Disconnect (RID), Change of Authorization (CoA), and lawful intercepts requests is the same as the subscriber user name sent to RADIUS server for authentication.

For example, if a subscriber with user name `user1@123.com$test1` has a resulting user name of `user1@123.com` due to the strip domain configuration, then the user name for all the incoming RID and CoA requests and the lawful intercept requests is `user1@123.com`.

This new user name, which has been used for RADIUS server authentication, is used for displaying subscriber information using **show subscribers** and **logout subscribers** commands.

---

### Using the Strip Domain Functionality Per Virtual Router When Strip Domain Is Enabled for an AAA Domain Map

---

When strip domain is enabled for an AAA domain map using the **strip-domain enable** command in the Domain Map Configuration mode, the strip domain configured for a virtual router may cause the user name stripping to happen twice depending on the configuration.

For example, consider a subscriber with user name `user1@test.com$test1$test2`. Consider the following configurations for a domain map:

```
host1(config)#aaa domain-map test2
host1(config-domain-map)#strip-domain enable
```

The following has also been configured on the non-default virtual router:

```
host1(config)#aaa strip-domain enable
host1(config)#aaa strip-domain delimiter domainname $
```

In this example, when the domain name is stripped for the subscriber with user name `user1@test.com$test1$test2`, the resulting string that is sent for RADIUS authentication is `user1`. Thus, when strip domain is configured for a domain map as well as a non-default virtual router, depending on the configurations, the domain name may get stripped twice, once at the virtual router level and then at the domain map level.

In order to prevent the domain name from being stripped twice for the same subscriber, you must ensure that the strip domain functionality is configured appropriately for the domain map and for the non-default virtual router.

### **Redirected Authentication When Strip Domain Is Enabled**

---

Strip domain configured on a virtual router does not work in case of a redirected authentication. In an authentication redirection, the RADIUS server sends an access-accept message for a subscriber from the virtual router on which the subscriber is already authenticated.

For example, on a virtual router `vr1`, we have configured the `aaa strip-domain`. A subscriber with user name `user1@123.com` is already authenticated on `vr1` using the RADIUS server authentication. Now, if you send an access request message trying to authenticate the same subscriber on `vr1`, the access request message carries the original user name, `user1@123.com`, and renders strip domain ineffective during authentication redirection.

#### **Related Documentation**

- [Example: Domain Name and Realm Name on page 195](#)
- [Example: Stripping Domain Name Per Virtual Router for RADIUS Server Authentication on page 196](#)



## CHAPTER 3

# Understanding Authentication and Accounting Servers Functions

- [RADIUS Authentication and Accounting Servers Configuration Overview on page 15](#)
- [Local Authentication Servers Configuration Overview on page 19](#)
- [Tunnel Subscriber Authentication Configuration Overview on page 20](#)

## RADIUS Authentication and Accounting Servers Configuration Overview

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.

The following sections explain how to configure RADIUS authentication and accounting servers:

- [Server Access on page 16](#)
- [Server Request Processing Limit on page 16](#)
- [Authentication and Accounting Methods on page 17](#)
- [Supporting Exchange of Extensible Authentication Protocol Messages on page 18](#)
- [Immediate Accounting Updates on page 18](#)
- [Duplicate and Broadcast Accounting on page 19](#)

## 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

You can configure RADIUS authentication servers and accounting servers to 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. However, you cannot use the same IP address 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 *JunosE Release Notes, Appendix A, System Maximums*.

---

The E Series router listens to a range of UDP source (or local) ports for RADIUS responses. Each UDP source port supports a maximum of 255 RADIUS requests. When the 255 per-port limit is reached, the router opens the next source port. When the **max-sessions** command limit is reached, the router submits the request to the next configured server.

[Table 3 on page 17](#) lists the range of UDP ports the router uses for each type of RADIUS request.

Table 3: Local UDP Port Ranges by RADIUS Request Type

RADIUS Request Type	ERX310, ERX710, ERX1410, and E120 Broadband Services Routers	ERX1440 and E320 Broadband Services Routers
RADIUS authentication	50000–50124	50000–50124
RADIUS accounting	50125–50249	50125–50499
RADIUS preauthentication	50250–50374	50500–50624
RADIUS route-download	50375–50500	50625–50749

## 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 JunosE 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 JunosE Software currently supports **radius** and **none** as accounting methods and **radius**, **none**, and **local** as authentication methods. See [“Local Authentication Servers Configuration Overview” on page 19](#) 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 JunosE 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. JunosE Software supports the exchange of EAP messages between JunosE applications, such as PPP, and an external RADIUS authentication server.

The JunosE Software's AAA service accepts and passes EAP messages between the JunosE 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 JunosE 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 *JunosE Link Layer Configuration Guide*.

## 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 JunosE 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 is always sent to the authenticating virtual router. The accounting information is sent to the operational virtual router only if duplicate accounting is not enabled and if authenticating virtual router is different than 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.

## 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.

**Related Documentation**

- [Remote Access Configuration Tasks on page 89](#)

## Local Authentication Servers Configuration Overview

---

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.

**Related Documentation**

- [Creating the AAA Local Authentication Environment on page 99](#)
- [Creating AAA Local User Databases on page 100](#)

## Tunnel Subscriber Authentication Configuration Overview

---

When a AAA domain map includes any tunnel configuration, users in this domain are considered to be tunnel subscribers. By default, any such subscriber is granted access without being authenticated by the authentication server. Access is granted even when the user provides an invalid username and password. The tunnel configuration for the subscriber comes from the AAA domain map.

For example, if the authentication protocol for a AAA domain map is RADIUS, AAA grants access to subscribers from this domain immediately without sending access requests to the configured RADIUS server. Because of this behavior, these subscribers cannot get any additional control attributes from the authentication server. This reduces your ability to manage the tunnel subscribers.

In this default situation, if you want the domain subscribers to be managed by the authentication server for any control attribute, then that domain map cannot have any tunnel configuration. Typically, this means you must configure the subscriber individually.

You can use the **tunnel-subscriber authentication** command to get around this limitation. When you enable authentication with this command, access requests for the tunnel subscribers in the domain are sent to the configured authentication server. When the access replies from authentication server are processed, various user attributes from the server can be applied to the subscribers.

When the authentication server returns tunnel attributes, these returned values take precedence over the corresponding local tunnel configuration values in the AAA domain map. If the server does not return any tunnel attributes, then the tunnel subscriber's tunnel settings are configured according to the domain map's tunnel settings.

If the authentication server returns a redirect VSA and the corresponding AAA domain map has local tunnel configurations, the VSA is ignored. Access is denied to the user when the authentication server rejects the access request.

The **tunnel-subscriber authentication** command has no effect on subscribers in a domain with no tunnel configuration. When a AAA domain map has no tunnel configuration, subscribers in the domain are authenticated by the authentication server. If the server grants access, then the subscribers get their tunnel settings only from the authentication server.

By default, tunnel subscribers in the domain are granted access with no external authentication. Use the **enable** keyword to enable authentication. Use the **disable** keyword to restore disable user authentication.

To configure authentication of tunnel subscribers within a AAA domain by an external authentication server.

- Example

```
host1(config-domain-map)#tunnel-subscriber authentication enable
```

- Related Documentation**
- [Overview of Mapping a User Domain to a Virtual Router on page 7](#)
  - tunnel-subscriber authentication



## CHAPTER 4

# Understanding Address Servers Functions

- [Name Server Addresses Configuration Overview on page 23](#)
- [Local Address Servers Configuration Overview on page 23](#)

## Name Server Addresses Configuration Overview

---

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.

### Related Documentation

- [ppp peer](#)

## Local Address Servers Configuration Overview

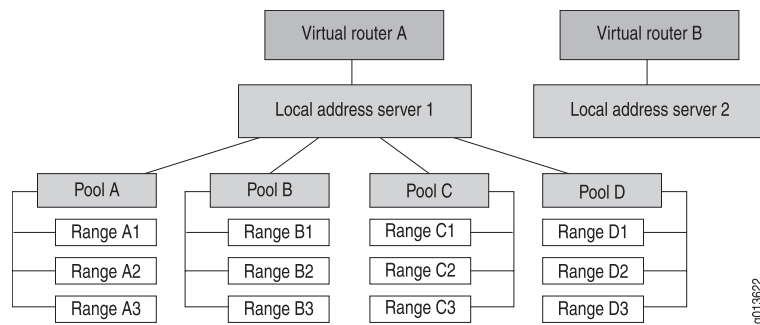
---

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 on page 24 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**



The following sections describe local address servers:

- [Local Address Pool Ranges on page 24](#)
- [Local Address Pool Aliases on page 24](#)
- [Shared Local Address Pools on page 25](#)
- [SNMP Thresholds on page 26](#)

## Local Address Pool Ranges

As shown in Figure 1 on page 24, 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.

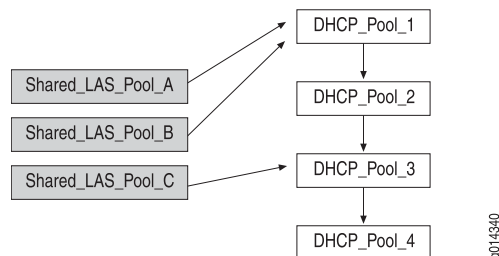
## Shared Local Address Pools

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 on page 25 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.

The following commands create the shared address pools in [Figure 2 on page 25](#):

```
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

A local 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 the outstanding addresses of a pool or a pool group 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 utilization threshold, SNMP is notified.

A local address pool can be linked to a second local address pool so that when the first pool utilization reaches 100%, the DHCP local server uses the second pool. For generation of SNMP traps, the utilization of addresses is calculated for all the pools that are in the linked pools and they are collectively considered as an aggregated pool group.

### Related Documentation

- [Configuring a Local Address Server on page 105](#)

## CHAPTER 5

# AAA Profiles

- [AAA Profile Configuration Overview on page 27](#)
- [AAA Logical Line Identifier for Subscriber Tracking Overview on page 28](#)
- [RADIUS Attributes in Preauthentication Request on page 29](#)
- [Considerations for Using the LLID on page 30](#)

### AAA Profile Configuration Overview

---

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. The domain name **default** indicates that no other match occurs.

#### Related Documentation

- [Single Name Specification for Users from a Domain Overview](#)
- [Example: Configuring AAA Local Authentication on page 200](#)

## AAA Logical Line Identifier for Subscriber Tracking Overview

---

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.

The following section explains how the router obtains and uses the LLID:

- [How the Router Obtains and Uses the LLID on page 28](#)

### 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.

- Related Documentation**
- [Configuring RADIUS AAA Servers on page 95](#)
  - [Configuring the Router to Obtain the LLID for a Subscriber on page 120](#)

## RADIUS Attributes in Preauthentication Request

Table 4 on page 29 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 4: 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

**Table 4: RADIUS IETF Attributes in Preauthentication Request**  
(continued)

Attribute Number	Attribute Name	Description
[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.

**Related Documentation**

- RADIUS IETF Attributes
- [Troubleshooting Subscriber Preauthentication on page 351](#)

## 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.

**Related Documentation** • [Configuring RADIUS AAA Servers on page 95](#)



## CHAPTER 6

# Route Download Servers for IPv4 and IPv6 Routes

- [RADIUS Route-Download Server for Route Distribution Overview on page 33](#)

## RADIUS Route-Download Server for Route Distribution Overview

---

The JunosE RADIUS route-download server provides periodic automatic distribution of IPv4 and IPv6 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 on page 33](#)
- [How the Route-Download Server Downloads Routes on page 34](#)

## 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 ]
```

For IPv4 routes, the route-download server accepts downloaded routes in either the Framed-Route attribute (RADIUS attribute 22) or the Cisco AV-pair attribute (Cisco VSA 26-1).

For IPv6 routes, the route-download server accepts downloaded routes in either the Framed-IPv6-Route attribute (RADIUS attribute 99) or the Cisco AV-pair attribute (Cisco VSA 26-1).

### 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 vrfsunny 192.168.0.0/16 null0 0 tag 8"
```

### Framed-IPv6-Route (RADIUS attribute 99)

```
NAS-1 Password = "14raddlsvr" User-Service-Type = Outbound-User
Framed-IPv6-Route = "2001:DB8:cc00:1::/48 null0"
Framed-IPv6-Route = "vrf test 2001:DB8:cc00:1::/48 null 0 0 tag 6"
Framed-IPv6-Route = "vir zzz vrf test1 2001:DB8:cc00:1::/48 null0 0 tag 8"
```

### Cisco AV-Pair (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 vrfsunny 192.168.0.0/16 null0 0 tag 8"
- NAS-1 Password = "14raddlsvr" User-Service-Type = Outbound-User  
cisco-avpair = "ipv6:route=2001:DB8:cc00:1::/48 null0"  
cisco-avpair = "ipv6:route=vrf test 2001:DB8:cc00:1::/48 null 0 0 tag 6"  
cisco-avpair = "ipv6:route=vir zzz vrf test1 2001:DB8:cc00:1::/48 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

- Related Documentation**
- [Configuring RADIUS AAA Servers on page 95](#)
  - [Configuring the Route-Download Server to Download Routes on page 123](#)



## CHAPTER 7

# Termination of PPP and L2TP Subscriber Sessions

- [Overview of Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 37](#)
- [Timeout Configuration Overview on page 39](#)

### Overview of Mapping Application Terminate Reasons and RADIUS Terminate Codes

The JunosE 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 5 on page 37](#) 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 5: 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

Table 5: Supported RADIUS Acct-Terminate-Cause Codes (*continued*)

Code	Name	Description
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
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

#### Related Documentation

- [Configuring Custom Mappings for PPP Terminate Reasons](#)

## Timeout Configuration Overview

---

You can configure an idle timeout or a session timeout. The values you set are the default values for Point-to-Point Protocol Broadband Remote Access Server users. Attributes returned by RADIUS override these default settings on a per-user basis.

When you set an idle timeout, the PPP application on the router monitors both ingress (inbound) traffic and egress (outbound) traffic by default for the configured idle timeout period to determine whether to disconnect an inactive PPP session. If there is no activity in either direction on the interfaces for more than the configured idle timeout period, the router terminates the PPP session.

You can optionally configure the router to monitor only ingress traffic for the configured idle timeout period to determine session inactivity and subsequent disconnection of an inactive PPP session. Monitoring only ingress traffic for the idle timeout is useful for networks in which the PPP keepalive timer is disabled for wireless subscribers. Without the keepalive timer, the router cannot detect whether a wireless subscriber has been disconnected. Monitoring egress traffic does not indicate inactivity for wireless subscribers because egress traffic is always flowing. Enabling the router to monitor only ingress traffic enables you to selectively disconnect subscribers, including wireless subscribers, if no traffic is received for the configured idle timeout period.

If you do not configure a session timeout, or you set its value to 0, the session remains active for an infinite lifetime. You can use the **show ppp session-To-Thirteen-Years** command along with **show ppp interface full** in Privileged Exec or User Exec mode to verify whether the capability to preserve PPP sessions for a timeout duration of 13 years is enabled. If the **show ppp session-To-Thirteen-Years** command is not executed, the session timeout value is set to the maximum session timeout value of 366 days.

If the RADIUS server returns the value 0 for the Session-Timeout attribute, then the session remains active for an infinite lifetime even if a value is configured through the CLI.

The following sections describe timeout configuration:

- [Limiting Active Subscribers on page 39](#)
- [AAA Failure Notification for RADIUS on page 39](#)
- [Configuring AAA Session Timeout on page 40](#)

### Limiting Active Subscribers

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

### AAA Failure Notification for RADIUS

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.

## Configuring AAA Session Timeout

You can use the **aaa timeout session *sessionTimeout*** command to configure a session timeout. Restoring the session timeout to the default value causes the PPP B-RAS session to remain active for an infinite lifetime.

- Related Documentation**
- [Configuring RADIUS AAA Servers on page 95](#)
  - [Configuring Custom Mappings for PPP Terminate Reasons](#)

## CHAPTER 8

# DHCPv6 Prefix Delegation and IPv6 Neighbor Discovery for AAA Subscribers

- [Standard RADIUS IPv6 Attributes for IPv6 Neighbor Discovery Router Advertisements and DHCPv6 Prefix Delegation Configuration on page 41](#)
- [Maximum Number of IPv6 Prefixes Assigned to Clients Using Both DHCPv6 Local Server and Neighbor Discovery Router Advertisements on page 42](#)
- [Maximum Number of IPv6 Prefixes Assigned to Clients Using Only the DHCPv6 Local Server on page 43](#)
- [DHCPv6 Local Address Pools for Allocation of IPv6 Prefixes Overview on page 44](#)
- [IPv6 Prefix Allocation Using Neighbor Discovery Router Advertisements from IPv6 Address Pools Overview on page 46](#)

## Standard RADIUS IPv6 Attributes for IPv6 Neighbor Discovery Router Advertisements and DHCPv6 Prefix Delegation Configuration

---

When an E Series router is configured for IP version 6, it uses router advertisements to announce its presence to other nodes connected to it. Hosts discover the addresses of their neighboring routers by listening for these advertisements. When the routing protocol process first starts on the server router, the server sends router advertisement packets every few seconds. Then, the server sends these packets less frequently. The server responds to route solicitation packets it receives from a client. The response is sent unicast, unless a router advertisement packet is due to be sent out momentarily. IPv6 supports the following router advertisement mechanisms:

- ICMPv6 Neighbor Discovery router advertisements
- DHCPv6 Prefix Delegation
- ICMPv6 Neighbor Discovery router advertisements followed by DHCPv6 Prefix Delegation

The AAA service on the router stores the prefixes that it receives from the RADIUS server during the PPPv6 authentication phase. After the PPPv6 link is established between the subscriber and the B-RAS application running on the router, the router receives the ICMPv6 router solicitation message, the DHCPv6 Solicit message, or both of them based on the prefix advertisement mechanism. In previous releases, you were not able to configure the RADIUS attribute or VSA to be used for IPv6 Neighbor Discovery router advertisements

and DHCPv6 Prefix Delegation through the CLI. As a result, the IPv6-NdRa-Prefix attribute returned in the Access-Accept message was used for IPv6 Neighbor Discovery router advertisements and the Framed-IPv6-Prefix RADIUS attribute in the Access-Accept message was used for DHCPv6 Prefix Delegation.

In this release, you can control the RADIUS IETF attribute or VSA to be used for IPv6 Neighbor Discovery router advertisements and DHCPv6 Prefix Delegation by using **aaa ipv6-nd-ra-prefix framed-ipv6-prefix** and **aaa dhcpv6-delegated-prefix delegated-ipv6-prefix** commands, respectively, in Global Configuration mode on each virtual router.

## Maximum Number of IPv6 Prefixes Assigned to Clients Using Both DHCPv6 Local Server and Neighbor Discovery Router Advertisements

When both IPv6 Neighbor Discovery router advertisements and DHCPv6 Prefix Delegation methods are used to assign IPv6 prefixes to clients, either two or three host routes for IPv6 might be consumed from the routing table depending on the way in which the router advertisement prefix is determined. The following sections describe sample configuration scenarios to illustrate how a maximum of 48,000 subscribers can be handled for delegation of IPv6 prefixes, based on whether a unique IPv6 prefix is allocated to a client or the same IPv6 prefix is allocated to multiple clients:

- [Delegation of a Unique IPv6 Prefix per Subscriber Example on page 42](#)
- [Delegation of the Same IPv6 Prefix for Multiple Subscribers Example on page 43](#)

### Delegation of a Unique IPv6 Prefix per Subscriber Example

Consider a scenario in which the RADIUS server is configured to assign a unique router advertisement prefix route to each IPv6 subscriber. In such a case, two routes are used for Neighbor Discovery and one IPv6 route is consumed for Prefix Delegation, which results in a total of three routes being utilized for each subscriber. If such a method for allocating prefixes to subscribers is configured, approximately 33,333 IPv6 bindings can be supported before the maximum IPv6 static route limit of 100,000 routes is reached. Therefore, in such a deployment, it is not possible to handle 48,000 subscribers for delegation of IPv6 prefixes using the DHCPv6 local server Prefix Delegation and Neighbor Discovery methods.

The following output of the **show ipv6 route** command displays how three routes are used by the same subscriber, as can be seen from the Interface field in the output. The routes are assigned using Prefix Delegation, Neighbor Discovery, and the access-internal route, such as the DHCP and AAA/PPP host route, which is a host route to directly connected clients. Access routes, also known as AAA framed routes, are sourced by AAA.

```
host1#show ipv6 route
```

Prefix/Length	Type	Dst/Met	Interface
1111:1111:1111:1111::/64	Access	3/0	GigabitEthernet0/2.600.6
1111:1111:2222:2222::/64	AccIntern	2/0	GigabitEthernet0/2.600.6
1111:1111:2222:2222:21b:c0ff:fe4	AccIntern	2/0	GigabitEthernet0/2.600.6 b:9d00/128

## Delegation of the Same IPv6 Prefix for Multiple Subscribers Example

Consider a scenario in which the same prefix with a length of /64 for ICMPv6 Neighbor Discovery router advertisements is assigned to all subscribers by configuring the prefix in the profile or by configuring the RADIUS server to send the same prefix in the Framed-IPv6-Prefix attribute (RADIUS IETF attribute 97) of the RADIUS-Access-Accept message. In such a topology, a unique /64 IPv6 route is not present per subscriber. Instead, one /64 prefix with multiple next-hops is assigned for all the subscribers.

If you use this method for allocating IPv6 prefixes of /64 length to subscribers, Neighbor Discovery consumes one IPv6 route and Prefix Delegation consumes one IPv6 route, which results in a total of two IPv6 routes per subscriber being used. Therefore, it is possible to scale up to a maximum of 48,000 subscribers for delegation of IPv6 prefixes.

The increased scaling limit of support for delegation of IPv6 prefixes using the DHCPv6 local server Prefix Delegation mechanism for 48,000 subscribers applies only to E120 and E320 routers and not to ERX14xx models, ERX7xx models, and the ERX310 router because the binding information is stored in the SRP modules of E120 and E320 routers. Also, a limitation exists on the number of IPv6 interfaces and the IPv6 routing table size supported by ERX routers that prevents the support for 48,000 subscribers for Prefix Delegation on DHCPv6 local servers running on those routers.

To enable support for 48,000 subscribers for IPv6 Prefix Delegation, about 5.5 MB of memory on the SRP module is consumed additionally.

- Related Documentation**
- [Maximum Number of IPv6 Prefixes Assigned to Clients Using Only the DHCPv6 Local Server on page 43](#)

---

## Maximum Number of IPv6 Prefixes Assigned to Clients Using Only the DHCPv6 Local Server

IPv6 prefixes are delegated to subscribers using two mechanisms: ICMPv6 Neighbor Discovery router advertisements and DHCPv6 Prefix Delegation. When the router receives the ICMPv6 router solicitation message, the DHCPv6 Solicit message, or both the messages based on the prefix advertisement mechanism, a prefix is assigned to the requesting router, which is the customer premises equipment (CPE) at the edge of the remote client site that acts as the DHCP client. Consider a scenario in which the CPE device uses the Prefix Delegation feature alone to obtain IPv6 prefixes from the delegating router, which is the DHCPv6 local server. Also, assume that IPv6 Neighbor Discovery is not configured for allocation of prefixes to the client. In such an environment, each IPv6 subscriber uses only a single route entry and the maximum number of subscribers to which IPv6 prefixes can be delegated from the DHCPv6 local server is 48,000.

- Related Documentation**
- [Maximum Number of IPv6 Prefixes Assigned to Clients Using Both DHCPv6 Local Server and Neighbor Discovery Router Advertisements on page 42](#)

## DHCPv6 Local Address Pools for Allocation of IPv6 Prefixes Overview

---

In previous releases, you configured DHCPv6 local servers on a virtual router to delegate IPv6 prefixes to DHCPv6 clients. In this release, you can configure IPv6 local address pools to allocate IPv6 prefixes to clients in networks that use DHCPv6. These pools can be used to assign prefixes from a delegating router, which is an E Series router configured as a DHCPv6 local server, to the requesting router, which is the customer premises equipment (CPE) at the edge of the remote client site that acts as the DHCP client.

The DHCPv6 prefix delegation feature is useful in scenarios in which the delegating router does not have information about the topology of the networks in which the customer edge device or requesting router is located. In such cases, the delegating router requires only the identity of the requesting router to choose a prefix for delegation. An IPv6 local pool is configured on the delegating router, which contains information about the prefixes, their validity periods, and other parameters to control their assignment to the requesting routers. The delegating router is configured with a set of prefixes that is used to assign to a CPE or DHCPv6 client, when it first establishes a connection with an Internet service provider (ISP).

When the delegating router receives a request from a DHCPv6 client, it selects an available prefix and delegates it to the client. The DHCPv6 client subnets the delegated prefix and assigns the prefixes to links at the customer edge.

Keep the following points in mind when you configure IPv6 local address pools to assign prefixes to requesting routers:

- You must enable the IPv6 local address pool feature to be able to configure IPv6 local address pools.
- You can configure IPv6 local address pools for DHCP to allocate prefixes to client requests that are received over PPP or non-PPP links, such as VLAN, S-VLAN, or Ethernet.
- You can configure multiple local address pools on a single virtual router, up to a maximum of 500 pools per virtual router.
- You can also configure multiple address pools on multiple virtual routers. Each IPv6 local address pool must have a unique name.
- You can configure a valid and preferred lifetime for each IPv6 prefix, which determines the length of time the requesting router can use the prefix.
- You can configure multiple prefix ranges in an IPv6 local pool. The ranges can have the same or different assigned prefix lengths.
- You cannot configure overlapping prefix ranges in an IPv6 local pool. If you try to configure a prefix range that overlaps with an existing prefix range in the IPv6 local pool, an error message is displayed stating that the prefix range could not be configured. Similarly, an error message is displayed if you try to configure a prefix range in an IPv6 local pool that overlaps with a prefix range in another IPv6 local pool on the same virtual router.

- You can configure certain prefix ranges to be excluded from being used for delegation to the requesting router.
- You can configure the IPv6 addresses of a primary and secondary DNS server in an IPv6 local pool. The DNS server addresses are returned to the client in DHCPv6 responses as part of the DNS Recursive Name Server option.
- You can configure a list of up to four domain names in an IPv6 local pool to be used during the resolution of hostnames to IP addresses. These domain names are returned to clients in the DHCPv6 responses as part of the Domain Search List option.
- You can configure an IPv6 local address pool in an AAA domain map to assign prefixes to requesting DHCPv6 clients using the **ipv6 prefix-pool-name** command in Domain Map Configuration mode. If the authentication server returns the IPv6 local address pool name in the Framed-IPv6-Pool attribute of the RADIUS-Access-Accept message, this pool overrides the IPv6 local address pool configured in the domain map.
- You cannot delete a pool or a prefix range from which prefixes have been allocated to requesting routers or DHCPv6 clients. However, you can forcibly delete such a pool or prefix range by using the **force** keyword in the **ipv6 local pool poolName** and **prefix** commands. If a pool is deleted or the prefix range associated with the pool is deleted, and prefixes have been assigned to DHCPv6 clients or requesting routers, the corresponding DHCPv6 bindings are also deleted.
- When multiple prefix ranges are configured in a pool, the DHCPv6 prefix delegation feature allocates prefixes from the configured ranges in the order of the assigned prefix length. The delegating router or the DHCPv6 server attempts to allocate a prefix from the range with lowest assigned prefix length. If this attempt fails because the pool has been fully allocated, the server tries to allocate a prefix from the subsequent prefix ranges. These ranges could have the same prefix length as the first one or a higher length.



**NOTE:** Although you can configure an IPv6 local pool with the assigned prefix length as /128, which implies a full IPv6 address, this assignment is not useful for the DHCPv6 prefix delegation feature because it assigns a prefix with a length of only /64 or less. A pool with an assigned prefix length of /128 is useful when complete IPv6 addresses are assigned to the DHCPv6 clients.

- When an IPv6 client that is connected to the requesting router using a PPP link is delegated a prefix by the DHCPv6 server, the client binding is removed when the PPP interface goes down and is not retained until the lease time expires. A new client binding is created for the PPP subscriber in response to a renew or rebind request sent to the DHCP server. This method of re-creating the client binding ensures that the client receives a new authentication configuration and is assigned a prefix when it sends a rebind or renew request after the PPP interface flaps (constantly goes up and down).

When a PPP user establishes a PPP connection with the E Series router functioning as a remote access server, the subscriber is first authenticated using the RADIUS protocol. The Access-Accept message returned from the RADIUS server can contain different IPv6 attributes, including the Framed-IPv6-Pool attribute, which contains the name of the

IPv6 pool from which a prefix needs to be assigned to the subscriber. The prefix is assigned to the subscriber using the DHCPv6 prefix delegation feature, which is covered in the next section.

**Related Documentation**

- [Example: Delegating the DHCPv6 Prefix on page 198](#)

## IPv6 Prefix Allocation Using Neighbor Discovery Router Advertisements from IPv6 Address Pools Overview

---

You can configure IPv6 local address pools for Neighbor Discovery router advertisements on a virtual router in order to allocate prefixes to Neighbor Discovery clients. These pools can be used to assign prefixes from the E Series router.

An IPv6 local address pool for Neighbor Discovery router advertisements is configured on the router running the B-RAS application, which contains information about the prefixes. When the B-RAS application running on the E Series router receives a request from a PPP IPv6 client, it selects an available prefix and allocates it to the client.

### Allocation of Neighbor Discovery Prefixes for IPv6 Subscribers over PPP Links

When a PPP user establishes a PPP connection with the E Series router functioning as a remote access server, the subscriber is first authenticated using the RADIUS protocol. The Access-Accept message returned from the RADIUS server can contain different IPv6 attributes, including the IPv6-NdRa-Pool attribute, which contains the name of the IPv6 pool from which a prefix needs to be assigned to the subscriber. The prefix is assigned to the subscriber using the Neighbor Discovery router advertisements feature.

### Order of Preference in Determining the Local Address Pool for Allocating Prefixes for Neighbor Discovery Router Advertisements

You can configure multiple local address pools for Neighbor Discovery router advertisements on a virtual router. When multiple pools are configured, the pool that is used to allocate the prefix to the requesting PPPv6 subscriber is selected using the following order of preference:

1. If the **aaa dhcpv6-ndra-pool override** command is not configured and a pool name is returned by the RADIUS server in the IPv6-Ndra-Pool attribute, that pool is used to allocate the prefix to the client.
2. If the **aaa dhcpv6-ndra-pool override** command is configured and a pool name is returned by the RADIUS server in the Framed-Ipv6-Pool attribute, that pool is used to allocate the prefix to the client.
3. If the RADIUS server does not return a pool name in either of the above-mentioned points, based on the **aaa dhcpv6-ndra-pool override** command, the pool name configured in the AAA domain map is used.

## Order of Preference in Assigning Prefixes when Neighbor Discovery Router Advertisements are Configured on an Interface

The router running the B-RAS application uses the following order of preference to determine the source from which the Neighbor Discovery router advertisements prefix is allocated to the requesting PPPv6 subscriber from the Neighbor Discovery Router Advertisements server:

1. An interface that is configured for the Neighbor Discovery router advertisements prefix is given priority over the RADIUS attributes returned in the Access-Accept message or the prefixes configured in the IPv6 local address pool for Neighbor Discovery router advertisements on the router running the B-RAS application.
2. The RADIUS server might return one or more of the following attributes in the Access-Accept message in response to the client authentication request:
  - Ipv6-NdRa-Prefix (VSA 26-129)
  - Framed-IPv6-Prefix (RADIUS IETF attribute 97)
  - Framed-IPv6-Pool (RADIUS IETF attribute 100)
  - IPv6-Ndra-Pool (VSA 26-157)

If either of the first two attributes are returned, then the prefix contained in those attributes is used, and the pool name in the Framed-IPv6-Pool or Ipv6-Ndra-Pool attribute is ignored.

3. If the RADIUS server does not return any of the above-mentioned attributes, the IPv6 prefix pool name of the Neighbor Discovery router advertisements mentioned in the AAA domain map will be used to allocate the prefix to the requesting PPPv6 subscriber.

## Guidelines for Allocating Neighbor Discovery Prefixes Using IPv6 Address Pools

The following are guidelines for allocating prefixes using IPv6 address pools for Neighbor Discovery router advertisements:

- You must enable the IPv6 local address pool for the Neighbor Discovery router advertisements feature to be able to configure IPv6 local address pools for Neighbor Discovery router advertisements.
- You can configure IPv6 local address pools for Neighbor Discovery router advertisements to allocate prefixes to client requests that are received over PPP.
- You can configure multiple local address pools on a single virtual router up to a maximum of 500 pools per virtual router.
- You can also configure multiple address pools on multiple virtual routers. Each IPv6 local address pool must have a unique name.
- You can configure up to ten prefix ranges in an IPv6 local address pool. The ranges can have only /64 prefix length.
- You can configure a maximum of 1,048,576 prefixes per prefix range to be used for allocation of prefixes to clients using Neighbor Discovery router advertisements. If you

attempt to configure prefixes after the maximum limit of prefixes per prefix range is exceeded, a warning message stating that automatic truncation will be performed is displayed.

- You can configure a maximum of 400,000,000 prefixes throughout the system for allocation of prefixes using Neighbor Discovery router advertisements. An error message is displayed if you attempt to configure a prefix for a pool when this maximum system-wide limit is exceeded.
- If you configure the maximum number of IPv6 prefixes, which is 1,048,576 per prefix range, for the first 383 local address pools for Neighbor Discovery router advertisements by using the **ipv6 local ndra-pool *poolName*** command, the system-wide maximum limitation of 400,000,000 is reached. In such a case, if you attempt to configure the IPv6 prefix ranges to be allocated for the 384th pool, an error message is displayed stating that the prefix cannot be configured. Although all of the 500 IPv6 local address pools are configured correctly, you cannot configure prefixes for Neighbor Discovery from the 384th pool through the 500th pool because the maximum number of prefixes supported for the entire system is reached with the 383rd pool.
- You cannot configure overlapping prefix ranges in an IPv6 local pool. If you try to configure a prefix range that overlaps with an existing prefix range in the IPv6 local pool, an error message is displayed stating that the prefix range could not be configured. Similarly, an error message is displayed if you try to configure a prefix range in an IPv6 local pool that overlaps with a prefix range in another IPv6 local pool on the same virtual router.
- You can configure certain prefix ranges to be excluded from being used for allocation to the requesting subscriber.
- You can configure the name of an IPv6 local address pool in an AAA domain map using the **ipv6-ndra-pool-name** command in Domain Map Configuration mode. If the authentication server returns the IPv6 local address pool name in the Framed-IPv6-Pool attribute or Ipv6-NdRa-Pool attribute of the RADIUS-Access-Accept message, this pool overrides the IPv6 local address pool configured in the domain map.
- You cannot delete a pool or a prefix range from which prefixes have been allocated to requesting routers or Neighbor Discovery router advertisements clients. However, you can forcibly delete such a pool or prefix range by using the **force** keyword in the **ipv6 local ndra-pool *poolName*** and **ndraprefix** commands. If a pool is deleted or the prefix range associated with the pool is deleted forcibly, corresponding subscribers will be logged out forcibly.
- Two new RADIUS attributes are added: Ipv6-Ndra-Pool and Delegated-Ipv6-Pool. For more information on these attributes see Juniper Networks VSAs.
- You can issue the **aaa dhcpv6-ndra-pool override** command to use Framed-Ipv6-Pool attribute for IPv6 Neighbor Discovery router advertisements and the Delegated-Ipv6-Pool attribute for DHCPv6 Prefix Delegation. The **no** version of this command causes the Ipv6-NdRa-Pool attribute to be used for IPv6 Neighbor Discovery router advertisements and the Framed-Ipv6-Pool attribute to be used for DHCPv6 Prefix Delegation.
- If you want the IPv6-NdRa-Prefix attribute to be included in the Acct-Start messages that the router sends to the RADIUS server, you can use the **radius include**

**ipv6-ndra-prefix acct-start enable** command. In such a case, the prefix allocated to the subscriber from the IPv6 local address pool for Neighbor Discovery is included in the Ipv6-NdRa-Prefix attribute or the Framed-Ipv6-Prefix attribute.

Similarly, to cause the Ipv6-NdRa-Prefix attribute to be included in the Acct-Stop messages sent to the RADIUS server, you can use the **radius include ipv6-ndra-prefix acct-stop enable** command. You can use the **disable** keyword with the **radius include ipv6-ndra-prefix acct-start** and **radius include ipv6-ndra-prefix acct-stop** commands to prevent the Ipv6-NdRa-Prefix attribute to be sent in the Acct-Start or Acct-Stop messages.

**Related  
Documentation**

- [Configuring the DHCPv6 Local Address Pools on page 106](#)
- [Configuring IPv6 Neighbor Discovery Local Address Pools on page 108](#)
- [aaa dhcpv6-ndra-pool override on page 134](#)
- [ipv6 address-pool ndra on page 161](#)
- [ipv6 local ndra-pool on page 162](#)



## CHAPTER 9

# Validation of Duplicate Prefixes and Addresses

- [Duplicate IPv6 Prefix Check Overview on page 51](#)
- [Duplicate IPv6 Prefix Detection in the AAA User Profile Database Overview on page 51](#)
- [Guidelines for Duplicate Address Verification on page 52](#)

### Duplicate IPv6 Prefix Check Overview

---

You can configure AAA service to detect duplicates of IPv6 Neighbor Discovery router advertisement prefixes and DHCPv6 delegated prefixes. If a non-unique IPv6 prefix is detected by AAA, the subscriber session corresponding to the duplicate prefix is terminated.

In some network environments where the same customer logs in from multiple locations, terminating sessions with duplicate IPv6 prefixes might result in breaking subscriber setup. The duplicate IPv6 prefix-check capability is disabled by default.

If a duplicate prefix is detected by AAA before a subscriber is granted access, the subscriber is denied access. However in some cases, when two subscribers having the same IPv6 prefix log in simultaneously, the duplicate might be detected only after access is granted to both subscribers. AAA terminates the duplicate subscriber session immediately upon detecting the duplicate IPv6 prefix.



**NOTE:** AAA cannot detect duplicates of overlapping IPv6 prefixes.

#### Related Documentation

- [Configuring Duplicate IPv6 Prefix Check on page 127](#)
- [Standard RADIUS IPv6 Attributes for IPv6 Neighbor Discovery Router Advertisements and DHCPv6 Prefix Delegation Configuration on page 41](#)

### Duplicate IPv6 Prefix Detection in the AAA User Profile Database Overview

---

You can configure AAA service to detect duplicates of both IP and IPv6 Neighbor Discovery router advertisement prefixes, Framed-IPv6-Prefixes, and DHCPv6 delegated prefixes by validating the prefixes against the AAA database instead of the IP route table. If AAA

detects a non-unique IP address or IPv6 prefix, the corresponding subscriber session is terminated.

In some network environments where the same customer logs in from multiple locations, terminating sessions with duplicate IP addresses and IPv6 prefixes might result in breaking subscriber setup. The enhanced duplicate prefix detection capability is disabled by default. Because the prefix is validated against the AAA table, enabling the enhanced prefix detection capability may impact performance.

AAA maintains a new table for IPv6 prefixes and Framed-IP-Address information for subscribers. The AAA service checks for duplication of IP addresses and prefixes in this new table after PPP authorization. If a duplicate address or prefix is detected by AAA before a subscriber is granted access, the subscriber is denied access. However, in some cases, when two subscribers with the same IPv6 prefix log in simultaneously, the duplicate might be detected only after access is granted to both subscribers. AAA terminates the duplicate subscriber session immediately upon detecting the duplicate IPv6 prefix.

The following scenarios can occur during the establishment of subscriber sessions:

- When the RADIUS server assigns the same IPv6-NdRa-Prefix or Delegated-IPv6-Prefix to two subscribers, the second subscriber that contains the same prefix as the first subscriber is disconnected.
- When the RADIUS server assigns the same Framed-IPv6-Prefix to two dual-stack subscribers, the second subscriber session is rejected.
- When the RADIUS server assigns the same Framed-IP-Address and different IPv6 prefixes to two subscribers, the second subscriber session is terminated.



**NOTE:** AAA cannot detect duplicates of overlapping IPv6 prefixes. Also, the `aaa duplicate-prefix-check-extension` command detects duplicate prefixes globally for all VRs and is not limited to detecting duplicates on a per-VR basis.

---

**Related  
Documentation**

- [Configuring Detection of Duplicate IPv6 Prefixes in the AAA User Profile Database on page 127](#)
- [Monitoring Duplicate IPv6 Prefixes in the AAA User Profile Database](#)
- [Standard RADIUS IPv6 Attributes for IPv6 Neighbor Discovery Router Advertisements and DHCPv6 Prefix Delegation Configuration on page 41](#)
- [aaa duplicate-prefix-check-extension on page 145](#)
- [show aaa duplicate-prefix-check-extension on page 307](#)

---

## Guidelines for Duplicate Address Verification

In dual-stack networks in which both IPv4 and IPv6 subscribers are available, the subscribers might be granted the same IPv4 and IPv6 addresses if one user logs in quickly

after another user has logged in. To avoid the problem of two sessions containing the same address, when you enable detection of duplicate addresses, the subscriber is completely terminated when a duplicate IPv4 or IPv6 address is detected. The duplicate check operation is performed for 32-bit IPv4 subnet masks and IPv6 addresses with a prefix length of 128.

The value of the Framed-IPv6-Address attribute is determined using the Framed-IPv6-Prefix and Framed-Interface-Id attributes, normally obtained from the MAC addresses of clients in the PPP Network Control Protocol (NCP) phase in the PPP link connection process. Because the Framed-IPv6-Address attribute is not available to AAA during the authentication phase (before NCP negotiation occurs), the duplicate address detection mechanism performed for IPv4 cannot be adopted for IPv6. To achieve this functionality, if IPv6 detects a duplicate address while adding the route, it notifies AAA about the duplicate and AAA terminates the subscriber.

To correctly enable duplicate address detection when subscribers log in simultaneously, the IP and AAA applications examine the access-route table instead of the route table. In certain scenarios, AAA cannot detect whether a subscriber requesting access uses the same address as another subscriber. When the IP application detects a duplicate address while adding the route, the IP application notifies AAA about the duplication to terminate the connection for that subscriber.

In certain cases, when two subscribers with the same address attempt to log in, the duplicate might be detected only after access is granted to both subscribers. AAA terminates the duplicate subscriber session immediately upon detecting the duplicate address.

If AAA cannot determine the virtual router (VR) context configured in the profile during subscriber authentication, the subscriber that uses the same address as another subscriber is terminated immediately after the IP application detects the duplicate address. Such a disconnection of subscribers occurs even if the duplicate subscriber was granted access previously when the VR context was not available to AAA for processing.

In a dual-stack environment in which both IPv4 and IPv6 subscribers are present, if a subscriber that uses a duplicate IPv6 address is detected, the subscriber is denied access even if the IPv4 interface address is unique. This method of terminating subscriber sessions occurs to avoid duplicate sessions from being established in scenarios in which the IPv6 interface address is the same as another client, whereas the IPv4 interface address is unique.

The following scenarios can occur during the establishment of subscriber sessions in a dual-stack network in which clients using both IPv4 and IPv6 protocols are present, and when detection of duplicate addresses is enabled on the router that delegates addresses to requesting clients. These scenarios assume that the RADIUS server is configured on a VR other than the default VR and that the AAA domain name is mapped to a non-default VR.

- When the VR context for subscribers is configured in the AAA domain map or obtained from the RADIUS server, and the same IP address is returned for two dual-stack subscribers from the RADIUS server, only the first subscriber session is configured and the second client session is terminated.
- When the same IP address is returned from the RADIUS server or the domain map for two dual-stack subscribers that log in simultaneously, only the first subscriber session is established and the second subscriber that contains the same address or prefix as the first subscriber is disconnected. Termination of the second subscriber occurs even if detection of the duplicate address occurs only after access is granted.
- When the VR context for subscribers is configured in the AAA profile, and the same IP address is returned from the RADIUS server or the domain map for two dual-stack subscribers, only the first subscriber session is configured and the second client session is terminated.
- If you disable the routing table address lookup for duplicate addresses by using the **no aaa duplicate-address-check** command, define the VR context for subscribers in the profile, and the same address is returned for two dual-stack subscribers, both the subscriber sessions are brought up successfully. However, for the second subscriber, which contains the same address as the first client, only the IPv6 interface is enabled and the IPv4 interface is not brought up.
- If the same IPv6-NdRa-Prefix (VSA 26-129) and Framed-Interface-Id (VSA 26-96) attributes are returned in the Access-Accept message from the RADIUS server for two dual-stack subscribers, and the VR context for the subscribers is specified in the profile, only the first subscriber is brought up and the second subscriber session is rejected.
- If you set the Framed-IPv6-Prefix RADIUS attribute for IPv6 Neighbor Discovery router advertisements by using the **aaa ipv6-nd-ra-prefix framed-ipv6-prefix** command, the same Framed-IPv6-Prefix (VSA 26-129) and Framed-Interface-Id (VSA 26-96) attributes are returned in the Access-Accept message from the RADIUS server for two dual-stack subscribers, and the VR context for the subscribers is specified in the profile or the domain map, only the first subscriber is brought up and the second subscriber session is rejected.
- If you set the Framed-IPv6-Prefix RADIUS attribute for IPv6 Neighbor Discovery router advertisements by using the **aaa ipv6-nd-ra-prefix framed-ipv6-prefix** command, disable the routing table address lookup for duplicate addresses, specify the VR context for subscribers in the domain map, and the same Framed-IPv6-Prefix (VSA 26-129) and Framed-Interface-Id (VSA 26-96) attributes are returned in the Access-Accept message from the RADIUS server for two dual-stack subscribers, only the first subscriber is brought up and the second subscriber session is rejected.

**Related  
Documentation**

- [Configuring Duplicate IPv6 Prefix Check on page 127](#)

## CHAPTER 10

# Interoperation with SRC Software

- [SRC Client Configuration Overview on page 55](#)
- [SRC Client and COPS Terminology on page 55](#)
- [Retrieval of DSL Line Rate Information from Access Nodes Overview on page 58](#)

## SRC Client Configuration Overview

---

The JunosE Software has an embedded client that interacts with the Juniper Networks Session and Resource Control (SRC) software, enabling the SRC software to manage the router's policy and QoS configuration.

The connection between the router and the SRC software 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 SRC client functions as the COPS client, or policy enforcement point (PEP). The SRC software functions as the COPS server, or policy decision point (PDP).

Rate limiters are aggregated for dual-stack subscribers (IPv4 and IPv6) managed by the SRC software, using external parent groups and hierarchical policy parameters. The external parent groups and policy parameters are pushed to lower interfaces from the SRC software through the Siemens Selection Switch or Service Selection Center client.



**NOTE:** You cannot override aggregation node values while attaching policies to the interface.

### Related Documentation

- [Configuring the SRC Client on page 129](#)

## SRC Client and COPS Terminology

---

[Table 6 on page 56](#) provides common terms used in the COPS environment.

**Table 6: SRC 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 SRC software is the PDP.
PEP	Policy enforcement point; the COPS client, which enforces policy decisions. The JunosE COPS interface is a PEP.
PIB	Policy Information Base; a collection of sets of attributes that represent configuration information for a device.
SRC	Session and Resource Control (SRC) software, formerly the Service Deployment System (SDX) software; functions as a COPS PDP.

The JunosE Software 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.



**NOTE:** When you upgrade from an earlier JunosE release, the software removes the instance of SSCC that was configured with XDR.

If you are going to perform a unified ISSU from a JunosE release numbered lower than Release 10.0.0 and you have an XDR configuration, unified ISSU is not supported while an XDR configuration is presented.

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).

JunosE Software uses the following PIBs:

#### Proprietary PIB

- JunosE-IP-PIB—This PIB defines the data model for manipulating IP service policies and addresses offered through DHCP in JunosE Software.

#### Non-proprietary PIBs

- COPS-PR-SPPI
- COPS-PR-SPPI-TC
- DIFFSERV-PIB
- FRAMEWORK-FEEDBACK-PIB
- FRAMEWORK-PIB
- FRAMEWORK-TC-PIB

The COPS-PR support in JunosE Software uses the proprietary PIB. This PIB consists of a series of tables that is supported in previous JunosE Software releases, including the proprietary accounting and address assignment mechanisms.

You can force the router to restart a COPS connection to, and resynchronize with, a PDP, without disabling the SRC client's COPS support. The SRC software and the SRC client maintain common state information in PIBs that both the SRC software and the SRC client use. Previously, you disabled the SRC client and reenabled it to start synchronization. The disabling of the SRC client's COPS support was undesirable for the applications that required resynchronization in addition to maintaining the COPS support. If the state of the SRC software is not synchronized with the router, the SRC software may be required to initiate resynchronization from the router.

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

The JunosE-IP-PIB file is updated with each JunosE release. Since the PIB is implemented by both Juniper Networks SRC and JunosE devices, distribution of the PIB file to customers is not necessary. Customers can access the proprietary PIB file, on approval from Juniper Networks, through Juniper support.

---

## Retrieval of DSL Line Rate Information from Access Nodes Overview

---

You can retrieve updated DSL line rate information from the Access Node Control Protocol (ANCP) and report this information to the SRC software with corresponding COPS messages. ANCP is also known as Layer 2 Control (L2C). To enable the router that functions as the SRC client to obtain updated line rate parameters from ANCP and transmit them to the COPS server, use the **sscc update-policy-request enable** command in Global Configuration mode. You can configure this setting on a per-virtual-router basis.

In networks with digital subscriber line access multiplexers (DSLAMs), after a connection is established between an subscriber and a routing gateway, the access node or DSLAM obtains the line rate information of the subscriber using a synchronization process. The line rate parameters are transferred in the COPS interface request by using the ANCP topology discovery message to the router that functions as the network access server (NAS). Typically, a COPS interface request is sent from the access node to the SRC client whenever an interface becomes operational.

You can configure the SRC client to obtain the line rate details from the access node whenever any change in the values of the parameters occurs. The capability to receive line rate data, when it changes on the access node, is disabled by default on the SRC client.

The access node passes the DSL line rate parameters, whenever they change, to the SRC client. The SRC client appends updated parameters to the COPS messages that it sends to the COPS server or SRC server. A COPS server processes the following topology parameters that it receives from the SRC client in the updated COPS messages:

- JunosElpInterfaceMode
- JunosElpInterfaceUpstreamRate
- JunosElpInterfaceDownstreamRate

- JunosElpInterfaceMinimumDataRateUpstream
- JunosElpInterfaceMinimumDataRateDownstream
- JunosElpInterfaceAttainableDataRateUpstream
- JunosElpInterfaceAttainableDataRateDownstream
- JunosElpInterfaceMaximumDataRateUpstream
- JunosElpInterfaceMaximumDataRateDownstream
- JunosElpInterfaceMinimumLowPowerDataRateUpstream
- JunosElpInterfaceMinimumLowPowerDataRateDownstream
- JunosElpInterfaceMaximumInterleavingDelayUpstream
- JunosElpInterfaceActualInterleavingDelayUpstream
- JunosElpInterfaceMaximumInterleavingDelayDownstream
- JunosElpInterfaceActualInterleavingDelayDownstream
- JunosElpInterfaceDSLlinestate

A COPS server that runs an SRC software release earlier than Release 3.0.0 does not support and process the preceding topology parameters that are appended to the COPS messages. Such COPS servers analyze the information, other than the parameters that describe updated DSL line rate details, that they receive in the COPS messages for policy management. Therefore, the COPS-PR operation ensures backward compatibility of the SRC clients with the COPS servers running SRC software releases earlier than Release 3.0.0 by ignoring the received line rate details.

When you configure the **sscc update-policy-request enable** command, a warning message is displayed, prompting you to confirm whether you want to enable the router that functions as the SRC client to forcibly send line rate information parameters to the COPS server, which is running a release of SRC software earlier than Release 3.0.0 that is not compatible with the line rate message format.

Even if you confirm the prompt to enable the SRC client to forcibly send updated DSL line rate parameters to the COPS server, the COPS server that is running a release of SRC software earlier than Release 3.0.0 ignores the updated line rate details that it receives and processes only the other information in the COPS messages.

The Policy Information Base (PIB) is modified to extend the JunosElpInterfaceEntry object. ANCP now notifies the SRC software about any change in the ANCP parameters. If this change in rate is greater than 10 percent or a change in mode, SRC software reports this upgrade to the service activation engine (SAE) in SRC version 3.0.0 and later.

#### Related Documentation

- [SRC Client Configuration Overview on page 55](#)
- [Monitoring SRC Client Connection Status on page 253](#)
- **sscc update-policy-request enable**



# Application Terminate Reasons

- [AAA Terminate Reasons on page 61](#)
- [L2TP Terminate Reasons on page 62](#)
- [PPP Terminate Reasons on page 79](#)
- [RADIUS Client Terminate Reasons on page 86](#)

## AAA Terminate Reasons

[Table 7 on page 61](#) 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 7: 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

Table 7: Default AAA Mappings (*continued*)

AAA Shutdown or Deny Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
deny no access challenge support	17	user error
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

**Related Documentation**

- [Overview of Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 37](#)
- [Monitoring Application Terminate Reason Mappings on page 283](#)

## L2TP Terminate Reasons

Table 8 on page 62 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 8: 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

Table 8: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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

Table 8: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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

Table 8: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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 8: 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 scccn authenticate failed challenge	17	user error
tunnel rx scccn avp bad hidden	15	service unavailable
tunnel rx scccn avp bad value challenge response	15	service unavailable
tunnel rx scccn avp malformed bad length	15	service unavailable
tunnel rx scccn avp malformed truncated	15	service unavailable
tunnel rx scccn avp missing challenge response	17	user error
tunnel rx scccn avp missing random vector	15	service unavailable
tunnel rx scccn avp missing secret	15	service unavailable
tunnel rx scccn avp unexpected challenge response	15	service unavailable
tunnel rx scccn avp unknown	15	service unavailable
tunnel rx scccn no resources	15	service unavailable
tunnel rx scccn session id not null	15	service unavailable
tunnel rx scccn 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

Table 8: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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

Table 8: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 8: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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

Table 8: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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 sccrq admin close	6	admin reset
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

Table 8: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
tunnel rx recovery stopccn avp missing mandatory assigned tunnel id	15	service unavailable

Table 8: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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

**Related Documentation**

- [Overview of Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 37](#)
- [Configuring Custom Mappings for PPP Terminate Reasons](#)
- [Monitoring Application Terminate Reason Mappings on page 283](#)

## PPP Terminate Reasons

Table 9 on page 79 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 9: 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
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

Table 9: Default PPP Mappings (continued)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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

Table 9: Default PPP Mappings (continued)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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









## RADIUS Client Terminate Reasons

Table 10 on page 86 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 10: 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

**Related  
Documentation**

- [Overview of Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 37](#)
- [Monitoring Application Terminate Reason Mappings on page 283](#)

## PART 2

# Configuration

- [Configuring B-RAS Services on page 89](#)
- [Enabling the B-RAS Application on page 91](#)
- [Configuration Tasks for AAA Accounting on page 93](#)
- [Configuration Tasks for AAA Servers on page 95](#)
- [Configuration Tasks for AAA Authentication and User Database on page 99](#)
- [Configuration Tasks for Local Address Pools on page 105](#)
- [Configuring Clients Logging In to Interfaces on page 111](#)
- [Configuration Tasks for AAA Profiles on page 117](#)
- [Configuration Task for Route-Download Servers for IPv4 and IPv6 on page 123](#)
- [Configuration Tasks for Duplicate Prefixes Detection on page 127](#)
- [Configuring COPS Interworking with SRC Client on page 129](#)
- [Configuration Commands on page 133](#)
- [Examples on page 195](#)





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 Session and Resource Control (SRC) client (formerly the SDX client).
19. (Optional) Set baselines for AAA statistics or RADIUS authentication and accounting statistics.

**Related Documentation**

- [Remote Access Overview on page 3](#)















## Configuring WINS Primary and Secondary NMS

---

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.

**Related Documentation**

- [aaa wins](#)























- [aaa dhcpv6-ndra-pool override on page 134](#)
- [exclude-ndraprefix on page 151](#)
- [ipv6 address-pool ndra on page 161](#)
- [ipv6 local ndra-pool on page 162](#)
- [ndraprefix on page 164](#)





























- `aaa route-download ipv6`
- `key`
- `radius route-download server`
- [show aaa route-download on page 313](#)
- [udp-port on page 192](#)













1. Create a PPP profile.

```
host1(config)#profile pppprofile1
```

2. Configure the transmission of COPS request messages to the SRC server for all subscribers that are assigned this PPP profile.

```
host1(config)#ip send-cops-request
```

By default, COPS messages are sent to the SRC server. You must configure at least one IP configuration parameter in the PPP profile to enable the default behavior of the command to be effective. This functionality is applicable in environments where PPP links between the customer premises equipment (CPE) and the provider edge (PE) device or the router are configured for IPv4 or IPv6 subscriber sessions, either as independent or combined sessions. Also, this capability is effective only for dynamic PPP subscribers and not for DHCP and static subscriber sessions.

Use the **no** version to disable the transmission of COPS messages from the SRC client to the SRC server for PPP subscribers.

**Related Documentation**

- [ip send-cops-request on page 152](#)

## CHAPTER 23

# Configuration Commands

## aaa dhcpv6-ndra-pool override

---

**Syntax** [ no ] aaa dhcpv6-ndra-pool override

**Release Information** Command introduced in JunosE Release 13.0.0.

**Description** If the authentication server returns the Neighbor Discovery router advertisement prefix pool name in the RADIUS-Accept-Request message, it causes the Framed-Ipv6-Pool attribute to be used for IPv6 Neighbor Discovery router advertisements and the Delegated-Ipv6-Pool attribute to be used for DHCPv6 Prefix Delegation. The **no** version of this command causes the Ipv6-NdRa-Pool attribute to be used for IPv6 Neighbor Discovery router advertisements and the Framed-Ipv6-Pool attribute to be used for DHCPv6 Prefix Delegation. When the Ipv6-NdRa-Pool attribute is used for Neighbor Discovery, the prefix to be allocated to requesting routers or subscribers is obtained from the IPv6 local address pool for Neighbor Discovery. When the Delegated-Ipv6-Pool attribute is used for Prefix Delegation, the prefix to be delegated to the clients is obtained from the IPv6 local address pool for Prefix Delegation.

**Mode** Global Configuration

**Related Documentation**

- [Configuring IPv6 Neighbor Discovery Local Address Pools on page 108](#)

## aaa dns

---

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

**Release Information**    Command introduced before JunosE Release 7.1.0.

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

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

**Mode**    Global Configuration

## aaa ipv6-dns

---

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

**Release Information**    Command introduced before JunosE Release 7.1.0.

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

**Options**

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

**Mode**    Global Configuration

## aaa accounting duplication

---

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

**Release Information**    Command introduced before JunosE Release 7.1.0.

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

**Options**    • *routerName*—Virtual router name

**Mode**    Global Configuration

## aaa accounting broadcast

---

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

**Release Information**    Command introduced before JunosE Release 7.1.0.

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

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

**Mode**    Global Configuration

## aaa accounting statistics

---

**Syntax**   aaa accounting statistics { volume-time | time }  
no aaa accounting statistics

**Release Information**   Command introduced in JunosE Release 7.2.0.

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

**Options**

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

**Mode**   Global Configuration

## aaa accounting vr-group

---

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

**Release Information** Command introduced before JunosE Release 7.1.0.

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

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

**Mode** Global Configuration

---

## aaa authentication default

---

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

**Release Information**    Command introduced before JunosE Release 7.1.0.

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

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

**Mode**    Global Configuration

## aaa domain-map

---

**Syntax**    `aaa domain-map domainName`  
              `[ routerName [ loopback interfaceNumber | ipAddress ipMask ] ]`  
  
              `no aaa domain-map domainName`

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

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

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

**Mode**    Global Configuration

---

## aaa duplicate-address-check

---

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

**Release Information**   Command introduced before JunosE Release 7.1.0.

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



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

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

**Mode**   Global Configuration

## aaa duplicate-prefix-check

---

**Syntax** [ no | default ] aaa duplicate-prefix-check { enable | disable }

**Release Information** Command introduced in JunosE Release 11.2.0.

**Description** Configures AAA to enable duplicate IPv6 prefix-check in a virtual router context. Duplicate IPv6 prefix checking by AAA is disabled by default . The **default** version restores the default condition. The **no** version disables the duplicate IPv6 prefix-check capability.

**Options**

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

**Mode** Global Configuration

## aaa duplicate-prefix-check-extension

---

**Syntax** [ no | default ] aaa duplicate-prefix-check-extension { enable | disable }

**Release Information** Command introduced in JunosE Release 12.2.0.

**Description** Configures AAA to enable the enhanced duplicate IPv6 prefix-check in a virtual router context. Enhanced duplicate IPv6 prefix checking by AAA is disabled by default . The **no** version disables the enhanced duplicate IPv6 prefix-check capability.

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

**Mode** Global Configuration

## aaa local select database

---

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

**Release Information**    Command introduced before JunosE Release 7.1.0.

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

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

**Mode**    Global Configuration

## aaa local username

---

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

**Release Information** Command introduced before JunosE Release 7.1.0.

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

**Options**

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

**Mode** Global Configuration

## dns-domain-search

---

**Syntax** [ no ] dns-domain-search *domainName*

**Release Information** Command introduced in JunosE Release 10.1.0.

**Description** Specifies a list of domain names in the IPv6 local address pool to be returned to clients in DHCPv6 responses as part of the Domain Search List option. The **no** version removes the configured domain name.



.....  
**NOTE:** You can configure one domain name per line. Enter the command on separate lines to configure additional domain names.  
.....

**Options**

- *domainName*—Domain name that the DHCPv6 client uses when it resolves hostnames with the DNS server. You can specify a maximum of four DNS domains for the search list of an IPv6 local pool; maximum of 32 characters

**Mode** IPv6 Local Pool Configuration

## dns-server

---

**Syntax**    `dns-server ipAddressPrimary [ ipAddressSecondary ]`  
              `no dns-server`

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Assigns a DNS server to an address pool. The **no** version removes the association between the address pool and the DNS server.

- Options**
- *ipAddressPrimary*—IP address of preferred DNS server
  - *ipAddressSecondary*—IP address of secondary DNS server

**Mode**    DHCP Local Pool Configuration

## exclude-prefix

---

**Syntax** [ no ] exclude-prefix *Ipv6Prefix* [ *endIpv6prefix* ]

**Release Information** Command introduced in JunosE Release 10.1.0.

**Description** Specifies the IPv6 prefix or range of prefixes to exclude from being allocated to the requesting router. You can exclude those prefixes that have been assigned to local interfaces from being delegated to the DHCPv6 clients. The **no** version removes the IPv6 prefix or prefix range from the exclusion set and makes it available again for delegation to clients.



**NOTE:** If you attempt to exclude a prefix range that overlaps with another prefix range that has been already excluded from delegation to clients in the IPv6 local address pool, an error message is displayed and the configuration fails.

- Options**
- *Ipv6Prefix*—IPv6 prefix or the starting IPv6 prefix of the range of prefixes to be excluded from being delegated to the requesting router.
  - *endIpv6Prefix*—Ending prefix of the range of IPv6 prefixes to be excluded from being delegated to the requesting router. If you specify this value, all prefixes from the starting IPv6 prefix up to this prefix are excluded from allocation.

**Mode** IPv6 Local Pool Configuration

## exclude-ndraprefix

**Syntax** [ no ] exclude-ndraprefix *IPv6Prefix* [ *endIPv6prefix* ]

**Release Information** Command introduced in JunosE Release 13.0.0.

**Description** Specifies the IPv6 prefix or range of prefixes to exclude from being allocated to the requesting router. You can exclude those prefixes that have been assigned to local interfaces from being delegated to the Neighbor Discovery router advertisement clients. The **no** version removes the IPv6 prefix or prefix range from the exclusion set and makes it available again for delegation to clients.



**NOTE:** If you attempt to exclude a prefix range that overlaps with another prefix range that has been already excluded from delegation to clients in the IPv6 local address pool, an error message is displayed and the configuration fails.

- Options**
- *IPv6Prefix*—IPv6 prefix or the starting IPv6 prefix of the range of prefixes to be excluded from being delegated to the requesting router
  - *endIPv6Prefix*—Ending prefix of the range of IPv6 prefixes to be excluded from being delegated to the requesting router. If you specify this value, all prefixes from the starting IPv6 prefix up to this prefix are excluded from allocation.

**Mode** IPv6 NdRa Pool Configuration

**Related Documentation**

- [Configuring IPv6 Neighbor Discovery Local Address Pools on page 108](#)

## ip send-cops-request

---

**Syntax** [ no ] ip send-cops-request

**Release Information** Command introduced in JunosE Release 13.3.0.

**Description** Enables the SRC client, which functions as the Common Open Policy Service (COPS) client, to send COPS messages to the SRC server or the COPS server based on the dynamic configuration manager (DCM) profile. This functionality is applicable only to dynamic PPP interfaces where the PPP links are configured for IPv4 or IPv6 subscriber sessions, either as independent or combined sessions. This behavior is not applicable for DHCP and static subscribers. By default, COPS messages are sent to the SRC server. You must configure at least one IP configuration parameter in the PPP profile to enable the default behavior of the command to be effective.

The **no** version disables the transmission of COPS messages from the SRC client to the SRC server for PPP subscribers.

**Mode** Profile Configuration

**Related Documentation**

- [Configuring the Forwarding of COPS Requests to the SRC Server Based on DCM Profiles on page 131](#)

## ipv6 address

**Syntax** [ no ] ipv6 address *ipv6Prefix* [ eui-64 ]  
 [ no ] ipv6 address [ *ipv6Address maskLength* [ eui-64 ] ]

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** Assigns an IPv6 address (or network) to an interface and enables IPv6 processing on that interface. The **no** version deletes the association from the interface.



**NOTE:** The link-local address for an interface is automatically configured when IPv6 is enabled on the interface.

- Options**
- *ipv6Prefix*—Prefix that defines the IPv6 interface or network in the format *ipv6Address / length*, where
    - *ipv6Address*—Base IPv6 address of the network route that you want to filter (for example, ::ffff:a:b:c:d)
    - *length*—Length of the network prefix; number of bits masking base address to produce address to be matched
  - *ipv6Address*—Base IPv6 address of the network route that you want to filter (for example, ::ffff:a:b:c:d); the *ipv6Address* must appear in hexadecimal format using 16-bit values between colons. Refer to RFC 2373—IP Version 6 Addressing Architecture (July 1998) for details.
  - *maskLength*—Length of the IPv6 mask. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).
  - eui-64—Specifies the use of the eui-64 interface identifier

**Mode** Interface Configuration, Profile Configuration

## ipv6 nd

---

**Syntax** [ no ] ipv6 nd

**Release Information** Command introduced before JunosE Release 7.1.0.  
Profile Configuration mode added in JunosE Release 9.0.0.

**Description** Enables the IPv6 Neighbor Discovery process on an interface. By default, the IPv6 Neighbor Discovery process is disabled on the router. However, if you configure an IPv6 address on a static interface, Neighbor Discovery process is automatically enabled. The **no** version disables the Neighbor Discovery process.

**Mode** Interface Configuration, Profile Configuration

## ipv6 unnumbered

**Syntax** `ipv6 unnumbered interfaceType interfaceSpecifier`  
`no ipv6 unnumbered`

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** Enables or disables IPv6 processing on an interface without assigning an explicit IPv6 address to that interface. The global IPv6 address of the interface, specified by the *interfaceType interfaceSpecifier* values, becomes the source address in packets that the unnumbered interface generates. Unnumbered interfaces are often used in point-to-point connections where an IPv6 address is not required. You must specify an interface location, which is the identifier of another interface on which the router has an assigned IPv6 address. This interface cannot be another unnumbered interface. The **no** version of the command removes the IPv6 address from the interface.



**NOTE:** Enabling IPv6 on an interface automatically configures the link-local address on an unnumbered interface.

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

**Mode** Interface Configuration, Profile Configuration

## prefix

**Syntax** `prefix startIpv6Prefix { assignedPrefixLength | endIpv6Prefix } [ [ preferred | valid ] { days [ hours [ minutes [ seconds ] ] ] | infinite } ]`

`no prefix startIpv6Prefix [ force | preferred [ valid ] | valid ]`

**Release Information** Command introduced in JunosE Release 10.1.0.

**Description** Specifies the prefix range from which IPv6 prefixes can be assigned to the DHCPv6 client. Also, configures the duration of time for which the requesting router can use the delegated prefix. If no value is specified for preferred or valid lifetime, the default lifetime of 1 day is used for the delegated prefix. The **no** version removes the IPv6 prefix range from the local address pool. You can also forcibly delete an IPv6 prefix range from which prefixes have been allocated.



**NOTE:** If you attempt to configure a prefix range that overlaps with an existing prefix range in the same pool, an error message is displayed and the configuration fails. Also, an error message is displayed if you try to configure a prefix range that overlaps with a prefix range in another IPv6 local address pool on the same virtual router.

- Options**
- *startIpv6Prefix*—Starting IPv6 prefix of the range of prefixes to be delegated to requesting routers.
  - *endIpv6Prefix*—Ending IPv6 prefix of the range of prefixes to be delegated to requesting routers.
  - *assignedPrefixLength*—Length of the IPv6 prefix to be assigned from this range of prefixes to the requesting router.
  - *preferred*—Specifies use of the preferred period of time for the requesting router to use the prefix delegated by the DHCPv6 server. If the preferred lifetime is not specified, the prefix can be used by the requesting router for the default period of 1 day.
  - *valid*—Specifies use of the valid period of time for the requesting router to use the prefix delegated by the DHCPv6 server. If the valid lifetime is not specified, the prefix can be used by the requesting router for the default period of 1 day.



**NOTE:** Although you can configure the valid lifetime for a prefix, the DHCPv6 server does not consider this value. The DHCPv6 server uses only the preferred lifetime for a prefix to determine the amount of time for which a prefix can be used by the requesting router.

- *days*—Number of days for the preferred or valid lifetime; in the range 0-32768.
- *hours*—Number of hours for the preferred or valid lifetime; in the range 0-24.

- *minutes*—Number of minutes for the preferred or valid lifetime; in the range 0-60.
- *seconds*—Number of seconds for the preferred or valid lifetime; in the range 0-60.
- *infinite*—Assigns a preferred or valid lifetime that does not expire for the delegated prefix.
- *force*—Forcibly deletes the IPv6 prefix range from the local address pool.

**Mode**    IPv6 Local Pool Configuration

## ipv6 address-pool local

---

**Syntax** [ no ] ipv6 address-pool local

**Release Information** Command introduced in JunosE Release 10.1.0.

**Description** Enables the IPv6 local address pool functionality to allow configuration of IPv6 local address pools to assign prefixes to DHCPv6 clients. The **no** version disables the IPv6 local address functionality.



.....  
**NOTE:** If you attempt to configure an IPv6 local address pool without enabling the IPv6 local pool feature, an error message is displayed.  
.....

**Mode** Global Configuration

## ipv6 local pool

---

**Syntax**    `ipv6 local pool poolName`  
              `no ipv6 local pool poolName [ force ]`

**Release Information**    Command introduced in JunosE Release 10.1.0.

**Description**    Accesses IPv6 Local Pool Configuration mode. Specifies the IPv6 local address pool from which prefixes are allocated to the requesting router in networks that use DHCPv6. The **no** version removes the IPv6 local pool.

- Options**
- *poolName*—Name of the IPv6 local address pool to be used to delegate prefixes to the requesting routers or DHCPv6 clients; string of up to 16 alphanumeric characters
  - *force*—Forcibly deletes an IPv6 local address pool from which prefixes have been allocated. When a pool from which prefixes have been assigned to DHCPv6 clients is deleted, the corresponding DHCPv6 bindings are also deleted.

**Mode**    Global Configuration

## ipv6-prefix-pool-name

---

**Syntax**    `ipv6-prefix-pool-name poolName`  
              `no ipv6-prefix-pool-name`

**Release Information**    Command introduced in JunosE Release 10.1.0.

**Description**    Specifies the IPv6 local prefix pool name to be used to delegate prefixes to the requesting router, when the RADIUS server does not return a pool name using the Framed-IPv6-Pool attribute. The **no** version removes the IPv6 local pool from the AAA domain map.

**Options**

- *poolName*—Name of the IPv6 local prefix pool to associate with the domain name; string of up to 16 alphanumeric characters

**Mode**    Domain Map Configuration

---

## ipv6 address-pool ndra

---

**Syntax** [ no ] ipv6 address-pool ndra

**Release Information** Command introduced in JunosE Release 13.0.0.

**Description** Enables the IPv6 local address pool functionality to allow configuration of IPv6 local address pools for Neighbor Discovery router advertisements to assign prefixes to Neighbor Discovery router advertisements. The **no** version disables the IPv6 local address functionality for Neighbor Discovery router advertisements.



.....  
**NOTE:** If you attempt to configure an IPv6 local address pools for Neighbor Discovery router advertisements without enabling the IPv6 local address pools for Neighbor Discovery router advertisements feature, an error message is displayed.  
.....

**Mode** Global Configuration

**Related Documentation**

- [Configuring IPv6 Neighbor Discovery Local Address Pools on page 108](#)

## ipv6 local ndra-pool

---

**Syntax**    `ipv6 local ndra-pool poolName`  
`no ipv6 local ndra-pool poolName [ force ]`

**Release Information**    Command introduced in JunosE Release 13.0.0.

**Description**    Accesses IPv6 NdRa Pool Configuration mode. Specifies the IPv6 local address pool from which prefixes are allocated to the requesting router in networks that use Neighbor Discovery router advertisements. The **no** version removes the IPv6 local address pool.

- Options**
- *poolName*—Name of the IPv6 local address pool to be used to delegate prefixes to the requesting routers or Neighbor Discovery router advertisement clients; string of up to 16 alphanumeric characters
  - *force*—Forcibly deletes an IPv6 local address pool from which prefixes have been allocated. When a pool from which prefixes have been assigned to Neighbor Discovery router advertisement clients is deleted, the corresponding Neighbor Discovery router advertisement bindings are also deleted.

**Mode**    Global Configuration

**Related Documentation**

- [Configuring IPv6 Neighbor Discovery Local Address Pools on page 108](#)

## license b-ras

---

**Syntax**    `license b-ras licenseKey`

`no license b-ras`

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Specifies the B-RAS license provided by your sales representative or Juniper Networks Customer Service. Depending on the license purchased, the router supports up to 2,000, 4,000, 8,000, 16,000, or 20,000 authenticated PPP or SRC sessions. The **no** version disables the license.

**Options**    • *licenseKey*—Unique string of up to 15 alphanumeric characters that we provide to you

**Mode**    Global Configuration



## radius override nas-info

---

**Syntax** [ no ] radius override nas-info

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** Configures the RADIUS client for a virtual router context to override the standard use of the NAS-IP-Address [4] and NAS-Identifier [32] attributes when the client performs AAA broadcast accounting. Normally, AAA accounting packets include the NAS-IP-Address and NAS-Identifier attributes of the virtual router that generates the accounting information. However, this command specifies that the broadcast accounting packets instead include the authenticating virtual router's NAS-IP-Address and NAS-Identifier attributes. The **no** version restores the standard use of the two attributes in AAA accounting information.

**Mode** Global Configuration

## radius accounting server

---

**Syntax** [ no ] radius accounting server *ipAddress*

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** Specifies the IP address of a RADIUS accounting server and puts the E Series router into RADIUS Configuration mode. The **no** version deletes the instance of the RADIUS server.

**Options** • *ipAddress*—IP address of the server

**Mode** Global Configuration

## radius authentication server

---

**Syntax** [ no ] radius authentication server *ipAddress*

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** Specifies the IP address of a RADIUS authentication server and puts the E Series router into RADIUS Configuration mode. The **no** version deletes the instance of the RADIUS server.

**Options** • *ipAddress*—IP address of the server

**Mode** Global Configuration

## radius rollover-on-reject

---

**Syntax** radius rollover-on-reject { enable | disable }  
no radius rollover-on-reject

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** On a virtual router, specifies whether the router should roll over to the next RADIUS server when the router receives an access-reject message for the user it is authenticating. The **no** version restores the default value, disable.

**Options**

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

**Mode** Global Configuration

## radius tunnel-accounting

---

**Syntax**    radius tunnel-accounting { enable | disable }  
              no radius tunnel-accounting

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Enables or disables tunnel accounting. The **no** version restores the default value, disable.

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

**Mode**    Global Configuration

## radius udp-checksum

---

**Syntax**    radius udp-checksum { enable | disable }  
             no radius udp-checksum

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Enables or disables UDP checksum for RADIUS packets on virtual routers that you configure for B-RAS. The **no** version restores the default value, enable.

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

**Mode**    Global Configuration

## radius trap acct-server-responding

---

**Syntax** radius trap acct-server-responding { enable | disable }  
no radius trap acct-server-responding

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** Enables or disables SNMP traps when a RADIUS accounting server returns to service after being marked as unavailable. The **no** version restores the default, disable.

**Options**

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

**Mode** Global Configuration

## radius trap acct-server-not-responding

---

**Syntax**    radius trap acct-server-not-responding { enable | disable }  
              no radius trap acct-server-not-responding

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Enables or disables SNMP traps when a RADIUS accounting server fails to respond to a RADIUS accounting request. The **no** version restores the default, disable.

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

**Mode**    Global Configuration

## radius trap no-acct-server-responding

---

**Syntax**    radius trap no-acct-server-responding { enable | disable }  
              no radius trap no-acct-server-responding

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Enables or disables SNMP traps when all the configured RADIUS accounting servers per VR fail to respond to a RADIUS accounting request. The **no** version restores the default, disable.

**Options**

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

**Mode**    Global Configuration

## radius trap auth-server-responding

---

**Syntax**    radius trap auth-server-responding { enable | disable }  
              no radius trap auth-server-responding

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Enables or disables SNMP traps when a RADIUS authentication server returns to service after being marked as unavailable. The **no** version restores the default, disable.

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

**Mode**    Global Configuration

## radius trap auth-server-not-responding

---

**Syntax** radius trap auth-server-not-responding { enable | disable }  
no radius trap auth-server-not-responding

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** Enables or disables SNMP traps when a RADIUS authentication server fails to respond to a RADIUS Access-Request message. The **no** version restores the default, disable.

**Options**

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

**Mode** Global Configuration

## radius trap no-auth-server-responding

---

**Syntax**    radius trap no-auth-server-responding { enable | disable }  
              no radius trap no-auth-server-responding

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Enables or disables SNMP traps when all the configured RADIUS authentication servers per VR fail to respond to a RADIUS Access-Request message. The **no** version restores the default, disable.

**Options**

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

**Mode**    Global Configuration

## retransmit

---

**Syntax**    `retransmit retries`

`no retransmit`

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Specifies the maximum number of times a router retransmits a RADIUS packet to an authentication or accounting server. The **no** version restores the default value.

**Options**    • *retries*—Number of retries, in the range 0–100; default value is 3

**Mode**    RADIUS Configuration

## snmp-server

---

**Syntax** [ no ] snmp-server

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** Enables the SNMP agent operation. The **no** version disables this operation.

**Mode** Global Configuration

---

## snmp-server community

---

**Syntax**    `snmp-server community commString [ view viewName ] [ priv ] [ accessListName ]`  
              `no snmp-server community commString`

**Release Information**    Command introduced before JunosE Release 7.1.0.  
                              **view** keyword and *viewName* variable added in JunosE Release 7.1.0.

**Description**    Configures an authorized SNMP community and associates SNMPv1/v2c communities with SNMPv3 views. The **no** version removes an authorized community from the list of communities.

- Options**
- *commString*—Name of the SNMPv1/v2c community
  - *viewName*—Name of the SNMPv3 view, which allows configuration using available dynamic views
  - *priv*—Privileged Exec level: ro (read-only), rw (read-write), or admin (administrator)
  - *accessListName*—Name of IP access list to filter SNMP clients

**Mode**    Global Configuration



- `ldp`—LDP traps
- `link`—SNMP linkUp and linkDown traps
- `log`—System log capacity traps
- `mobileipv4`—Mobile IPv4 traps
- `mplste`—Mplste traps
- `mrouter`—Mrouter traps
- `ntp`—E Series router proprietary traps
- `ospf`—OSPF traps
- `packetMirror`—Secure packet mirroring traps; visible only if packet mirroring is enabled
- `pim`—PIM traps
- `ping`—Ping operation traps (in `disman remops` MIB)
- `radius`—RADIUS authentication and authorization servers
- `routeTable`—Maximum route limit and warning threshold traps; when this trap is generated, the actual value of the exceeded warning threshold is displayed
- `sonet`—SONET traps
- `snmp`—SNMP coldStart, warmStart, link, and authenticationFailure traps
- `traceroute`—Traceroute operation traps (in `disman remops` MIB)
- `vrrp`—VRRP traps
- `snmp`—Specifies the SNMP coldStart, warmStart, and authenticationFailure traps
- `authentication`—Specifies the SNMP authenticationFailure trap
- `trapFilters`—Specifies the trap severity level at a global level; if the per-category trap severity level is not set for a particular category, this setting is applied to that category
- `trapFilter`—Minimum severity level for filtering traps at a global level or for a specified category
  - `emergency`—Severity level 0
  - `alert`—Severity level 1
  - `critical`—Severity level 2
  - `error`—Severity level 3
  - `warning`—Severity level 4
  - `notice`—Severity level 5

- informational—Severity level 6
- debug—Severity level 7
- per-category-trapFilters—Specifies the trap severity level for a particular category; this setting overrides the severity level set at the global level for this category
- *trapFilter*—Minimum severity level for filtering traps for the specified category

**Mode** Global Configuration

**Related Documentation** • Monitoring SNMP Secure Packet Mirroring Traps



- dvmrp—DVMRP traps
- dvmrpUni—E Series router proprietary DVMRP traps
- environment—Power/temperature/fan traps
- fileXfer—File transfer status change traps
- inventory—Router inventory/status traps
- ip—Internet Protocol traps
- ldp—LDP traps
- link—SNMP linkUp/linkDown traps
- log—System log capacity traps
- mobileIpv4—Mobile IPv4 traps
- mplste—Mplste traps
- mrouter—Mrouter traps
- packetMirror—Secure packet mirroring traps; visible only if packet mirroring is enabled
- ospf—OSPF traps
- ping—Ping operation traps (in disman remops MIB)
- radius—RADIUS traps
- snmp—SNMP coldstart, warmstart, link, authenticationFailure traps
- traceroute—Traceroute operation traps (in disman remops MIB)
- \*—Indicates that one or more parameters can be repeated multiple times in a list in the command line
- *trapFilter*—Minimum severity level for filtering traps sent to this host
  - alert—Severity level 1
  - critical—Severity level 2
  - debug—Severity level 7
  - emergency—Severity level 0
  - error—Severity level 3
  - informational—Severity level 6
  - notice—Severity level 5
  - warning—Severity level 4

- *timeOutValue*—Ping timeout in minutes, in the range 1–90; default value is 1
- *trapQueue*—Configures the SNMP trap queue for traps sent to this host
- *queueDrainRate*—Maximum number of traps per second to be sent to the host, in the range 0–2147483647; default value is 0. By default, there is no limit on the number of traps sent per second to the host.
- *queueFull*—Method used to drop traps when the trap queue is full
  - *dropFirstIn*—Drops the oldest trap in the queue
  - *dropLastIn*—Drops the most recent trap added to the queue
- *queueSize*—Maximum number of traps to be kept in the trap queue, in the range 32–214748364; default value is 32

**Mode**    Global Configuration

**Related Documentation**    • Monitoring SNMP Secure Packet Mirroring Traps





## sscc enable

---

**Syntax**    `sscc enable cops-pr`  
`no sscc enable`

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Enables the SRC client's COPS support, which is used when the SRC service application engine communicates with a policy decision point, such as the SRC application. The **no** version disables COPS support.

**Options**

- `cops-pr`—Enables COPS-policy provisioning operation.

**Mode**    Global Configuration



- `send-local-qos-profile-config`—Enables the local QoS profile attachment information to be sent to the PDP
- `send-lac-nas-ip`—Enables the LAC side NAS-IP address information to be sent to the PDP
- `send-lac-nas-port`—Enables the LAC side NAS-Port information to be sent to the PDP

**Mode**    Global Configuration





































## PART 3

# Administration

- [Monitoring AAA Server and Authentication Settings on page 211](#)
- [Monitoring AAA Accounting Details on page 219](#)
- [Monitoring the Mapping of User Domains to Virtual Routers on page 223](#)
- [Verifying Settings for Detection of Duplicate Prefixes on page 229](#)
- [Monitoring AAA Profiles and Subscriber Sessions on page 231](#)
- [Monitoring Route-Download Server Settings on page 235](#)
- [Monitoring AAA Accounting Details on page 243](#)
- [Monitoring COPS Layer Settings on page 247](#)
- [Monitoring SRC Client Settings on page 253](#)
- [Monitoring the IP Local Address Pools Configuration on page 261](#)
- [Monitoring RADIUS Servers and Services for AAA Features on page 265](#)
- [Verifying Active Subscriber Session Details on page 275](#)
- [Investigating Causes for Termination of User Sessions on page 283](#)
- [Monitoring IPv6 Local Address Pool Settings on page 285](#)
- [Monitoring Commands on page 293](#)























```
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
```

**Meaning** [Table 16 on page 221](#) lists the **show aaa accounting vr-group** command output fields.

**Table 16: show aaa accounting vr-group Output Fields**

Field Name	Field Description
vr-group	Name of the virtual router group

- Related Documentation**
- [Configuring AAA Broadcast Accounting on page 93](#)
  - `show aaa accounting vr-group`











```
host1#show aaa domain-map
Domain: tunnel.com; auth-router-name: default; ip-router-name: default
ipv6-router-name: default; tunnel-subscriber authentication: enable
```

**Meaning** Authentication is enabled.

**Related Documentation** • [show aaa domain-map on page 305](#)





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

**Meaning** Refer to the description of the **show ip route** command in *JunosE IP, IPv6, and IGP Configuration Guide* for additional information about the **show ip route** command.

**Related Documentation**

- [show ip route on page 328](#)





## Monitoring Session Timeouts

---

**Purpose** Display idle and session timeouts.

**Action** To display idle and session timeouts:

```
host1#show aaa timeout  
idle timeout 1200 seconds monitor ingress only  
session timeout 3600 seconds
```

**Related Documentation**

- [show aaa timeout on page 321](#)



































Table 26: show cops statistics Output Fields (*continued*)

Field Name	Field Description
CC Rcv	Number of Client Closes packets received on this COPS session
SSC Sent	Number of Sync Complete packets sent on this COPS session

**Related Documentation**

- [show cops statistics on page 324](#)













































**Related Documentation**

- [show radius update-source-addr](#)













Table 36: show subscribers Output Fields (*continued*)

Field Name	Field Description
Slot	Number of slot in the chassis

**Related Documentation**

- [show subscribers on page 343](#)























## CHAPTER 39

# Monitoring Commands

## baseline aaa

---

**Syntax**    baseline aaa

**Release Information**    Command introduced before JunosE Release 7.1.0.

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

**Mode**    Privileged Exec



## baseline cops

---

**Syntax**   baseline cops

**Release Information**   Command introduced in JunosE Release 7.1.0.

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

**Mode**   Privileged Exec

## baseline local pool

---

**Syntax**    baseline local pool

**Release Information**    Command introduced before JunosE Release 7.1.0.

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

**Mode**    Privileged Exec

## baseline radius

---

**Syntax**    baseline radius

**Release Information**    Command introduced before JunosE Release 7.1.0.

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

**Mode**    Privileged Exec

## baseline ssc

---

**Syntax**    baseline ssc

**Release Information**    Command introduced in JunosE Release 7.1.0.

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

**Mode**    Privileged Exec





































## show aaa statistics

---

**Syntax**    show aaa statistics [ *delta* ] [ *filter* ]

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Displays the authentication and authorization statistics.

- Options**
- *delta*—Displays baselined statistics
  - *filter*—See Filtering show Commands

**Mode**    Privileged Exec





## show aaa timeout

---

**Syntax**    show aaa timeout [ *filter* ]

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Displays information about the idle and session timeouts.

**Options**    • *filter*—See Filtering show Commands

**Mode**    Privileged Exec









## show ip local pool

---

**Syntax**    show ip local pool [ *poolName* | statistics [ delta ] ] [ *filter* ]

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Displays information about the local address pools configured on the router.

- Options**
- *poolName*—Name of a specific local address pool
  - statistics—Specifies that local pool statistics are to be shown
  - delta—Displays baselined statistics
  - *filter*—See Filtering show Commands

**Mode**    Privileged Exec

## show ip local shared-pool

---

**Syntax**    show ip local shared-pool [ *poolName* ] [ *filter* ]

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Displays information about the shared local address pools configured on the router.

**Options**

- *poolName*—Name of a specific shared local address pool
- *filter*—See Filtering show Commands

**Mode**    Privileged Exec



- *static*—Displays the best static routes added by network management to the routing table
- *static-rpf*—Displays the best static RPF routes added by network management to the routing table
- *summary*—Displays summary counters for all routes in the IP routing table
- *filter*—See Filtering show Commands

**Mode** Privileged Exec, User Exec





























- *profileName*—Displays subscribers that share the same profile name
- *slot*—Displays active subscribers for the slot
- *slotNumber*—Number of the chassis slot of the line module in the range 0–2 (ERX310 model), 0–6 (ERX7xx models), 0–13 (ERX14xx models), 0–5 (E120 router), and 0–16 (E320 router)
- *virtual-router*—Displays active subscribers for the VR
- *vrName*—Name of the VR to which interfaces of active subscribers are bound
- *lag*—Displays the consolidated information about active subscribers that are logged in on top of a LAG bundle
- *filter*—See Filtering show Commands
- *summary*—Displays the active subscribers for each domain, interface, port, slot, or virtual router

**Mode** Privileged Exec

## PART 4

# Troubleshooting

- [SNMP Traps and System Logs for Authentication Failures on page 347](#)
- [Configuring SNMP Traps on page 349](#)
- [Troubleshooting RADIUS Preauthentication Failure on page 351](#)











## CHAPTER 42

# Troubleshooting RADIUS Preauthentication Failure

- [Troubleshooting Subscriber Preauthentication on page 351](#)

### Troubleshooting Subscriber Preauthentication

---

**Problem** 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.

**Solution** 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.

- Related Documentation**
- [Configuring SNMP Traps on page 349](#)
  - [radius trap auth-server-not-responding on page 175](#)



## PART 5

# Index

- [Index on page 355](#)

























